



**WS6603 Radio Access Controller
V100R003C05**

Configuration Guide

Issue 03
Date 2012-07-10

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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

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

Email: support@huawei.com

About This Document

Product Version

The following table lists the applicable product version of this document.

Product Name	Product Version
WS6603	V100R003C05
U2560	V100R003C00

Intended Audience




This document describes the configuration of the WS6603.



This document is intended for:

- Installation and commissioning engineers
- System maintenance engineers
- Data configuration engineers

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.

Symbol	Description
 NOTE	Indicates a tip that may help you solve a problem or save time.
 TIP	Provides additional information to emphasize or supplement important points in the main text.

Change History

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

Changes in Issue 03 (2012-07-10)

This issue is the third official release.

The third commercial release has the following updates:

The following sections are modified:

- Example for Configuring the WLAN Service
- Configuring a WLAN Security Policy

Changes in Issue 02 (2011-09-30)

This issue is the second official release.

Changes in Issue 01 (2011-08-15)

This issue is the first official release.

Contents

About This Document.....	ii
1 Commissioning.....	1
1.1 Logging In to the AC to Check the Software Version.....	2
1.1.1 Logging in Through the Serial Port.....	2
1.1.2 Checking the Software Version.....	5
1.2 WS6603 Maintenance Configuration.....	6
1.2.1 Maintaining the WS6603 Locally.....	6
1.2.2 Maintaining the AC Remotely.....	7
1.3 Basic Configurations.....	29
1.3.1 Changing the System Name.....	29
1.3.2 Setting the System Time.....	29
1.3.3 Configuring a System User.....	31
1.3.4 Configuring a Port.....	35
1.4 Configuring the License Function.....	38
1.5 Saving and Backing Up Data.....	39
1.5.1 Configuring the File Transfer Mode.....	40
1.5.2 Saving and Backing Up Data Manually.....	46
1.5.3 Saving and Backing Up Data Automatically.....	50
2 Basic Configurations.....	56
2.1 Configuring the Network Time.....	57
2.1.1 (Optional) Configuring NTP Authentication.....	58
2.1.2 Configuring the NTP Broadcast Mode.....	59
2.1.3 Configuring the NTP Multicast Mode.....	61
2.1.4 Configuring the NTP Client/Server Mode.....	64
2.2 Configuring System Security.....	65
2.2.1 Configuring the Firewall.....	66
2.2.2 Configuring Defense Against Malicious Attacks.....	68
2.2.3 Configuring a Permitted/Denied IP Address Segment.....	69
2.3 Configuring an ACL.....	71
2.3.1 Configuring a Basic ACL.....	72
2.3.2 Configuring an Advanced ACL.....	73
2.3.3 Configuring a Link Layer ACL.....	75

2.3.4 Configuring a User-defined ACL.....	76
2.4 Configuring QoS.....	78
2.4.1 Configuring Traffic Management.....	79
2.4.2 Configuring Queue Scheduling.....	81
2.4.3 Configuring ACL-based Traffic Management.....	84
3 Configuring the WLAN Service.....	89
3.1 Configuring an Carrier ID and an AC ID.....	93
3.2 Configuring the Layer 3 Interfaces.....	93
3.3 Configuring the DHCP Server.....	94
3.4 Configuring the Version Upgrade Mode for an AP.....	95
3.5 Configuring the Data Forwarding Mode.....	96
3.6 Adding an AP and Getting it Online.....	97
3.7 Configuring a WLAN Radio.....	98
3.7.1 Configuring a Radio Profile.....	99
3.7.2 Binding a Radio Profile to a Radio.....	100
3.7.3 Configuring the Radio Calibration Function for an AP Region.....	101
3.7.4 (Optional) Configuring AP Radio Resource Management.....	101
3.7.5 (Optional) Configuring an AP Load Balancing Group.....	102
3.8 Configuring the ESS and VAP.....	102
3.8.1 Configuring an ESS.....	103
3.8.2 Configuring a VAP and Binding an ESS to the VAP.....	104
3.9 Configuring a QoS Policy on a WLAN.....	105
3.9.1 Configuring a Radio QoS Policy.....	105
3.9.2 Configuring a VAP QoS Policy.....	106
3.10 Configuring a WLAN Security Policy.....	108
3.11 Configuring 802.11n.....	110
3.12 Viewing AP Information.....	111
4 Configuring WLAN Services.....	113
4.1 WLAN Networking.....	114
4.2 WLAN Service Configuration Procedure.....	115
4.3 Example for Configuring the WLAN Service.....	116
4.3.1 Example for Configuring Services for Layer 2 Chain Networking (Data Forwarded by Tunnel).....	116
4.3.2 Example for Configuring VLAN Services in a Layer 2 Branched Networking (Direct Forwarding)	125
4.3.3 Example for Configuring VLAN Services in a Layer 3 Chain Networking (Direct Forwarding).....	134
4.3.4 Example for Configuring VLAN Services in a Layer 3 Branched Networking (Tunnel Forwarding)	144
4.3.5 Example for Configuring VLAN Services in a Layer 2 Chain Networking (Two-Node Hot Backup)	153
4.3.6 Example for Configuring VLAN Services in a Layer 3 Branched Networking (Two-Node Hot Backup)	168
4.3.7 Configuring QoS Policies for APs.....	185
4.3.8 Configuring Security Policies for APs.....	191

4.3.9 Example for Configuring an AP Load Balancing Group.....	198
5 Protocol Configurations.....	204
5.1 Configuring Routing.....	205
5.1.1 Example for Configuring a Routing Policy.....	205
5.1.2 Example for Configuring Static Routes.....	207
5.1.3 Example for Configuring RIP.....	209
5.1.4 Example for Configuring OSPF.....	212
5.1.5 Example for Configuring IS-IS.....	216
5.1.6 Example for Configuring BGP.....	218
5.2 Configuring DHCP.....	222
5.2.1 Configuring the Standard DHCP Mode.....	223
5.2.2 Configuring the DHCP Server Mode.....	225
5.2.3 Configuring the DHCP Option 43 Function.....	226
5.2.4 Configuring the DHCP Option 60 Mode.....	227
5.2.5 Configuring the DHCP Option 15 Function.....	229
5.2.6 Configuring the DHCP MAC Address Segment Mode.....	231
5.3 Configuring AAA.....	233
5.3.1 Configuring Remote AAA (RADIUS).....	234
5.3.2 Example for Configuring RADIUS Authentication and Accounting.....	237
5.4 Configuring MSTP.....	240
5.5 Configuring Ethernet CFM OAM.....	243
6 Configuring the Multicast Service.....	247
6.1 Default Settings of the Multicast Service.....	248
6.1.1 Setting Global Multicast Parameters.....	248
6.1.2 Configuring a Multicast VLAN and a Multicast Program.....	250
7 Operation and Maintenance Management.....	253
7.1 Configuring Alarms.....	254
7.2 Configuring a New AP Replacement Quickly.....	255

1 Commissioning

About This Chapter

This document describes the commissioning of the basic functions provided by the WS6603 in terms of hardware, software, interconnection, and maintenance and management.

[1.1 Logging In to the AC to Check the Software Version](#)

This section describes how to log in to an AC through the serial port to check the software version.

[1.2 WS6603 Maintenance Configuration](#)

You can use a maintenance terminal to log in to and maintain the WS6603 locally or remotely.

[1.3 Basic Configurations](#)

This section describes the basic configurations, including modification of the system name and configuration of the system time and system user.

[1.4 Configuring the License Function](#)

The license platform provides the registration mechanism for the AC. During system initialization, the AC needs to register controlled resource entries or function entries.

[1.5 Saving and Backing Up Data](#)

The AC supports data saving and backup to prevent data loss in case of an upgrade failure or any other critical events.

1.1 Logging In to the AC to Check the Software Version

This section describes how to log in to an AC through the serial port to check the software version.

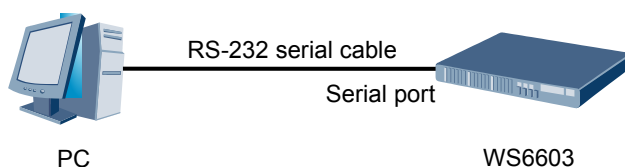
1.1.1 Logging in Through the Serial Port

This section describes how to connect the maintenance terminal to the AC through the serial port and log in to the AC to maintain it.

Network Diagram

Figure 1-1 shows the network for login through a local serial port.

Figure 1-1 Network diagram for login through a local serial port



Procedure

Step 1 Connect a serial cable.

Use a standard RS-232 serial cable to connect the serial port of the PC to the CON port (the maintenance serial port) on the WAC board of the AC, as shown in **Figure 1-1**.

Step 2 Start the HyperTerminal.

1. Set up a connection.

Choose **Start > Programs > Accessories > Communications > HyperTerminal** on the PC. The **Connection Description** dialog box is displayed. Enter the connection name, as shown in **Figure 1-2**, and click **OK**.

Figure 1-2 Setting up a connection



2. Configure the serial port.

Select the number of the standard character terminal or PC terminal serial port on the PC that is connected to the AC, for example, "COM1", as shown in [Figure 1-3](#). Click **OK**.

Figure 1-3 Selecting the serial port



Step 3 Set communication parameters of the HyperTerminal.

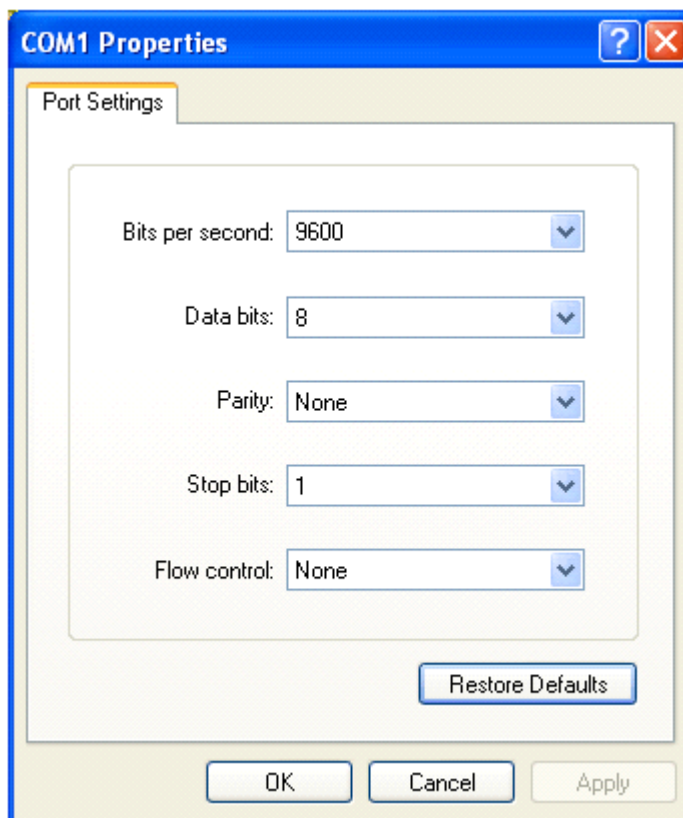
Set the parameters in the **COM1 Properties** dialog box, as shown in [Figure 1-4](#). The parameters are as follows:

- Baud rate: 9600 bit/s
- Data bit: 8
- Parity: None
- Stop bit: 1
- Flow control: None

 **NOTE**

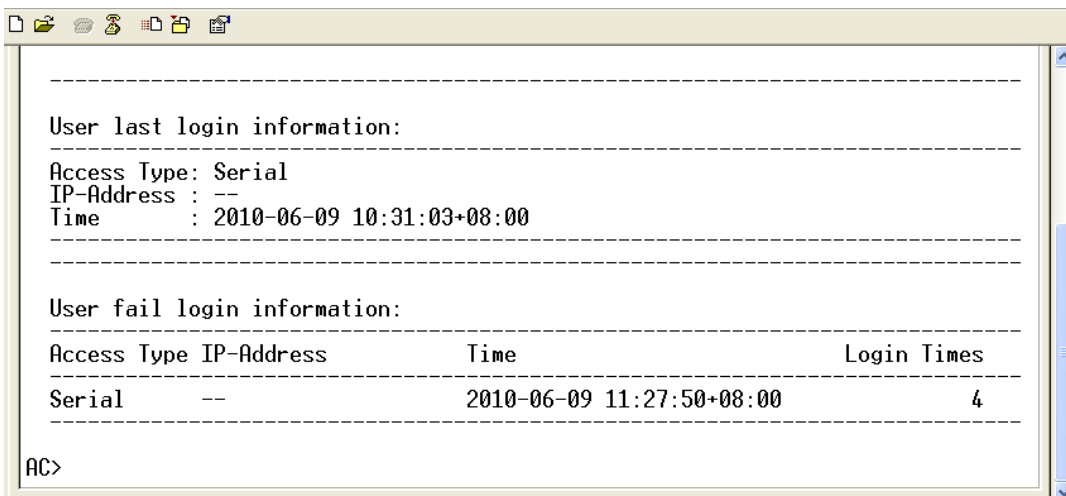
- The baud rate of the HyperTerminal must be the same as the baud rate of the serial port on the AC. By default, the baud rate of the serial port is 9600 bit/s.
- There may be garbled characters in the displayed input information after you log in to the system. This is because the baud rates on the HyperTerminal and the AC are different. Set a different baud rate to log in to the system. The system supports the baud rates of 9600 bit/s, 19200 bit/s, 38400 bit/s, 57600 bit/s, and 115200 bit/s.

Figure 1-4 Setting the parameters of the HyperTerminal



Click **OK** to display the HyperTerminal interface, as shown in [Figure 1-5](#).

Figure 1-5 HyperTerminal interface



----End

Result

On the HyperTerminal interface, press **Enter**, and the system prompts you to enter the user name. Enter the user name and the password (by default, the super user name is **root** and the password is **admin**), and wait until the CLI prompt (such as WAC>) is displayed.

If the login fails, click the **Hang-up** icon, and then click the **Dial** icon. If the login still fails, return to step 1 to check the parameter settings and the physical connections, and then try again.

1.1.2 Checking the Software Version

This section describes how to check the software version.

Procedure

- Step 1** Run the **display language** command to check whether the version of the host software meets deployment requirements.
- Step 2** Run the **display version** command to check whether the version of the board software meets deployment requirements.
- Step 3** Run the **filesystem cmd dir /all** to check whether the version software in the flash memory is correct.

----End

Result

- The version of the host software and the version of the board software meet deployment requirements.
- If the version of the host software and the version of the board software do not meet deployment requirements, contact the Huawei Customer Service Center. Upgrade the host software if necessary.

Example

Check the host software version and the board software version that are running in the system.

```

huawei>display language
Local:
  Description: CHINESE SIMPLIFIED (DEFAULT LANGUAGE)
  Version:    WS6603V100R003C05
  Encoding:   GBK

General:
  Description: ENGLISH (DEFAULT LANGUAGE)
  Version:    WS6603V100R003C05
  Encoding:   ANSI
huawei>display version
{ <cr>|backplane<K>|frameid/slotid<S><Length 1-15> }:
Command:
    display version

VERSION : WS6603V100R003C05
PATCH  : SPC100
PRODUCT WS6603
Uptime is 5 day(s), 1 hour(s), 16 minute(s), 44 second(s)
huawei>enable
huawei#filesystem cmd dir /all
Directory of flash:/

 0  -rw-   227824  Nov 13 2010 02:29:01  data_bak.dat
 1  -rw-  15162118  Nov 11 2010 02:11:49  program.efs
 2  -rw-  15162118  Nov 13 2010 02:26:15  program_bak.efs
 3  -rw-   227824  Nov 11 2010 02:15:01  data.dat
 4  -rw-    774    Nov 11 2010 02:06:40  ver_match.efs
 5  -rw-   52490   Nov 11 2010 02:14:51  cpldl.efs
 6  -rw-     4     Apr 08 2010 13:13:53  lic_switch.efs
 7  -rw-   1584   Oct 25 2010 00:30:40  lic.efs
 8  -rw-    396   Apr 08 2010 16:25:54  rsa_host_key.efs
 9  -rw-    540   Jul 18 2010 15:58:27  rsa_server_key.efs
10  -rw-   4512   Nov 11 2010 02:45:44  patch_load.efs
11  -rw-     11   Jul 01 2010 19:27:50  test.txt
12  -rw-   1192   Nov 16 2010 02:24:44  alm_static.efs
13  -rw-    494   Nov 09 2010 00:24:02  cfm.efs
14  -rw-  6365506  Nov 02 2010 21:53:13  wa6x3xn_v100r003c01b013.bin
15  -rw-    394   Aug 05 2010 22:42:43  owner.efs
16  -rw-   32667  Oct 19 2010 02:15:56  iposlogbufffile.dat
17  -rw-   19147  Apr 21 2010 23:11:44  iposlogfile1.dat
18  -rw-  6379423  Nov 05 2010 04:16:11  wa6x1_v100r003c01b013_k.bin
19  -rw- 16511555  Oct 10 2010 05:27:51  ws6x3xn_v100r003c01b012_k.bin
20  -rw-  6365506  Oct 12 2010 00:21:47  wa6x3xn_v100r003c01b015.bin
21  -rw-   16600  Jul 30 2010 14:33:43  wlan_log.txt
22  -rw-  6160412  Aug 06 2010 11:49:23  wa6x1_v100r001c01spc300b075.bin
23  -rw-  6379423  Nov 04 2010 19:31:39  wa6x1_v100r003c01b021_k.bin
24  -rw-  6184860  Nov 07 2010 06:29:36  wa6x1_v100r003c01b021.bin

116392960 bytes total (31116288 bytes free)

```

1.2 WS6603 Maintenance Configuration

You can use a maintenance terminal to log in to and maintain the WS6603 locally or remotely.

1.2.1 Maintaining the WS6603 Locally

This section describes how to log in to the WS6603 (AC) through a local serial port to maintain the AC.

Context

For details on how to log in to the AC through the local serial port, see [1.1.1 Logging in Through the Serial Port](#).

1.2.2 Maintaining the AC Remotely

This section describes how to log in to the WS6603 (AC) remotely to maintain the AC.

Login Through Telnet (Inband Management)

This section describes how to log in to an AC through the uplink port (inband management port) in Telnet mode to maintain and manage the AC.

Prerequisites

You have logged in to the AC through the local serial port. For details on how to log in to the AC through the local serial port, see [1.1.1 Logging in Through the Serial Port](#).

NOTE

In the following operations, the configurations on the AC must be performed through a local serial port.

Networking

[Figure 1-6](#) and [Figure 1-7](#) show the networks for configuring outband management over a LAN and a WAN through Telnet.

Figure 1-6 Network for configuring inband management over a LAN through Telnet

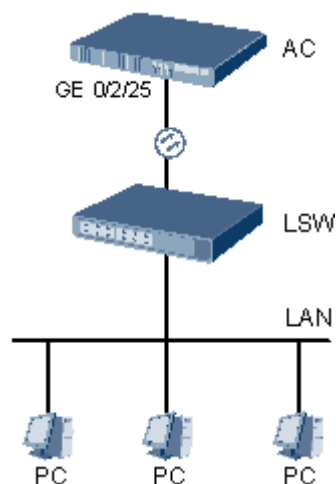
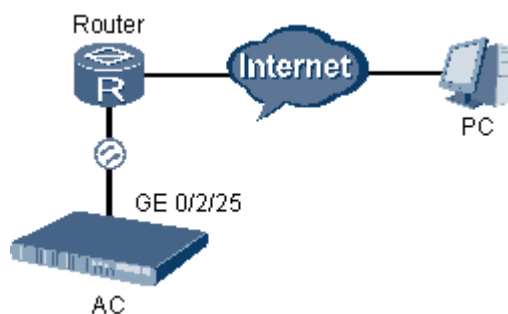


Figure 1-7 Network for configuring inband management over a WAN through Telnet



Data Plan

Table 1-1 provides the data plan for configuring inband management through Telnet.

Table 1-1 Data plan for configuring inband management through Telnet

Configuration Item	Data
Uplink port	<ul style="list-style-type: none">● VLAN ID: 30● Port number: 0/2/25● IP address: 10.50.1.10/24
Maintenance terminal	IP address: 10.10.1.10/24
Interface of the router connected to the AC (used when inband management is configured over a WAN through Telnet)	IP address: 10.50.1.1/24

Procedure

Step 1 Set up a network environment.

- If you log in to the AC through Telnet in inband management mode over a LAN, set up a network environment according to [Figure 1-6](#).
- If you log in to the AC through Telnet in inband management mode over a WAN, set up a network environment according to [Figure 1-7](#).

Step 2 Configure an IP address for the VLANIF interface.

1. Run the **vlan** command to create a management VLAN.

```
huawei(config)#vlan 30
```
2. Run the **port vlan** command to add an uplink port to the VLAN.

```
huawei(config)#port vlan 30 0/2 25
```
3. Run the **ip address** command to assign an IP address to the VLANIF interface.

```
huawei(config)#interface vlanif 30  
huawei(config-if-vlanif30)#ip address 10.50.1.10 24
```



NOTE

If incoming packets do not carry VLAN tags on the Ethernet port, run the **native-vlan** command to configure the default VLAN of the uplink port to be the same as the VLAN of the uplink port.

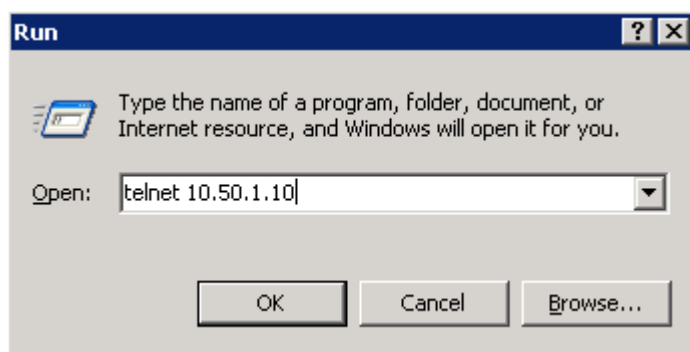
Step 3 Add a route for inband management.

- If the network environment is set up according to [Figure 1-6](#), you do not need to add a route.
- If the network environment is set up according to [Figure 1-7](#), run the **ip route-static** command to add a route from the maintenance network port on the AC to the maintenance terminal.

```
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 4 Run the Telnet application.

On the maintenance terminal running Windows, choose **Start > Run**. Enter **telnet 10.50.1.10** in the **Run** window as shown in [Figure 1-8](#), and click **OK**. The Telnet window is displayed.

Figure 1-8 Running the Telnet application**Step 5** Log in to the AC.

In the Telnet window, enter the user name and the password. By default, the user name is **root** and the password is **admin**. When login is successful, the system displays the following information:

```
>>User name:root
>>User password:admin //It is not displayed on the maintenance
terminal.
```

```
Huawei Integrated Access Software.
Copyright(C) Huawei Technologies Co., Ltd. 2002-2009. All rights reserved.
```

----End

Result

After logging in to the AC, you can maintain and manage the AC.

Logging In to the WS6603 Through Telnet (Outband Management)

This section describes how to log in to an AC through the local maintenance network port (Ethernet port or outband management port) in Telnet mode to maintain and manage the AC.

Prerequisites

You have logged in to the AC through the local serial port. For details on how to log in to the AC through the local serial port, see [1.1.1 Logging in Through the Serial Port](#).

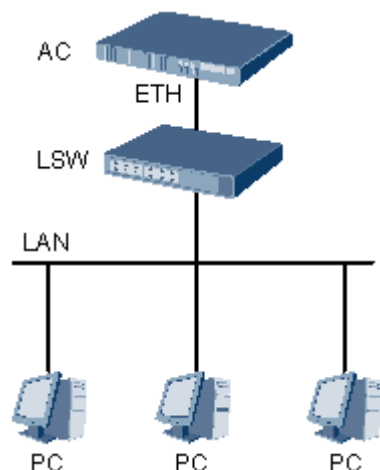
 **NOTE**

In the following operations, the configurations on the AC must be performed through a local serial port.

Networking

[Figure 1-9](#) and [Figure 1-10](#) show the networks for configuring outband management over a LAN and a WAN through Telnet.

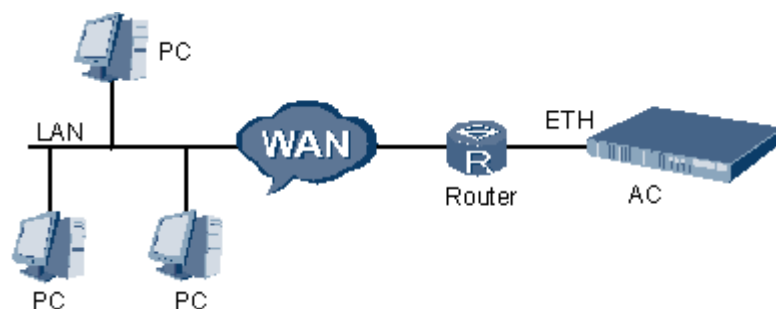
Figure 1-9 Network for configuring outband management over a LAN through Telnet



NOTE

The AC connects to the LAN through a straight-through cable, and the IP address of the maintenance network port on the AC and the IP address of the maintenance terminal are located on the same network segment. Alternatively, the Ethernet port on the maintenance terminal can directly connect to the maintenance network port on the AC through a crossover cable, implementing outband management.

Figure 1-10 Network for configuring outband management over a WAN through Telnet



Data Plan

Table 1-2 and **Table 1-3** provide the data plan for configuring outband management over a LAN through Telnet.

Table 1-2 Data plan for configuring outband management over a LAN through Telnet

Configuration Item	Data
Maintenance network port	IP address: 10.50.1.10/24 NOTE By default, the IP address of the maintenance network port (ETH port on the main control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.
Maintenance terminal	IP address: 10.50.1.20/24 (it must be on the same network segment as the IP address of the maintenance network port)

Table 1-3 Data plan for configuring outband management over a WAN through Telnet

Configuration Item	Data
Maintenance network port	IP address: 10.50.1.10/24 NOTE By default, the IP address of the maintenance network port (ETH port on the main control board) is 10.11.104.2, and the subnet mask is 255.255.255.0.
Maintenance terminal	IP address: 10.10.1.10/24
Port on the router connected to the AC	IP address: 10.50.1.1/24

Procedure

Step 1 Set up a network environment.

- If you log in to the AC through Telnet in outband management mode over a LAN, set up a network environment according to [Figure 1-9](#).
- If you log in to the AC through Telnet in outband management mode over a WAN, set up a network environment according to [Figure 1-10](#).

Step 2 Configure an IP address for the maintenance network port.

Run the **ip address** command on the MEth port to configure the IP address for the maintenance network port.

```
huawei (config) #interface meth 0
huawei (config-if-meth0) #ip address 10.50.1.10 24
```

Step 3 Add a route for outband management.

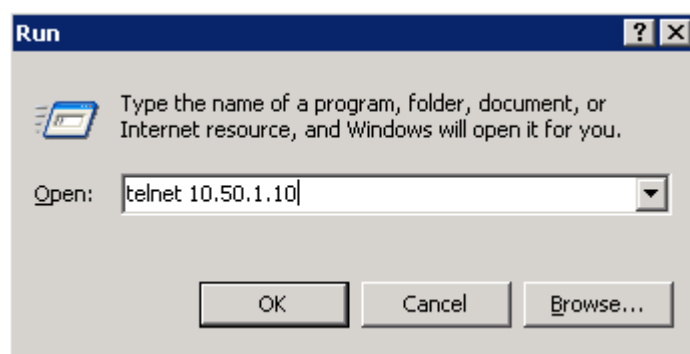
- If the configuration environment is set up according to [Figure 1-9](#), you do not need to add a route.
- If the network environment is set up according to [Figure 1-10](#), run the **ip route-static** command to add a route from the maintenance network port on the AC to the maintenance terminal.

```
huawei (config-if-meth0) #quit
huawei (config) #ip route-static 10.10.1.0 24 10.50.1.1
```

Step 4 Run the Telnet application.

On the maintenance terminal running Windows, choose **Start > Run**. Enter **telnet 10.50.1.10** in the **Run** window as shown in [Figure 1-11](#), and click **OK**. The Telnet window is displayed.

Figure 1-11 Running the Telnet application



Step 5 Log in to the AC.

In the Telnet window, enter the user name and the password. By default, the user name is **root** and the password is **admin**. When login is successful, the system displays the following information:

```
>>User name:root
>>User password:admin //It is not displayed on the maintenance
terminal.
```

```
Huawei Integrated Access Software.
Copyright(C) Huawei Technologies Co., Ltd. 2002-2009. All rights reserved.
```

----End

Result

After logging in to the AC, you can maintain and manage the AC.

Login Through SSH (Inband Management)

This section describes how to log in to an AC through the uplink port (inband management port) in SSH mode to maintain and manage the AC. SSH provides authentication, encryption, and authorization to guarantee security of networks. When a user logs in to an AC on an insecure network, SSH guarantees security and provides authentication for the login user, and defends against various attacks, including IP address spoofing and plain text password interception.

Prerequisites

- You have logged in to the AC through the local serial port. For details on how to log in to the AC through the local serial port, see [1.1.1 Logging in Through the Serial Port](#).

NOTE

In the following operations, the configurations on the AC must be performed through a local serial port.

- The tools for commissioning login through Telnet are ready: client software key generator Puttygen.exe, client software key converter sshkey.exe, and SSH client software putty.exe.

Networking

[Figure 1-12](#) and [Figure 1-13](#) show the networks for configuring inband management over a LAN and a WAN through SSH.

Figure 1-12 Network for configuring inband management over a LAN through SSH

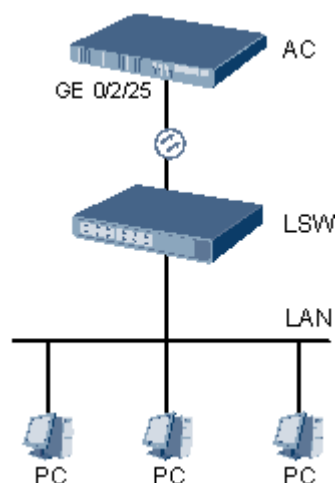
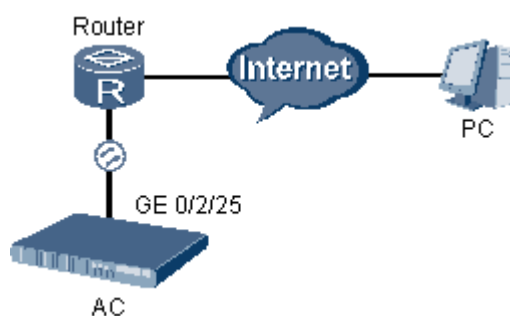


Figure 1-13 Network for configuring inband management over a WAN through SSH



Data Plan

Table 1-4 provides the data plan for logging in to the AC through SSH.

Table 1-4 Data plan for logging in to the AC through SSH

Configuration Item	Data
Uplink port of the AC	<ul style="list-style-type: none"> ● VLAN ID: 30 ● Port number: 0/2/25 ● IP address: 10.50.1.10/24 ● User authentication: RSA public key authentication ● RSA public key name: key
New user	<ul style="list-style-type: none"> ● User name/Password: huawei/test01 ● Authority: operator ● Number of permitted times that the user can log in: 4
Maintenance terminal	IP address: 10.10.1.10/24

Configuration Item	Data
Interface of the router connected to the AC (used when inband management is configured over a WAN through SSH)	IP address: 10.50.1.1/24

Procedure

Step 1 Set up a network environment.

- If you log in to the AC through SSH in inband management mode over a LAN, set up a network environment according to [Figure 1-12](#).
- If you log in to the AC through SSH in inband management mode over a WAN, set up a network environment according to [Figure 1-13](#).

Step 2 Configure an IP address for the VLANIF interface.

1. Run the **vlan** command to create a management VLAN.

```
huawei(config)#vlan 30
```
2. Run the **port vlan** command to add an uplink port to the VLAN.

```
huawei(config)#port vlan 30 0/2 25
```
3. Run the **ip address** command to assign an IP address to the VLANIF interface.

```
huawei(config)#interface vlanif 30
huawei(config-if-vlanif30)#ip address 10.50.1.10 24
```



NOTE

If incoming packets do not carry VLAN tags on the Ethernet port, run the **native-vlan** command to configure the default VLAN of the uplink port to be the same as the VLAN of the uplink port.

Step 3 Add a route for inband management.

- If the network environment is set up according to [Figure 1-12](#), you do not need to add a route.
- If the network environment is set up according to [Figure 1-13](#), run the **ip route-static** command to add a route from the maintenance network port on the AC to the maintenance terminal.

```
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 4 Add a user.

Run the **terminal user name** command to add a user.

```
huawei(config)#terminal user name
User Name(length<6,15>):huawei
User Password(length<6,15>):test01//It is not displayed on the maintenance
terminal.
Confirm Password(length<6,15>):test01//It is not displayed on the maintenance
terminal.
User profile name(<=15 chars)[root]:
User's Level:
  1. Common User  2. Operator:2
Permitted Reenter Number(0--4):4
User's Appended Info(<=30 chars):
Adding user succeeds
Repeat this operation? (y/n)[n]:n
```

Step 5 Create a local RSA key pair.

Run the **rsa local-key-pair create** command to create a local RSA key pair.



CAUTION

The prerequisite for login through SSH is that the local RSA key pair must be configured and generated. Before performing other SSH configuration, ensure that the local RSA key pair is generated.

```
huawei(config)#rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..+++++++
.....+++++++
.....+++++++
.....+++++++
```

Step 6 Set the SSH user authentication mode.

Run the **ssh user huawei authentication-type rsa** command to select an authentication mode.

The AC provides the following authentication modes: (RSA authentication is used as an example.)

- password: indicates authentication based on a password.
- rsa: indicates authentication based on an RSA public key.
- all: indicates authentication based on a password or an RSA public key. A user can log in to the AC using the password or the RSA public key.
- password-publickey: indicates authentication based on a password and a public key. A user can log in to the AC only after the user is authenticated in password authentication and RSA public key authentication.

```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

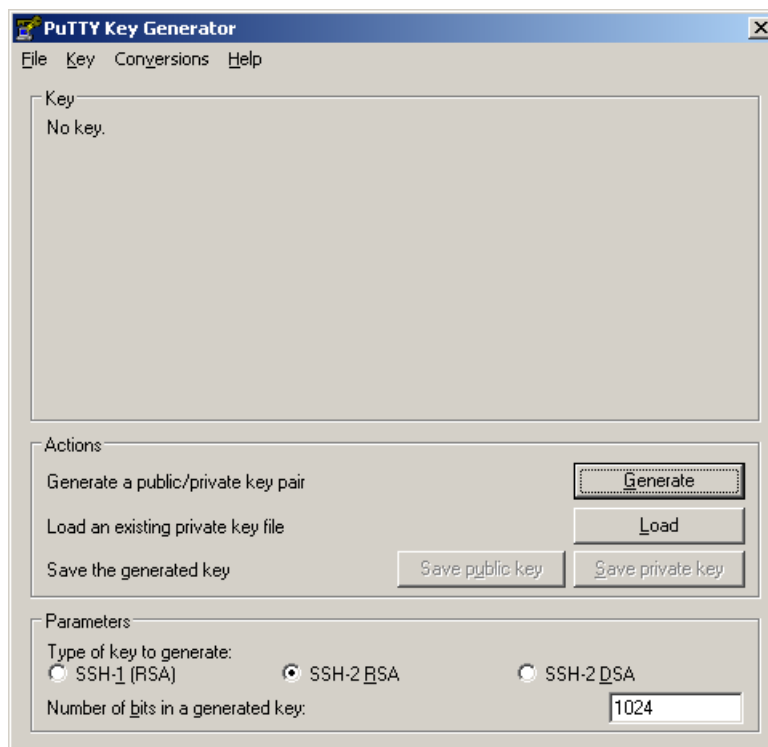
Command:
ssh user huawei authentication-type rsa
%Authentication type setted, and will be in effect next time.
```

Step 7 Generate an RSA public key.

1. Run the key generator.

Run the key generator Puttygen.exe. [Figure 1-14](#) shows the interface of the key generator.

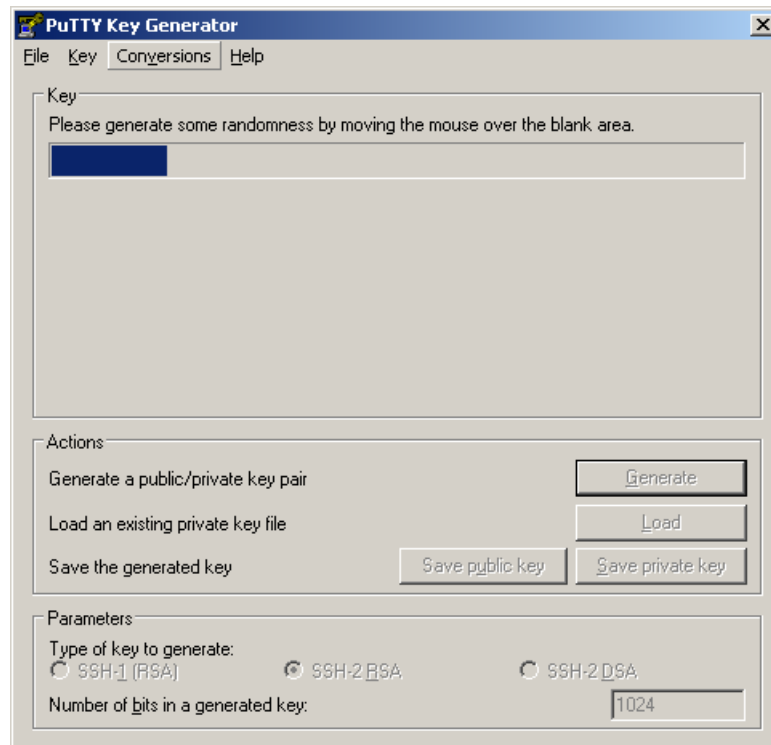
Figure 1-14 Interface of the key generator



2. Generate a client key.

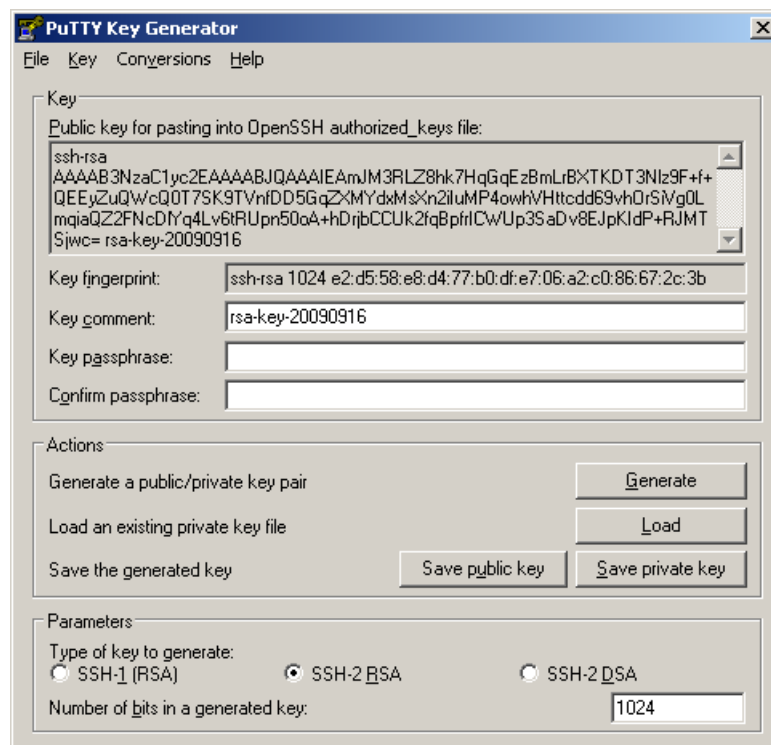
Select **SSH-2 RSA** as the key type under **Parameters**, click **Generate**, and move the cursor as prompted to generate a client key, as shown in [Figure 1-15](#).

Figure 1-15 Interface of the key generator



Click **Save public key** and **Save private key** to save the generated public key and private key, as shown in [Figure 1-16](#).

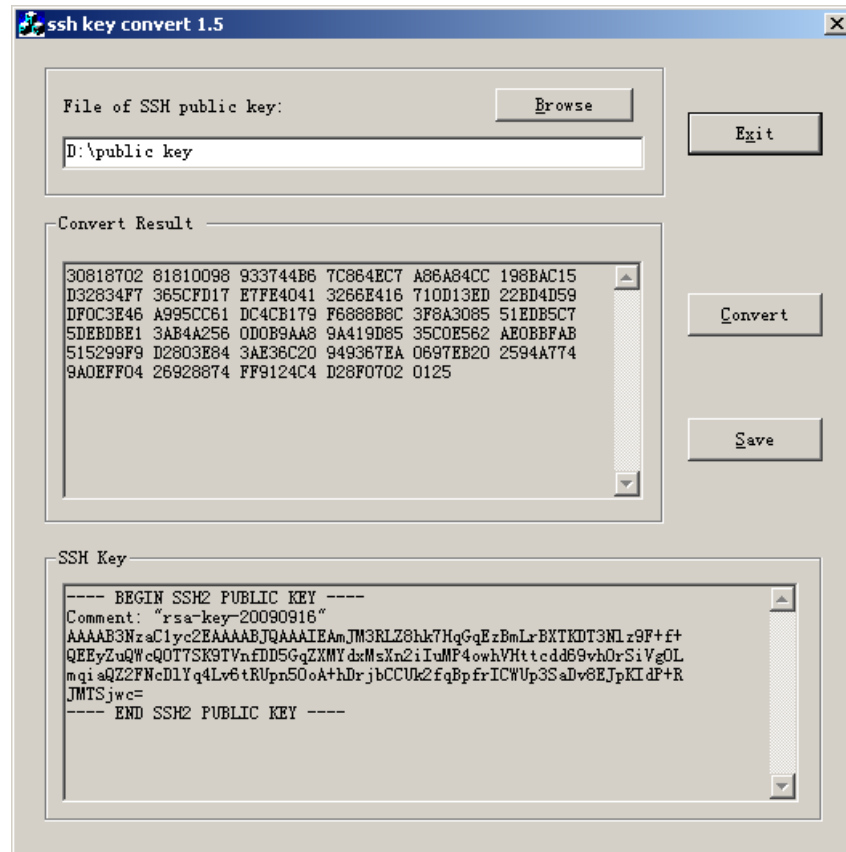
Figure 1-16 Saving the public key and the private key



3. Generate an RSA public key.

Run the key converter sshkey.exe. click **Browse**, and choose the public key file saved in the preceding step. Then click **Convert** to change the client public key to the RSA public key, as shown in [Figure 1-17](#).

Figure 1-17 Interface of converting the client public key to the RSA public key



Step 8 Generate a public key for the SSH user.

Create an RSA public key. Copy the RSA public key to the SSH server in config-rsa-key-code command line mode.

```
huawei(config)#rsa peer-public-key key
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.
```

```
huawei(config-rsa-public-key)#public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
```

```
huawei(config-rsa-key-code)#30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC15
```

```
huawei(config-rsa-key-code)#D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D59
```

```
huawei(config-rsa-key-code)#DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C7
```

```
huawei(config-rsa-key-code)#5DEDBE1 3AB4A256 0D0B9AA8 9A419D85 35C0E562 AE0BBFAB
```

```
huawei(config-rsa-key-code)#515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A774
```

```
huawei (config-rsa-key-code) #9A0EFF04 26928874 FF9124C4 D28F0702 0125
huawei (config-rsa-key-code) #public-key-code end
huawei (config-rsa-public-key) #peer-public-key end
```

Step 9 Assign the RSA public key to the SSH user.

Run the **ssh user assign rsa-key** command to assign the RSA public key to user **huawei**.

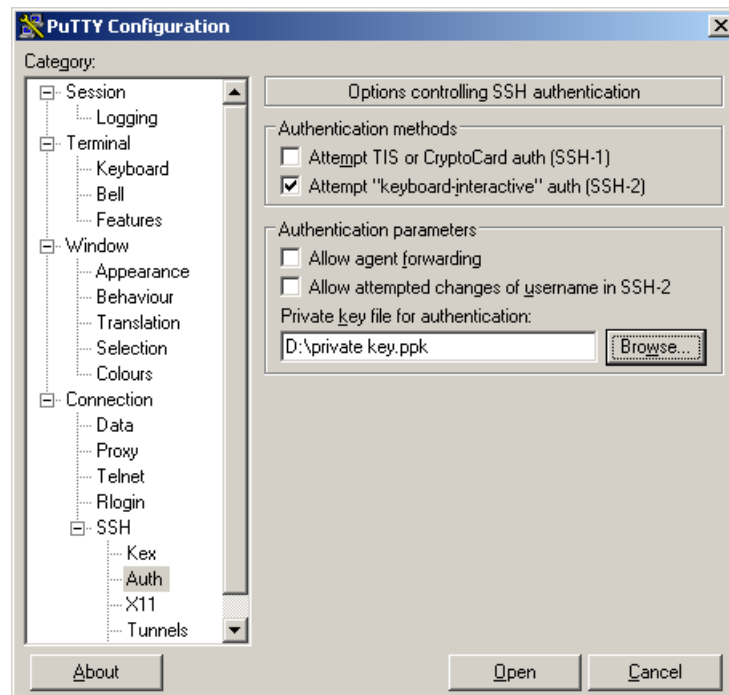
```
huawei (config) #ssh user huawei assign rsa-key key
```

Step 10 Log in to the AC.

1. Run the client software.

Run the SSH client software `putty.exe`, choose **SSH > Auth** from the navigation tree, and assign a file for the RSA private key, as shown in [Figure 1-18](#). Click **Browse** to display the window for selecting a file. In the window, select the file for the private key, and click **OK**.

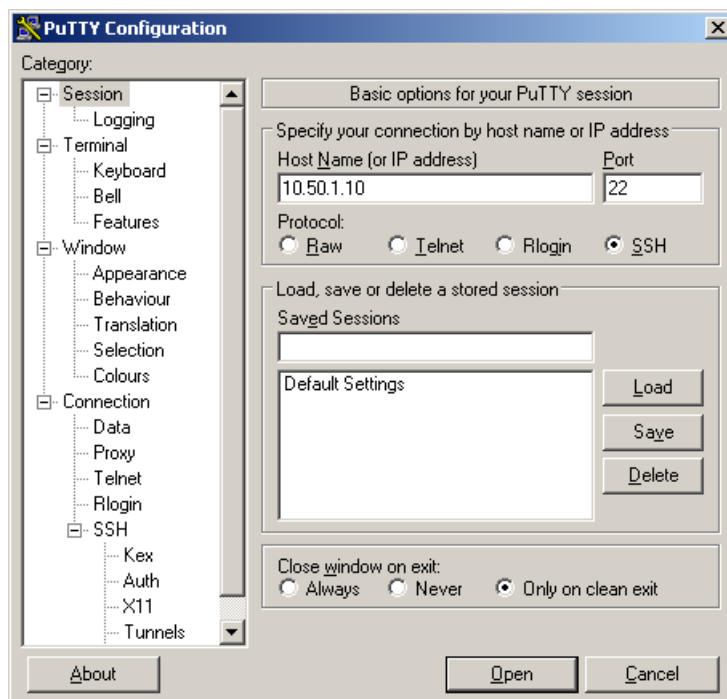
Figure 1-18 Interface of the SSH client software



2. Log in to the AC.

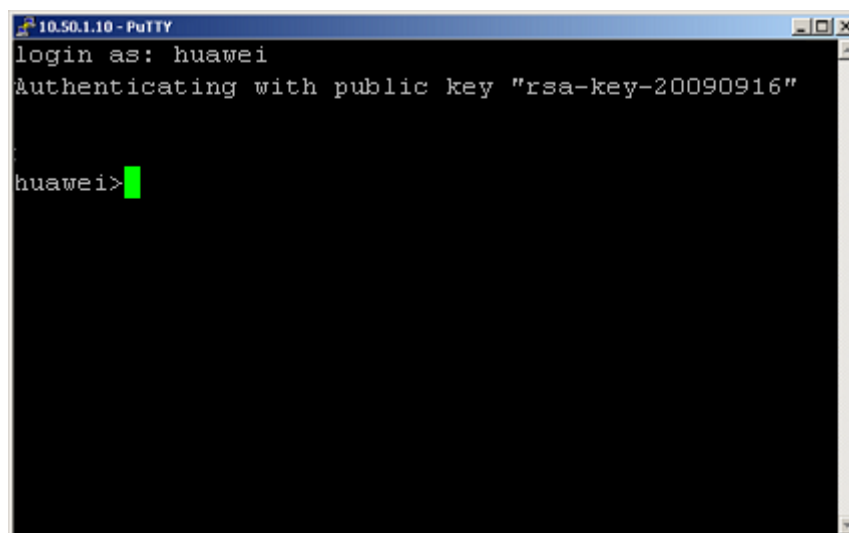
Click **Session**, enter the IP address of the AC in the **Host Name (or IP address)** text box, as shown in [Figure 1-19](#). Then click **Open** to log in to the AC.

Figure 1-19 Interface for logging in to the AC through the SSH client software



The user authentication mode is set to RSA authentication; therefore, the system displays the following message, as shown in **Figure 1-20**. Enter the user name to log in to the AC (here, the user name is **huawei**).

Figure 1-20 Interface for logging in to the AC through the SSH client software



----End

Result

After logging in to the AC, you can maintain and manage the AC.

Login Through SSH (Outband Management)

This section describes how to log in to an AC through the local maintenance network port (Ethernet port or outband management port) in SSH mode to maintain and manage the AC. SSH provides authentication, encryption, and authorization to guarantee security of networks. When a user logs in to an AC on an insecure network, SSH guarantees security and provides authentication for the login user, and defends against various attacks, including IP address spoofing and plain text password interception.

Prerequisites

- You have logged in to the AC through the local serial port. For details on how to log in to the AC through the local serial port, see [1.1.1 Logging in Through the Serial Port](#).

 **NOTE**

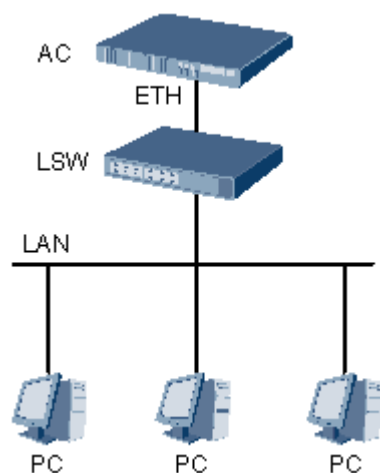
In the following operations, the configurations on the AC must be performed through a local serial port.

- The tools for commissioning login through Telnet are ready: client software key generator Puttygen.exe, client software key converter sshkey.exe, and SSH client software putty.exe.

Networking

[Figure 1-21](#) and [Figure 1-22](#) show the networks for configuring outband management over a LAN and a WAN through SSH.

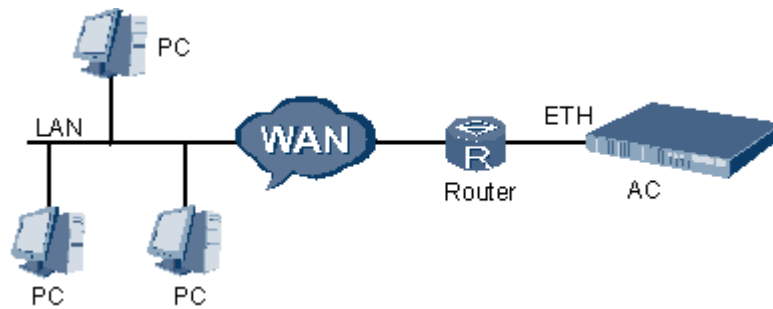
Figure 1-21 Network for configuring outband management over a LAN through SSH



 **NOTE**

The AC connects to the LAN through a straight-through cable, and the IP address of the maintenance network port on the AC and the IP address of the maintenance terminal are located on the same network segment. Alternatively, the Ethernet port on the maintenance terminal can directly connect to the maintenance network port on the AC through a crossover cable, implementing outband management.

Figure 1-22 Network for configuring outband management over a WAN through SSH



Data Plan

Table 1-5 provides the data plan for logging in to the AC through SSH.

Table 1-5 Data plan for logging in to the AC through SSH

Configuration Item	Data
AC network cable	<ul style="list-style-type: none"> ● IP address: 10.50.1.10/24 ● User authentication: RSA public key authentication ● RSA public key name: key
New user	<ul style="list-style-type: none"> ● User name/Password: huawei/test01 ● Authority: operator ● Number of permitted times that the user can log in: 4
Maintenance terminal	IP address: 10.10.1.10/24
Interface of the router connected to the AC (used when outband management is configured over a WAN through SSH)	IP address: 10.50.1.1/24

Procedure

Step 1 Set up a network environment.

- If you log in to the AC through SSH in outband management mode over a LAN, set up a network environment according to [Figure 1-21](#).
- If you log in to the AC through SSH in outband management mode over a WAN, set up a network environment according to [Figure 1-22](#).

Step 2 Configure an IP address for the maintenance network port.

Run the **ip address** command on the MEth port to configure the IP address for the maintenance network port.

```
huawei (config) #interface meth 0
huawei (config-if-meth0) #ip address 10.50.1.10 24
```

Step 3 Add a route for outband management.

- If the network environment is set up according to [Figure 1-21](#), you do not need to add a route.
- If the network environment is set up according to [Figure 1-22](#), run the **ip route-static** command to add a route originating from the AC's maintenance network port to the maintenance terminal.

```
huawei(config-if-meth0)#quit
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

Step 4 Add a user.

Run the **terminal user name** command to add a user.

```
huawei(config)#terminal user name
  User Name(length<6,15>):huawei
  User Password(length<6,15>):test01//It is not displayed on the maintenance
terminal.
  Confirm Password(length<6,15>):test01//It is not displayed on the maintenance
terminal.
  User profile name(<=15 chars)[root]:
  User's Level:
    1. Common User  2. Operator:2
  Permitted Reenter Number(0--4):4
  User's Appended Info(<=30 chars):
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n
```

Step 5 Create a local RSA key pair.

Run the **rsa local-key-pair create** command to create a local RSA key pair.



CAUTION

The prerequisite for login through SSH is that the local RSA key pair must be configured and generated. Before performing other SSH configuration, ensure that the local RSA key pair is generated.

```
huawei(config)#rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
        It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..+++++++
.....+++++++
.....+++++++
.....+++++++
.....+++++++
```

Step 6 Set the SSH user authentication mode.

Run the **ssh user huawei authentication-type rsa** command to select an authentication mode.

The AC provides the following authentication modes: (RSA authentication is used as an example.)

- password: indicates authentication based on a password.
- rsa: indicates authentication based on an RSA public key.
- all: indicates authentication based on a password or an RSA public key. A user can log in to the AC using the password or the RSA public key.

- password-publickey: indicates authentication based on a password and a public key. A user can log in to the AC only after the user is authenticated in password authentication and RSA public key authentication.

```
huawei(config)#ssh user huawei authentication-type  
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa
```

Command:

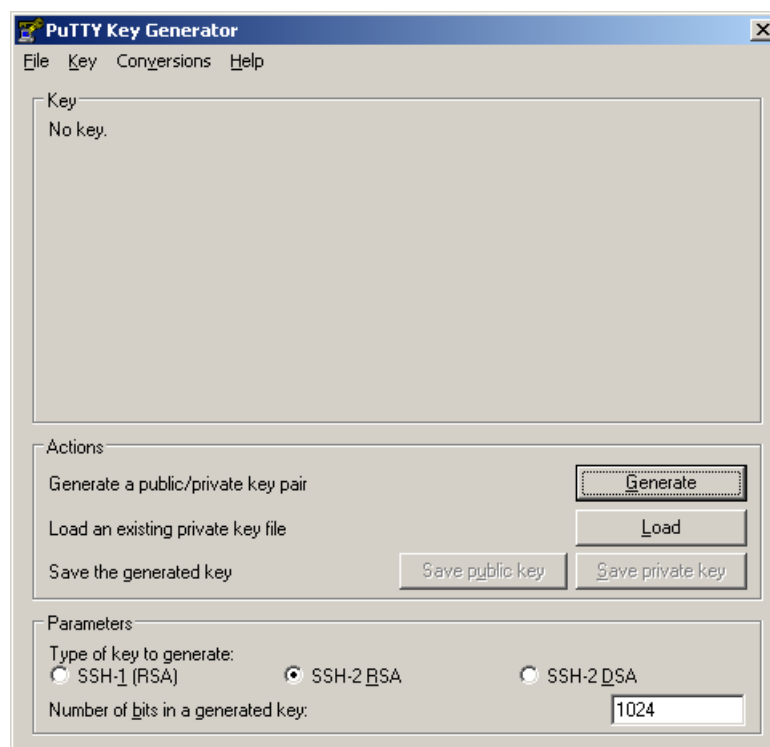
```
ssh user huawei authentication-type rsa  
%Authentication type setted, and will be in effect next time.
```

Step 7 Generate an RSA public key.

1. Run the key generator.

Run the key generator Puttygen.exe. **Figure 1-23** shows the interface of the key generator.

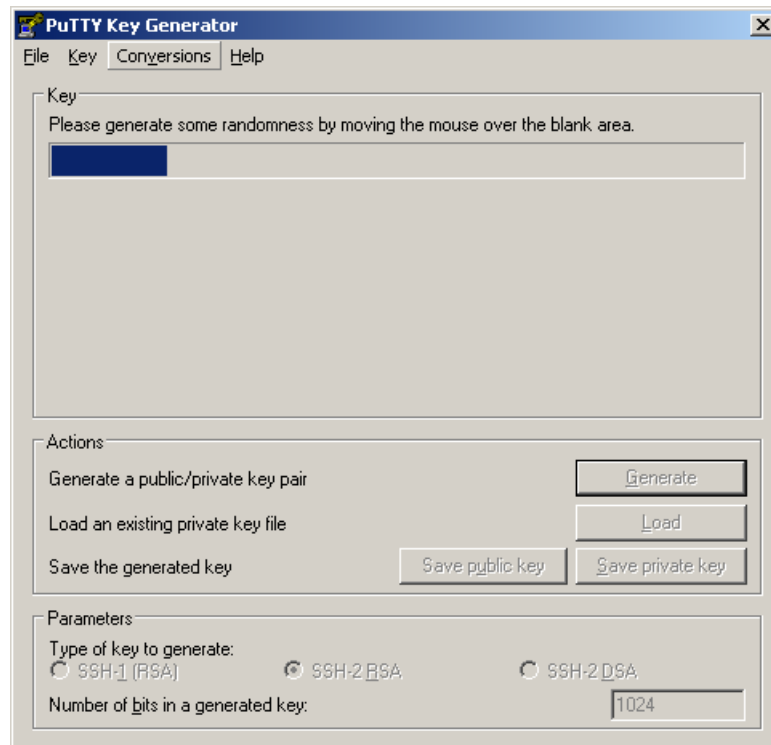
Figure 1-23 Interface of the key generator



2. Generate a client key.

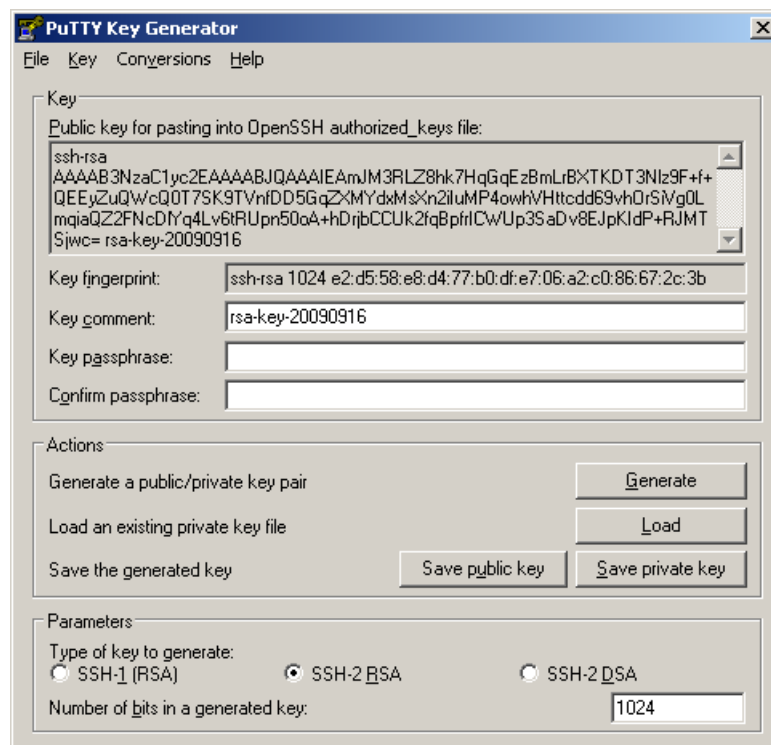
Select **SSH-2 RSA** as the key type under **Parameters**, click **Generate**, and move the cursor as prompted to generate a client key, as shown in **Figure 1-24**.

Figure 1-24 Interface of the key generator



Click **Save public key** and **Save private key** to save the generated public key and private key, as shown in [Figure 1-25](#).

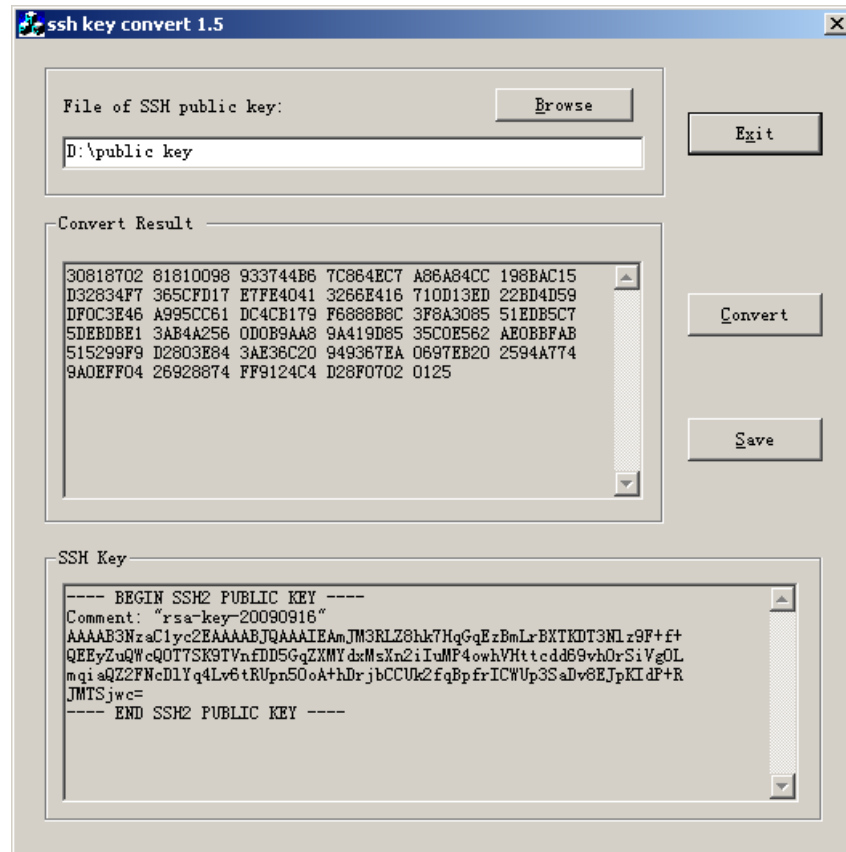
Figure 1-25 Saving the public key and the private key



3. Generate an RSA public key.

Run the key converter sshkey.exe. click **Browse**, and choose the public key file saved in the preceding step. Then click **Convert** to change the client public key to the RSA public key, as shown in [Figure 1-26](#).

Figure 1-26 Interface of converting the client public key to the RSA public key



Step 8 Generate a public key for the SSH user.

Create an RSA public key. Copy the RSA public key to the SSH server in config-rsa-key-code command line mode.

```
huawei(config)#rsa peer-public-key key
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.
```

```
huawei(config-rsa-public-key)#public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
```

```
huawei(config-rsa-key-code)#30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC15
```

```
huawei(config-rsa-key-code)#D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D59
```

```
huawei(config-rsa-key-code)#DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C7
```

```
huawei(config-rsa-key-code)#5DEDBE1 3AB4A256 0D0B9AA8 9A419D85 35C0E562 AE0BBFAB
```

```
huawei(config-rsa-key-code)#515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A774
```

```

huawei (config-rsa-key-code) #9A0EFF04 26928874 FF9124C4 D28F0702 0125
huawei (config-rsa-key-code) #public-key-code end
huawei (config-rsa-public-key) #peer-public-key end

```

Step 9 Assign the RSA public key to the SSH user.

Run the **ssh user assign rsa-key** command to assign the RSA public key to user **huawei**.

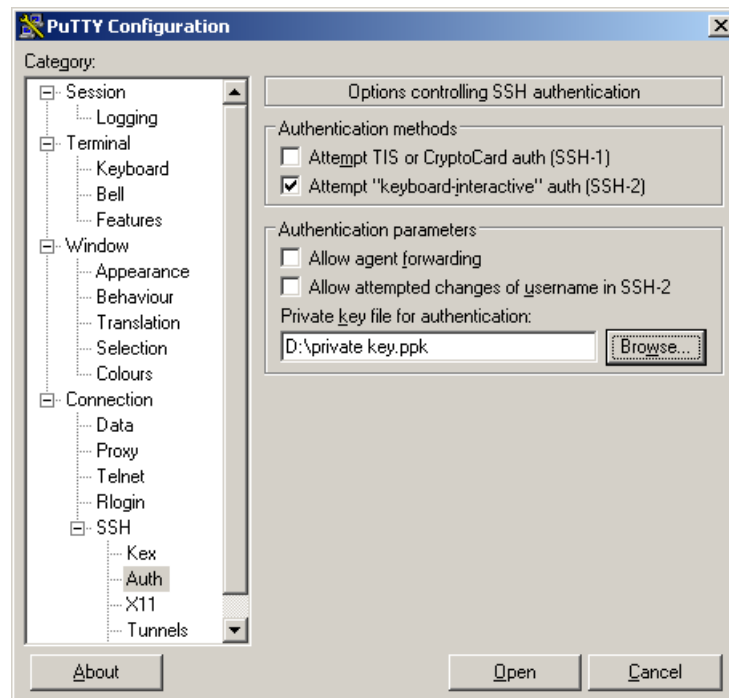
```
huawei (config) #ssh user huawei assign rsa-key key
```

Step 10 Log in to the AC.

1. Run the client software.

Run the SSH client software `putty.exe`, choose **SSH > Auth** from the navigation tree, and assign a file for the RSA private key, as shown in [Figure 1-27](#). Click **Browse** to display the window for selecting a file. In the window, select the file for the private key, and click **OK**.

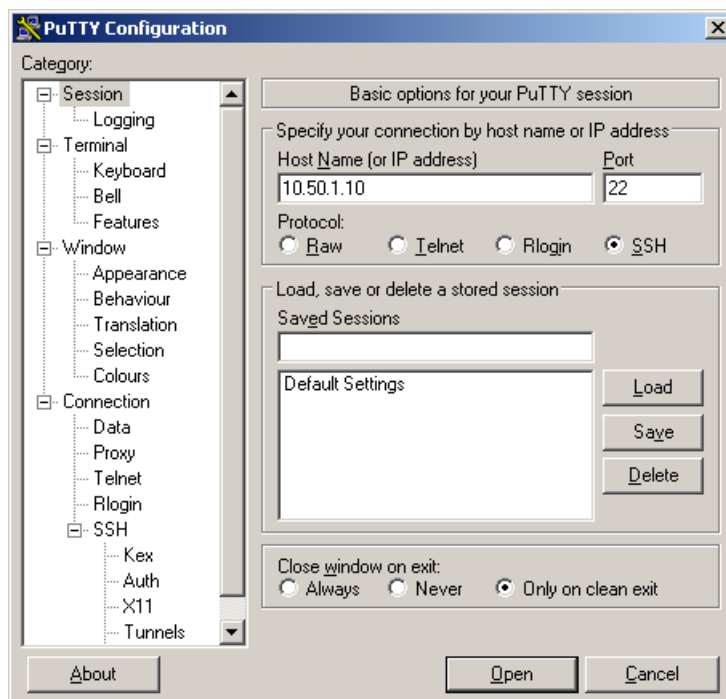
Figure 1-27 Interface of the SSH client software



2. Log in to the AC.

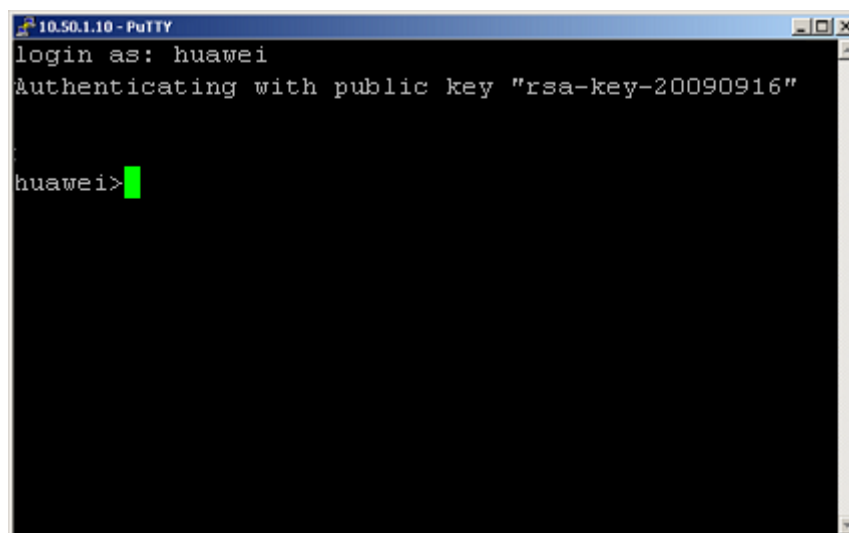
Click **Session**, enter the IP address of the AC in the **Host Name (or IP address)** text box, as shown in [Figure 1-28](#). Then click **Open** to log in to the AC.

Figure 1-28 Interface for logging in to the AC through the SSH client software



The user authentication mode is set to RSA authentication; therefore, the system displays the following message, as shown in **Figure 1-29**. Enter the user name to log in to the AC (here, the user name is **huawei**).

Figure 1-29 Interface for logging in to the AC through the SSH client software



----End

Result

After logging in to the AC, you can maintain and manage the AC.

1.3 Basic Configurations

This section describes the basic configurations, including modification of the system name and configuration of the system time and system user.

1.3.1 Changing the System Name

You can change the system name to differentiate ACs, facilitating AC management.

Context

- The default system name is WAC.
- The modification takes effect immediately.
- After the system name is modified, the command prompt changes to the new name accordingly.

Procedure

Step 1 In privilege mode, run the **sysname** command to change the system name.

----End

Result

The command prompt changes to the configured system name after the **sysname** command is executed.

Example

```
Name the first AC at Shenzhen office in China SZ_WS6603_1.  
WAC (config) #sysname SZ_WS6603_1  
SZ_WS6603_1 (config) #
```

1.3.2 Setting the System Time

This section describes how to configure the system time, time zone, timestamp, Network Time Protocol (NTP), and start time and end time of the daylight saving time (DST).

Procedure

Step 1 Set the system time.

Run the **display time** command to view the current system time. If the system time is the same as the local time, you do not need to change the system time. If the system time is different from the local time, run the **time** command to change the system time.

Step 2 Configure the system time zone.

Run the **display timezone** command to view the current system time zone. If the system time zone is the same as the local time zone, you do not need to change the system time zone. If the system time zone is different from the local time zone, run the **timezone** command to change the system time zone.

 **NOTE**

- The system time zone includes the eastern time zone and western time zone. GMT+ refers to the eastern time zone in which the local time is earlier than the Coordinated Universal Time (UTC). GMT- refers to the western time zone in which the local time is later than the UTC.
- By default, the system time zone is GMT+8:00.

Step 3 Configure the timestamp.

Run the **display time time-stamp** command to view the timestamp between the NMS and the NE, the displayed time format of the SNMP interface. If the timestamp is the same as the data plan, you do not need to change the timestamp. If the timestamp is different from the data plan, run the **time time-stamp** command to change the timestamp.

 **NOTE**

The time of the SNMP interface between the NMS and the NE uses the UTC format or the NE local time format. By default, the SNMP interface uses the NE local time format.

Step 4 Configure NTP to synchronize the clocks of all the devices on a network.

- (Optional) Run the **ntp-service refclock-master** command to configure the NTP master clock.
- Run the **ntp-service unicast-server** command to configure the NTP unicast server mode, and specify the IP address of the remote server that functions as the local timer server and the interface for transmitting and receiving NTP packets.

 **NOTE**

- NTP supports four operating modes: client/server mode, peer mode, broadcast mode, and multicast mode. Here, the client/server mode is used as an example. To configure other operating modes, see [2.1 Configuring the Network Time](#).
- Layer 3 interfaces must be configured on the client and the server and must be allocated must have IP addresses.
- In client/server mode, you only need to configure the client and configure the NTP master clock on the server.
- In client/server mode, the client can synchronize with the server, but the server cannot synchronize with the client.
- The clock stratum of the client must be lower than that of the server. Otherwise, clock synchronization fails.
- A device running NTP can be synchronized with other clock sources or function as a clock source to synchronize other clock sources. When a device works in client mode, you do not need to set the system time because the device synchronizes with the remote server.

Step 5 Configure the DST start time and end time.

Run the **display time dst** command to view the DST start time and end time. If the DST start time and end time are the same as actual values, you do not need to change the DST start time and end time. If the DST start time and end time are different from actual values, run the **time dst** command to change the DST start time and end time.

----End

Result

The system time, time zone, timestamp, NTP configuration, and DST start time and end time are the same as actual settings.

Example

Configure the time of the SNMP interface between the NMS and the NE to use the UTC format.

```
huawei#display time time-stamp
Current time-stamp is: local time //The timestamp before change is the local NE
time.

huawei#time time-stamp
{ local<K>|utc<K> }:utc

Command:
time time-stamp utc

huawei#display time time-stamp
Current time-stamp is: UTC(Coordinated Universal Time) //The timestamp after
change is the UTC time.
```

AC_A uses GMT+7:00 and sends a clock synchronization request packet to NTP server AC_B through VLANIF 2. The IP address of AC_B is 10.20.20.20/24 and AC_B works on clock stratum 4. Set the DST start time to 00:00:00 in May 1, end time to 00:00:00 in September 30, and adjust time to 01:00:00. (For example, if the local time is 05:00:00, the time changes to 06:00:00 after the modification takes effect.)

```
huawei(config)#timezone GMT+ 7:00
huawei(config)#ntp-service refclock-master 4
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 1:00
```

AC_A uses GMT-4:00 and the local time. The current time is 2010-01-01 12:10:10. Set the DST start time to 00:00:00 in May 1, end time to 00:00:00 in September 30, and adjust time to 02:00:00. (For example, if the local time is 05:00:00, the time changes to 07:00:00 after the modification takes effect.)

```
huawei(config)#timezone GMT- 4:00
huawei(config)#time 2010-01-01 12:10:10
huawei(config)#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 2:00
```

1.3.3 Configuring a System User

This section describes how to add a system user and modify user attributes of a system user.

Adding a System User

This section describes how to add system users of different attributes for logging in to, configuring, and managing the AC. This facilitates management of the AC.

Prerequisites

You must have the administrator's authority or higher.

Context

- The super user and the administrator have the authority to add a user at a lower level:
 - A super user can add an administrator, an operator, or a common user.
 - An administrator can add only an operator or a common user.
- The user name must be unique, and cannot be **all** or **online**.
- The super user and the administrator can add multiple users consecutively. Up to 127 (total 128 including the root user) users can be added to the system.
- The system supports up to 10 concurrent online terminal users.

When adding a user, you must configure user attributes, including the user account, password, profile, authority, maximum number of login times, and appended information. **Table 1-6** lists the user attributes.

Table 1-6 User attributes

User Attribute	Description
Account	An account is also called a user name and consists of 6-15 characters. The user name is unique in the system. It cannot contain any space and is case insensitive.
Password	A password consists of 6-15 characters. It must contain at least one digit and one letter, and is case sensitive.
User profile	A user profile name consists of 1-15 characters. A user profile specifies the validity period of the user name, validity period of the password, login time, and logout time.
Authority	<p>Users are classified into four levels: common user, operator, administrator, and super user. The user at one level can add only the user at a lower level. The following lists the authority of all users:</p> <ul style="list-style-type: none"> ● Common users can perform basic system operations and query operations. ● Operators can configure the AC and services. ● Administrator and super users have the following similarities and differences: <ul style="list-style-type: none"> - Similarities: <ul style="list-style-type: none"> - Perform all configurations. - Maintain and manage the AC, user account, and user authority. - Differences: <ul style="list-style-type: none"> - Only one super user exists in the system, whereas multiple administrators can coexist in the system. - The super user can add an administrator, but an administrator has no authority to add the super user.
Maximum number of login times	This parameter determines whether a user name can be used to log in to the system from several terminals simultaneously. The value ranges from 0 to 4, and is generally set to 1.
Appended information	Appended information is additional information about the user. It is a string of 0-30 characters. It can be the telephone number or the address of a user.

Procedure

Step 1 Run the **terminal user name** command to add a user in accordance with the data plan.

Step 2 Run the **display terminal user** command to check the user information.

---End

Result

The displayed user information is the same as the actual data plan.

Example

With the administrator authority, add a common user with the account as **huawei**, password as **test01**, user profile as the default root user profile, user level as **Common User**, maximum number of login times as 3, and appended information as user.

```
huawei(config)#terminal user name
  User Name(length<6,15>):huawei
  User Password(length<6,15>):test01//It is not displayed on the maintenance
terminal.
  Confirm Password(length<6,15>):test01//It is not displayed on the maintenance
terminal.
  User profile name(<=15 chars)[root]:
  User's Level:
    1. Common User  2. Operator:1
  Permitted Reenter Number(0--4):3
  User's Appended Info(<=30 chars):user
  Adding user succeeds
  Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#display terminal user name huawei
```

Name	Level	Status	Reenter Num	Profile	Append Info
huawei	User	Offline	3	root	user

Modifying System User Attributes

This section describes how to modify attributes of a system user, including the password, user profile, authority, number of times a user can log in, and appended information if user attributes are not consistent with the current data plan.

Prerequisites

Users have corresponding authorities. See [Table 1-7](#).

Context

[Table 1-7](#) lists the user attributes that can be modified and restrictions.

Table 1-7 User attributes and restrictions

User Attribute	Restriction
Password	<ul style="list-style-type: none"> ● The super user and the administrator can change their own passwords and passwords of users at lower levels. When changing the password of a user at a lower level, the super user and the administrator do not need to enter the old password. ● The common user and the operator can change only their own passwords, and they must enter their old passwords when changing passwords.
User profile	<ul style="list-style-type: none"> ● The super user and the administrator can modify the profiles bound to them and the profiles bound to users at lower levels. ● The user name and the password must meet specifications described in the user profile. Otherwise, the profile cannot be bound.
Authority	The super user and the administrator can modify the authority of users at lower levels, and they can modify the user authority only to a level lower than them.
Maximum number of login times	<ul style="list-style-type: none"> ● The super user and the administrator can change this attribute for a user at a lower level. ● The maximum number of login times for a super user cannot be changed.
Appended information	<ul style="list-style-type: none"> ● The super user and the administrator can modify their own appended information and the appended information about users at lower levels. ● The common user and the operator can modify only their own appended information.

Procedure

Step 1 Modify system user attributes.

 **NOTE**

Before modifying user attributes, run the **display terminal user** command to view the existing user attributes.

- Run the **terminal user password** command to change the password of a user.
The password of a user consists of 6-15 case-sensitive characters. It must contain at least one digit and one letter.
- Run the **terminal user user-profile** command to modify the profile bound to a user.
- Run the **terminal user level** command to modify the authority of a user.
- Run the **terminal user reenter** command to change the maximum number of login times.
- Run the **terminal user apdinfo** command to modify the appended information about a user.

When the system encounters a fault, you can contact the user by querying the appended information. The information such as contact method and address is recommended.

Step 2 Check the user information.

Run the **display terminal user** command to check the user information.

---End

Result

The modified user information is correct, and you can log in to the AC using the original user name and password.

Example

Modify the attributes of user **huawei**: change the password to **test02**, user profile to operator profile, user level to operator, maximum number of login times to 4, and appended information to operator.

```
huawei(config)#terminal user password
User Name(<=15 chars):huawei
New Password(length<6,15>):test02//It is not displayed on the console.
Confirm Password(length<6,15>):test02//It is not displayed on the console.
Information takes effect
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#terminal user user-profile
User Name(<=15 chars):huawei
Permitted user-profile[root]:operator
Confirm user-profile:operator
Configuration will take effect when the user logs on next time.
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#terminal user level
User Name(<=15 chars):huawei
1. Common User 2. Operator:
User's Level:2
Confirm Level:2
Information will take effect when this user logs on next time
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#terminal user reenter
User Name(<=15 chars):huawei
Permitted Reenter Number(0--4):4
Confirm Reenter Number(0--4):4
Information will take effect when this user logs on next time
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#terminal user apdinfo
User Name(<=15 chars):huawei
User's Appended Info(<=30 chars):operator
Information takes effect
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#display terminal user name huawei
-----
Name           Level   Status  Reenter Profile  Append
              Num
-----
huawei         Operator Offline  4 operator  operator
-----
```

1.3.4 Configuring a Port

This section describes how to configure description and attributes for a port.

Configuring Port Description

This section describes how to configure the description for a port on an AC.

Context

Port description facilitates information query during system maintenance.

Procedure

- Step 1** In global config mode, run the **port desc** command to configure the description for a port. The description is a character string and identifies a port on a board in a subrack.
- Step 2** Run the **display port desc** command to view the port description.

----End

Example

Plan the format of user port description as "community ID-building ID-floor ID/subrack ID-slot ID-port ID". "Community ID-building ID-floor ID" indicates the location where the AP is deployed, and "shelf ID-slot ID-port ID" indicates the physical port on the local device that connects to the AP. This plan shows the AP location and the connection between the AP and the AC, which facilitates query in maintenance. Assume that the AP connected to port 0/2/0 on the AC is deployed in floor 1, building 01 of community A. Configure the description for port 0/2/0 according to the plan.

```
huawei (config) #port desc 0/2/0 description A-01-01/0-2-0
huawei (config) #display port desc 0/2/0
```

```
-----
F/ S/ P   IMA Group   Port Description
-----
0/ 2/ 0   -           A-01-01/0-2-0
-----
```

Configuring Port Attributes

This section describes how to configure the attributes for a specified port on an AC so that the AC can communicate with APs, switches, or upper-layer devices.

Context

The AC connects to APs, switches, or upper-layer devices through ports. Therefore, port attributes of two connected devices must match each other.

Default Settings

Table 1-8 lists the default attribute settings of an AC port.

Table 1-8 Default attribute settings of an AC port

Item	Default Setting (Optical Port)	Default Setting (Electrical Port)
Auto-negotiation mode	Auto-negotiation	Auto-negotiation
Port rate	<ul style="list-style-type: none">● GE optical port: 1000 Mbit/s● 10GE optical port: 10000 Mbit/s	N/A NOTE After auto-negotiation is disabled on the port, you can set the port rate.
Duplex mode	Full-duplex	N/A NOTE After auto-negotiation is disabled on the port, you can configure the duplex mode.
Network adaptation type	Not supported	Supported
Flow control	Disabled	Disabled

Procedure

- Configure physical attributes of an Ethernet port.
 1. (Optional) Set the auto-negotiation mode of the Ethernet port.

Run the **auto-neg** command to enable or disable auto-negotiation:

 - After auto-negotiation is enabled, the port automatically negotiates with the interconnected port for the rate and operating mode.
 - After auto-negotiation is disabled, the port uses the default or configured rate and operating mode.
 2. (Optional) Set the rate of the Ethernet port.

Run the **speed** command to set the rate of the Ethernet port. After the port rate is set successfully, the port works at the configured rate. When setting the rate of an Ethernet port, pay attention to the following points:

 - The ports of two interconnected devices use the same rate. This prevents a communication failure.
 - Auto-negotiation must be disabled.
 3. (Optional) Set the duplex mode of the Ethernet port.

Run the **duplex** command to set the duplex mode of the Ethernet port. An Ethernet port works in full duplex, half duplex, or auto-negotiation mode. When setting the duplex mode of the Ethernet port, pay attention to the following points:

 - Ensure that the ports of two interconnected devices work in the same duplex mode. This prevents a communication failure.
 - Auto-negotiation must be disabled.
 4. (Optional) Configure the network adaptation type of the Ethernet port.

Run the **mdi** command to configure the network adaptation type of the Ethernet port so that the Ethernet port adapts to the actual network cable type. The network adaptation types are as follows:

- **normal**: indicates that the network cable connected to the Ethernet port must be a straight-through cable.
- **across**: indicates that the network cable connected to the Ethernet port must be a crossover cable.
- **auto**: indicates that the Ethernet port automatically identifies the network cable type. The Ethernet port can connect to a straight-through cable or a crossover cable.

- Configure flow control on the port.

Run the **flow-control** command to enable flow control on the port. When traffic on a port is heavy, run this command to prevent network congestion and packet loss. Both the local and remote devices must support flow control. When configuring flow control on the port, pay attention to the following points:

- If the peer device supports flow control, enable flow control on the local device.
- If the peer device does not support flow control, disable flow control on the local device.

By default, flow control is disabled.

- Configure mirroring on the Ethernet port.

When the system is faulty, run the **mirror port** command to copy the traffic on an affected port to another port. Port mirroring is used for traffic observation, network fault diagnosis, and data analysis.

----End

Example

Configure Ethernet port 0/2/0 (an electrical port) to work at a rate of 1000 Mbit/s in full duplex mode, and enable flow control and disable auto-negotiation for Ethernet port 0/2/0.

```
huawei(config)#interface scu 0/2
huawei(config-if-scu-0/2)#auto-neg 0 disable
huawei(config-if-scu-0/2)#speed 0 1000
huawei(config-if-scu-0/2)#duplex 0 full
huawei(config-if-scu-0/2)#flow-control 0
```

1.4 Configuring the License Function

The license platform provides the registration mechanism for the AC. During system initialization, the AC needs to register controlled resource entries or function entries.

Prerequisites

The license file has been obtained. For details on how to obtain the license file, see the *Commercial License Delivery Process*.

 **NOTE**

When obtaining the license file, learn about the ESN of the AC. You can run the **display license** command to view the ESN of the AC.

Context



CAUTION

- The license function is enabled on the WS6603 by default.
 - If the license file is not loaded or the license file is incorrect, the system enters the trial period. The default trial period is 30 days.
 - In the trial period, the AC supports a maximum number of 1024 online APs. If the AC is not loaded with the correct license file after the trial period expires, the system allows the first registered five APs to go online and disconnects other APs.
 - After the AC is loaded with the correct license file, the maximum number of APs depends on the license file.
-

Procedure

Step 1 Run the **load license** command to load the license file of the AC.

After the license file is successfully loaded, the AC determines the allowed number of online APs according to the loaded license file.

Step 2 Run the **display license** command to view information about the loaded license file.

---End

Example

Load the license file to the AC through TFTP with the SN of LIC2010032900A800 and the ESN of B5EA73AB92469D177B0EE92C4F56FDF78B357BFC.

```
WAC(config)#display license
License function is disabled

Active main board license protocol version:1.2
Active main board LIB version:1.2.038
Active main board license serial No.:...//There is no license file at this time.
Active main board ESN:B5EA73AB92469D177B0EE92C4F56FDF78B357BFC...//ESN
information
huawei(config)#load license tftp 10.11.104.2 license
huawei(config)#display license
License function is enabled

Active main board license protocol version:1.2
Active main board LIB version:1.2.038
Active main board license serial No.:LIC2010032900A800...//The license file is
loaded.
Active main board ESN:B5EA73AB92469D177B0EE92C4F56FDF78B357BFC
```

1.5 Saving and Backing Up Data

The AC supports data saving and backup to prevent data loss in case of an upgrade failure or any other critical events.

1.5.1 Configuring the File Transfer Mode

This section describes how to configure the FTP, SFTP, TFTP, and Xmodem transfer mode.

Configuring the FTP File Transfer Mode

This section describes how to configure the FTP file transfer mode to enable an AC to upload files to or download files from an FTP server through the inband or outband network management port.

Prerequisites

- The Ethernet port on the FTP server is directly connected to the inband or outband management network port on the AC with a network cable.
 - Use a crossover cable if the inband network management port (uplink port) is used.
 - Use a straight-through cable if the outbound management port (maintenance network port) is used.
- You have logged in to the AC from the maintenance terminal using Telnet and entered the global config mode.

Tools, Meters, and Materials

Crossover cable or straight-through cable

Impact on the System

None.

Precautions

When the FTP server is directly connected to the AC, a crossover cable must be used. In other cases, a straight-through cable is required.

Procedure

Step 1 Configure the IP address of the Ethernet port on the FTP server.

Configure the IP address of the Ethernet port on the FTP server according to the data plan. Ensure that the Ethernet port on the FTP server and the inband or outband network management port on the AC can ping each other successfully.

For example, if the Ethernet port on the FTP server is directly connected to the AC, the IP address of this Ethernet port and the IP address of the inband or outband network management port on the AC must be on the same network segment.

Step 2 Run the FTP application on the FTP server and set relevant parameters.

Run the FTP application and set the path for saving files, FTP user name, and password.

Step 3 Run the **ftp set** command on the AC to set the FTP user name and password. (Perform this step when you need to transfer files manually.)

```
huawei(config)#ftp set
User Name(<=40 chars):huawei
User Password(<=40 chars):huawei//It is hidden.
```

 **NOTE**

The default FTP user name is **anonymous**, and the default password is **anonymous@huawei.com**.

Step 4 (Optional) Run the **file-server auto-backup data** command to enable the AC to back up the database file and set the FTP user name, password, and port number.

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 ftp path test user
User Name(<=40 chars):huawei
User Password(<=40 chars):huawei//It is hidden.
```

----End

Reference

- Any PC that runs the FTP software can function as an FTP server.
- The user name and password must be verified during file transfer through the FTP protocol. The same user name and password must be configured on both the FTP server and the FTP client (such as the AC).

Configuring the SFTP File Transfer Mode

This section describes how to configure the SFTP file transfer mode to enable an AC to upload files to or download files from an SFTP server through the inband or outband network management port.

Prerequisites

- The Ethernet port on the SFTP server is directly connected to the inband or outband management network port on the AC with a network cable.
 - Use a crossover cable if the inband network management port (uplink port) is used.
 - Use a straight-through cable if the outbound management port (maintenance network port) is used.
- You have logged in to the AC from the maintenance terminal using Telnet and entered the global config mode.

Tools, Meters, and Materials

Crossover cable or straight-through cable

Impact on the System

None.

Precautions

When the SFTP server is directly connected to the AC, a crossover cable must be used. In other cases, a straight-through cable is required.

Procedure

Step 1 Configure the IP address of the Ethernet port on the SFTP server.

Configure the IP address of the Ethernet port on the SFTP server according to the data plan. Ensure that the Ethernet port on the SFTP server and the inband or outband network management port on the AC can ping each other successfully.

For example, if the Ethernet port on the SFTP server is directly connected to the AC, the IP address of this Ethernet port and the IP address of the inband or outband network management port on the AC must be on the same network segment.

Step 2 Run the SFTP application on the SFTP server and set relevant parameters.

Run the SFTP application and set the path for saving files, SFTP user name, password, and port number. The default port number is 22.

Step 3 Run the **ssh sftp set** command on the AC to set the SFTP user name, password, and port number. (Perform this step when you need to transfer files manually.)

```
huawei(config)#ssh sftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//It is hidden.
  Listening Port(0--65535):22
```

Step 4 (Optional) Run the **file-server auto-backup data** command to enable the AC to back up the database file and set the SFTP user name, password, and port number.

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 sftp path test port
22 user
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//It is hidden.
```

 **NOTE**

The AC does not have a default SFTP user name, password, or port number.

----End

Reference

- Any PC that runs the SFTP software can function as an SFTP server.
- The user name and password must be verified during file transfer through the SFTP protocol. The same user name, password, and port number must be configured on both the SFTP server and the SFTP client (such as the AC).

Configuring the TFTP File Transfer Mode

This section describes how to configure the TFTP file transfer mode to enable an AC to upload files to or download files from an TFTP server through the inband or outband network management port.

Prerequisites

- The Ethernet port on the TFTP server is directly connected to the inband or outband management network port on the AC with a network cable.
 - Use a crossover cable if the inband network management port (uplink port) is used.
 - Use a straight-through cable if the outbound management port (maintenance network port) is used.
- You have logged in to the AC from the maintenance terminal using Telnet and entered the global config mode.

Tools, Meters, and Materials

Crossover cable or straight-through cable

Impact on the System

None.

Precautions

When the TFTP server is directly connected to the AC, a crossover cable must be used. In other cases, a straight-through cable is required.

Procedure

Step 1 Configure the IP address of the Ethernet port on the TFTP server.

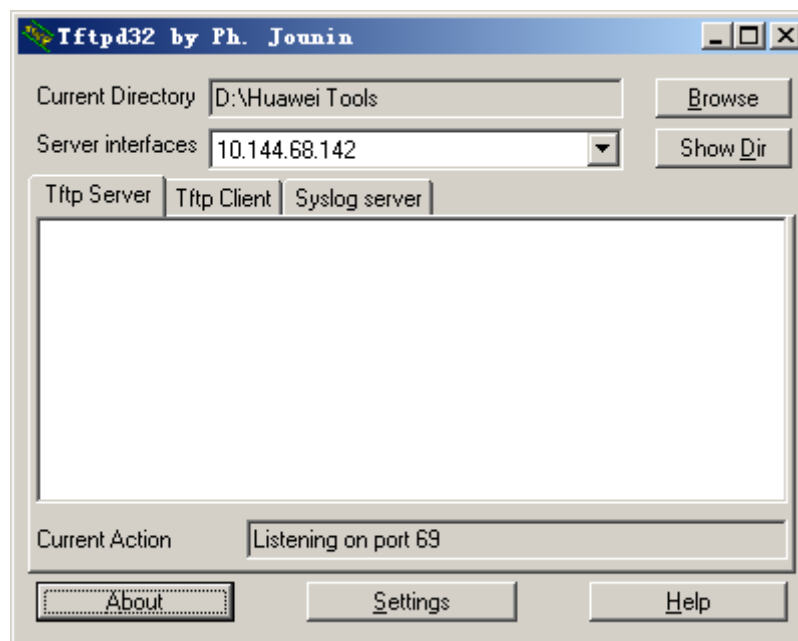
Configure the IP address of the Ethernet port on the TFTP server according to the data plan. Ensure that the Ethernet port on the TFTP server and the inband or outband network management port on the AC can ping each other successfully.

For example, if the Ethernet port on the TFTP server is directly connected to the AC, the IP address of this Ethernet port and the IP address of the inband or outband network management port on the AC must be on the same network segment.

Step 2 Run the TFTP application on the TFTP server and set relevant parameters.

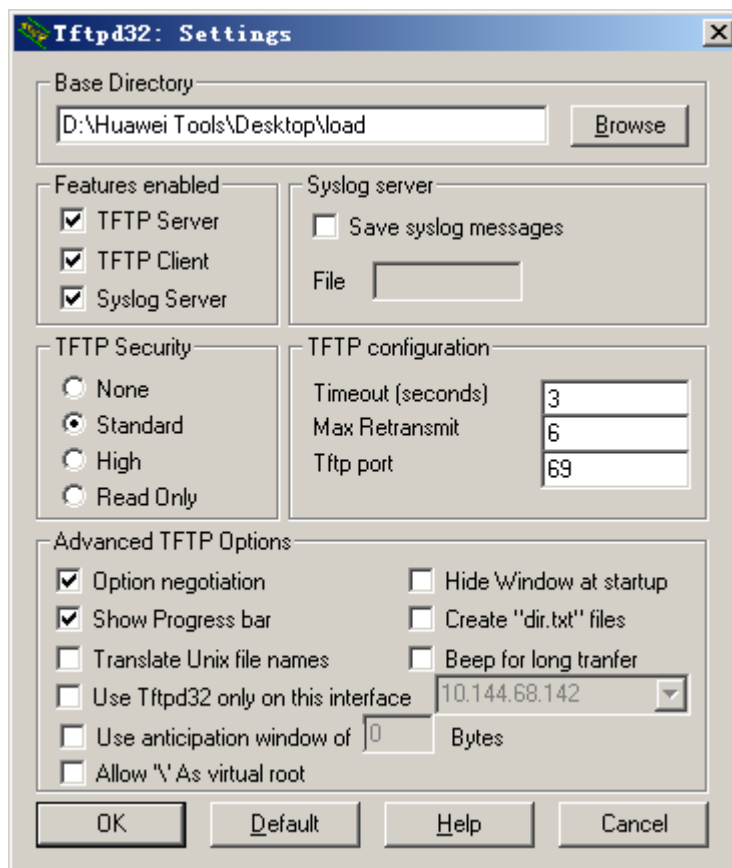
1. When the TFTP application is running on the TFTP server, the page as shown in [Figure 1-30](#) is displayed. Select the IP address configured in step 1 from the **Server interfaces** drop-down list box.

Figure 1-30 TFTP page



2. On the page as shown in [Figure 1-30](#), click **Settings**.
3. In the dialog box that is displayed, click **Browse** to select a path for saving the program file to be loaded, as shown in [Figure 1-31](#).

Figure 1-31 TFTP parameter setting page



----End

Reference

- Any PC that runs the TFTP software can function as a TFTP server.
- The IP address selected from the **Server interfaces** drop-down list box is the IP address of the TFTP server. The TFTP application can identify the IP address. If the TFTP server has multiple IP addresses, select the correct one.
- If file transfer through TFTP fails, check whether the following conditions are satisfied:
 - The entered IP address of the TFTP server is correct.
 - The TFTP server can ping the IP address of the inband or outbound network management port of the AC.
 - The TFTP application is running properly on the TFTP server.
 - The directory configured in the TFTP application is correct.
 - The TFTP transfer function has been enabled through the CLI.
 - The entered file name is correct.

Configuring the Xmodem File Transfer Mode

This section describes how to configure the Xmodem file transfer mode to enable an AC to upload files to or download files from a maintenance terminal through the serial port on the AC.

Prerequisites

You have logged in to the AC from the maintenance terminal through the serial port and entered the global config mode.

Tools, Meters, and Materials

RS232 serial port

Impact on the System

None.

Precautions



CAUTION

The speed of Xmodem file transfer through the serial port is slow; therefore, the FTP file transfer mode is recommended.

-
- The baud rate of the serial port on the AC must be the same as that of the serial port on the maintenance terminal.
 - Only the master main control board can use the Xmodem file transfer mode.
 - Users that log in to the AC through Telnet are not allowed to transfer files in Xmodem mode.

Procedure

Step 1 Check the baud rate on the AC.

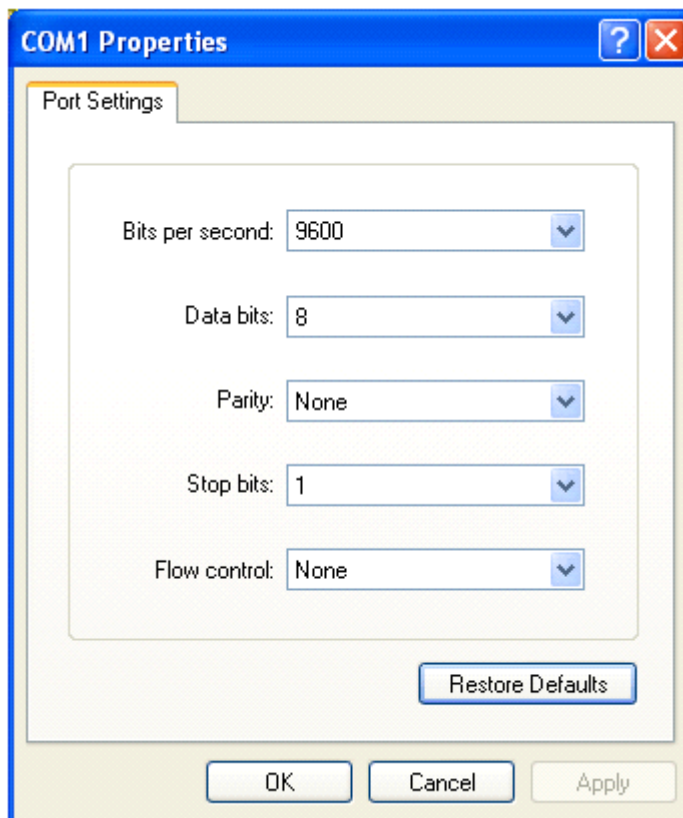
```
huawei(config)#display baudrate
Current active serial baudrate: 9600 bps
```

Step 2 (Optional) Run the **baudrate** command to set the baud rate of the serial port on the AC. A high baud rate improves the transfer speed.

This example assumes that the baud rate of the serial port on the maintenance terminal is 9600 bit/s and the baud rate of the serial port on the AC is 4800 bit/s. Run the following command on the AC:

```
huawei(config)#baudrate 9600
```

Step 3 Start the HyperTerminal on the maintenance terminal and set the baud rate of the serial port to be the same as that of the AC.



---End

1.5.2 Saving and Backing Up Data Manually

This section describes how to manually save data in the flash memory or server to prevent data loss because of emergency restart.

Saving Data Manually

This section describes how to save data manually.

Context

The database file and the configuration file must be saved. [Table 1-9](#) lists the commands used to save data and describes functions of the commands. The database file saves the configuration data in binary format and the configuration file saves the configuration data in command line format. [Table 1-9](#) lists the commands used to save data.

Table 1-9 Commands used to save data

Command	Function
save data	Saves only the database file.
save configuration	Saves only the configuration file.

Command	Function
save	Saves the database file and the configuration file.

Procedure

Step 1 Run one of the preceding commands to save data.

---End

Result

The system displays a message indicating that the database file and the configuration file have been saved successfully.

Example

- Save the database file.

```
huawei(config)#save data
The data is being saved, please wait a moment...

huawei(config)#
1 [2010-07-12 14:32:00+08:00]:The percentage of saved data on 6 slot's main
control board is: 21%

huawei(config)#
1 [2010-07-12 14:32:03+08:00]:The percentage of saved data on 6 slot's main
control board is: 27%

huawei(config)#
1 [2010-07-12 14:32:06+08:00]:The percentage of saved data on 6 slot's main
control board is: 66%

huawei(config)#
1 [2010-07-12 14:32:09+08:00]:The percentage of saved data on 6 slot's main
control board is: 72%

huawei(config)#
1 [2010-07-12 14:32:12+08:00]:The percentage of saved data on 6 slot's main
control board is: 96%

huawei(config)#
1 [2010-07-12 14:32:15+08:00]:The percentage of saved data on 6 slot's main
control board is: 98%

huawei(config)#
1 [2010-07-12 14:32:18+08:00]:The percentage of saved data on 6 slot's main
control board is: 98%

huawei(config)#

huawei(config)#
1 [2010-07-12 14:32:19+08:00]:The data of 6 slot's main control board is
saved
completely
```

- Save the configuration file.

```
huawei#save configuration

huawei#
It will take several minutes to save configuration file, please wait...
```

```
huawei#  
Configuration file had been saved successfully  
Note: The configuration file will take effect after being activated
```

- Save the current database file and configuration file.

```
WS6803(config)#save  
{ <cr>|configuration<K>|data<K> }:  
  
Command:  
save  
  
huawei(config)#  
It will take several minutes to save configuration file, please wait...  
  
huawei(config)#  
Configuration file had been saved successfully  
Note: The configuration file will take effect after being activated  
  
huawei(config)#  
The data is being saved, please wait a moment...  
  
huawei(config)#  
1 [2010-07-12 14:35:05+08:00]:The percentage of saved data on 6 slot's main  
control board is: 21%  
  
huawei(config)#  
1 [2010-07-12 14:35:08+08:00]:The percentage of saved data on 6 slot's main  
control board is: 27%  
  
huawei(config)#  
1 [2010-07-12 14:35:11+08:00]:The percentage of saved data on 6 slot's main  
control board is: 66%  
  
huawei(config)#  
1 [2010-07-12 14:35:14+08:00]:The percentage of saved data on 6 slot's main  
control board is: 72%  
  
huawei(config)#  
1 [2010-07-12 14:35:17+08:00]:The percentage of saved data on 6 slot's main  
control board is: 78%  
  
huawei(config)#  
1 [2010-07-12 14:35:20+08:00]:The percentage of saved data on 6 slot's main  
control board is: 96%  
  
huawei(config)#  
1 [2010-07-12 14:35:23+08:00]:The percentage of saved data on 6 slot's main  
control board is: 98%  
  
huawei(config)#  
  
huawei(config)#  
1 [2010-07-12 14:35:25+08:00]:The data of 6 slot's main control board is  
saved  
completely
```

Backing Up Data Manually

This section describes how to back up data manually.

Prerequisites

The data has been saved. For details, see [Saving Data Manually](#).

Context

The database file and the configuration file must be backed up. [Table 1-10](#) lists the commands used to back up data and describes functions of the commands.

Table 1-10 Commands used to back up data

Command	Function
back data	Manually backs up the database file to the backup server. The IP address of the backup server must be the same as the IP address configured in FTP, SFTP, or TFTP application.
backup configuration	Manually backs up the configuration file to the backup server. The IP address of the backup server must be the same as the IP address configured in FTP, SFTP, or TFTP application.

Procedure

Step 1 Run one of the preceding commands to back up data.

----End

Result

The files have been backed up in a specified path.

Example

1. Configure the FTP server and start the FTP application on the backup server. For details, see [Configuring the FTP File Transfer Mode](#).
2. Back up the database file or configuration file to the backup server.

- Specify the IP address of the backup server as 10.10.10.1 and the database file name as **data0.dat**, and back up the database file to the backup server through FTP.

```
huawei(config)#backup data ftp 10.10.10.1 data0.dat
Please save database file before backup, or the database file that is
backed
up may be not the latest one. Are you sure to continue? (y/n)[n]:
y
```

```
Load(backup,duplicate,...) begins, please wait and notice the rate of
progress
```

```
Any operation such as reboot or switchover will cause failure
and
unpredictable result
```

- Assume that the IP address of the backup server is 10.10.10.1 and the configuration file name is **config0.txt**. To back up the configuration file to the backup server through FTP, perform the following operations:

```
huawei(config)#backup configuration ftp 10.10.10.1 config0.txt
Please save configuration file before backup, or the configuration
file
```



```

backupid may be not the latest. Are you sure to continue? (y/n)[n]:
y
Load(backup,duplicate,...) begins, please wait and notice the rate of
progress
Any operation such as reboot or switchover will cause failure
and
unpredictable result
    
```

1.5.3 Saving and Backing Up Data Automatically

This section describes how to configure the WS6603 to save data in the flash memory or server to prevent data loss because of emergency restart.

Saving Data Automatically

When the auto-save function is enabled, the WS6603 periodically checks whether the configuration data is modified at the preset intervals. If the configuration data has been modified, the WS6603 saves the modified data. If the configuration data is not modified, the WS6603 uses the original configuration.

Context

The database file and the configuration file must be saved. [Table 1-11](#) lists the commands used to save data and describes functions of the commands.

Table 1-11 Commands used to save data

Command	Function
autosave type { all configuration data }	Sets the auto-save file type. The parameters are described as follows: <ul style="list-style-type: none"> ● data: indicates the database file. ● configuration: indicates the configuration file. ● all: indicates the database file and the configuration file.
autosave time	Saves the database file automatically at the specified time. By default, the WS6603 saves the database file at 00:00:00 every day.
autosave interval	Saves the database file automatically at intervals. By default, the WS6603 saves the database file every 30 minutes.

 **NOTE**

- By default, the auto-save function is disabled. You need to back up data manually.
- When the auto-save function is enabled, you can still save data manually. For details, see [Saving Data Manually](#).



CAUTION

If the database file is saved frequently, the system performance deteriorates. Therefore, it is recommended that you set the auto-save interval to be longer than or equal to one day.

Procedure

Step 1 Run one of the preceding commands to save data.

----End

Result

Run the **display autosave configuration** command to check the specified time or interval.

Example

1. Configure the type of data to be saved.

```
Huawei(config)#autosave  
type  
{ all<K>|configuration<K>|  
data<K> }:all
```

Command:

```
autosave type all
```

2. Configure the WS6603 to save the database file at the specified time or at intervals.

- Configure the WS6603 to save the database file at 02:00:00 and enable the auto-save function.

```
huawei(config)#autosave time  
02:00:00  
System autosave time switch:  
off  
Autosave time:  
02:00:00  
Autosave type: data and configuration file
```

```
huawei(config)#autosave time  
on  
System autosave time switch:  
on  
Autosave time:  
02:00:00  
Autosave type: data and configuration file
```

- Configure the WS6603 to save the database file every 1440 minutes and enable the auto-save function. The WS6603 checks whether the configuration data is modified every 1440 minutes. If the configuration data has been modified, the system saves the modified data. If the configuration data is not modified, the WS6603 uses the original configuration.



CAUTION

The **autosave interval** and **autosave time** commands cannot be used together.

```
huawei(config)#autosave interval  
1440
```

```
System autosave interval switch:
off
Autosave interval: 1440
minutes
Autosave type: data and configuration file

huawei(config)#autosave interval
on
System autosave interval switch:
on
Autosave interval: 1440
minutes
Autosave type: data and configuration
file

System autosave modified configuration switch:
on
Autosave interval: 30
minutes
Autosave type: data and configuration file
```

Configuring the Automatic Backup Server

This section describes how to configure the server that is used for automatic backup.

Context

- You can configure primary and secondary backup servers to ensure data reliability or only a primary backup server.
- If you configure primary and secondary backup servers, data is automatically backed up on the secondary server when the active server fails.

Procedure

Step 1 Back up the database file, configuration file, or log file to the server according to actual requirements:

- Back up the database file to the active server (10.10.10.1) and secondary server (10.10.10.1) in FTP mode.

```
huawei(config)#file-server auto-backup data primary 10.10.10.1 ftp user
User Name(<=40 chars):123
User Password(<=40 chars):123
```

```
huawei(config)#file-server auto-backup data secondary 10.10.10.2 ftp user
User Name(<=40 chars):123
User Password(<=40 chars):123
```

- Back up the configuration file to the primary server (10.10.10.1).

```
huawei(config)#file-server auto-backup configuration primary 10.10.10.1 ftp
user
User Name(<=40 chars):123
User Password(<=40 chars):123
```

- Back up the log file to the primary server (10.10.10.1).

```
huawei(config)#file-server auto-backup log primary 10.10.10.1 ftp user
User Name(<=40 chars):123
User Password(<=40 chars):123
```

----End

Follow-up Procedure

- To query the IP addresses of servers that have backed up the database file, run the **display file-server auto-backup data** command.

```
huawei(config)#display file-server auto-backup data
```

```
-----
Server type: Primary
Trans mode : FTP
IP address : 10.10.10.1
User name  : 123
Path       :
-----
```

```
-----
Server type: Secondary
Trans mode : FTP
IP address : 10.10.10.2
User name  : 123
Path       :
-----
```

```
-----
Current Server: Primary server
-----
```

- To query the IP address of server that has backed up the configuration file, run the **display file-server auto-backup configuration** command.

```
huawei(config)#display file-server auto-backup configuration
```

```
-----
Server type: Primary
Trans mode : FTP
IP address : 10.10.10.1
User name  : 123
Path       :
-----
```

```
-----
Current Server: Primary server
-----
```

- To query the IP address of server that has backed up the log file, run the **display file-server auto-backup log** command.

```
huawei(config)#display file-server auto-backup log
```

```
-----
Server type: Primary
Trans mode : FTP
IP address : 10.10.10.1
User name  : 123
Path       :
-----
```

```
-----
Current Server: Primary server
-----
```

Backing Up Data Automatically

This section describes how to configure the WS6603 to back up the system configuration data, database file, or log file.

Prerequisites

- The data has been saved automatically. For details, see [Saving Data Automatically](#).
- The backup server has been configured. For details, see [Configuring the Automatic Backup Server](#).

Context

The database file, configuration file, and log file must be backed up. [Table 1-12](#) lists the commands used to back up data and describes functions of the commands.

Table 1-12 Commands used to back up data

Command	Function
auto-backup manual data	Automatically backs up the database file to the backup server.
<ul style="list-style-type: none">● auto-backup period data interval● auto-backup period data enable	Backs up the database file to the backup server at intervals. You need to configure the auto-backup interval and start time, and enable the auto-backup function.
auto-backup manual configuration	Automatically backs up the configuration file to the backup server.
<ul style="list-style-type: none">● auto-backup period configuration interval● auto-backup period configuration enable	Automatically backs up the configuration file to the backup server at intervals. You need to configure the auto-backup interval and start time, and enable the auto-backup function.
<ul style="list-style-type: none">● auto-backup period log interval● auto-backup period log enable	Backs up the log file automatically. You need to configure the auto-backup interval and start time, and enable the auto-backup function.

Procedure

Step 1 Run one of the preceding commands to back up data.

---End

Result

The backed up files with default names are found in the specified path.

Example

1. Configure the FTP server and start the FTP application on the backup server. For details, see [Configuring the FTP File Transfer Mode](#).
2. Back up the database file, configuration file, or log file to the backup server based on site requirements.
 - Back up the database file to the backup server.
huawei(config)#**auto-backup manual data**
 - Back up the configuration file to the backup server.
huawei(config)#**auto-backup manual configuration**
 - Enable the auto-backup function for the database file, and set the auto-backup interval for the database file to one day and the start time to 02:30:00.
huawei(config)#**auto-backup period data interval 1 time 02:30**
huawei(config)#**auto-backup period data enable**
 - Enable the auto-backup function for the configuration file, and set the auto-backup interval for the configuration file to one day and the start time to 03:30:00.

```
huawei(config)#auto-backup period configuration interval 1 time 03:00  
huawei(config)#auto-backup period configuration enable
```

- Enable the auto-backup function for the log file, and set the auto-backup interval for the log file to one day and the start time to 06:00:00.

```
huawei(config)#auto-backup period log interval 1 time 06:00  
huawei(config)#auto-backup period log enable
```



CAUTION

In step 1, the backup server is an FTP server.

2 Basic Configurations

About This Chapter

Basic configurations mainly include certain common configurations, public configurations, and pre-configurations in service configurations. There is no logical relationship between basic configurations. You can perform basic configurations according to actual requirements.

[2.1 Configuring the Network Time](#)

The Network Time Protocol (NTP) synchronizes all the clocks of devices on a network so that these devices can provide multiple applications (such as the network management system and the network charging system) based on the uniform time.

[2.2 Configuring System Security](#)

This section describes how to configure system security to protect the system against malicious attacks.

[2.3 Configuring an ACL](#)

This section describes access control list (ACL) types and rules.

[2.4 Configuring QoS](#)

This section describes how to configure quality of service (QoS) on the AC.

2.1 Configuring the Network Time

The Network Time Protocol (NTP) synchronizes all the clocks of devices on a network so that these devices can provide multiple applications (such as the network management system and the network charging system) based on the uniform time.

Background

NTP has the following characteristics:

- NTP is defined in RFC 1305 to synchronize the time between distributed time servers and clients. NTP defines architectures, algorithms, entities, and protocols in its implementation.
- NTP evolves from the Time Protocol (TP) and the ICMP Timestamp Message, with special design on accuracy and robustness.
- NTP runs over UDP with the port number of 123.
- A local system running NTP can be synchronized by other clock sources or acts as a clock source to synchronize other clocks.

NTP applies to the scenario where clocks of all hosts or routers on the network must be the same. For example:

- To analyze the log and debugging information collected from different routers, the device needs to use the time as the reference.
- The charging system requires that the clocks of all devices be the same.
- To implement certain functions, such as restarting all routers on the network at the specified time, the clocks of these routers must be the same.
- When multiple systems cooperate with each other to process a complex event, these systems must synchronize their clocks to ensure that they process the event in a correct sequence.
- To implement incremental backup between the backup server and clients, the clocks of the backup server and all clients must be synchronized.

It is impossible for an administrator to modify the system clock on each network device by entering a command because there is a heavy workload and clock precision cannot be ensured. NTP synchronizes all the clocks of devices on a network and ensures high clock precision.

NTP supports four operating modes: client/server mode, peer mode, broadcast mode, and multicast mode. The AC supports all the four operating modes.

Default Settings

Table 2-1 lists the default settings of the network clock.

Table 2-1 Default settings of the network clock

Item	Default Setting
Authentication	Disabled
NTP authentication key	None
Maximum number of NTP connections	100

Item	Default Setting
Clock stratum	16

2.1.1 (Optional) Configuring NTP Authentication

This section describes how to configure NTP authentication to improve network security and prevent unauthorized users from modifying the clock.

Prerequisites

The network interface and the routing protocol of the AC have been configured so that an NTP server and a client can communicate with each other at the network layer.

Background

On NTP-enabled networks demanding high security, NTP authentication is required. NTP authentication must be separately configured on the client and the server.

Precautions

- If NTP authentication is disabled on a client, the client can synchronize with the server, regardless of whether NTP authentication is enabled on the server.
- If NTP authentication is enabled, configure a key and declare the key as reliable.
- The NTP configuration of the server must be the same as that of the client.
- When NTP authentication is enabled on the client, the client can be authenticated as long as the server is configured with the same key as the client. In this case, you do not need to enable NTP authentication on the server or declare the key as reliable.
- The client synchronizes with only the server that provides the reliable key. If the key provided by the server is unreliable, the client does not synchronize with the server.

Procedure

- Step 1** Run the **ntp-service authentication enable** command to enable NTP authentication.
- Step 2** Run the **ntp-service authentication-keyid** command to configure an NTP authentication key.
- Step 3** Run the **ntp-service reliable authentication-keyid** command to declare the key as reliable.

----End

Example

Enable NTP authentication, set the NTP authentication key to **aNiceKey** with the key number of 42, and declare key 42 as a reliable key.

```
huawei (config) #ntp-service authentication enable
huawei (config) #ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
huawei (config) #ntp-service reliable authentication-keyid 42
```

2.1.2 Configuring the NTP Broadcast Mode

This section describes how to configure the AC to synchronize the clock in NTP broadcast mode. After the configuration is complete, the server periodically broadcasts clock synchronization packets through a specified port, and the client synchronizes the local clock according to the received broadcast packets.

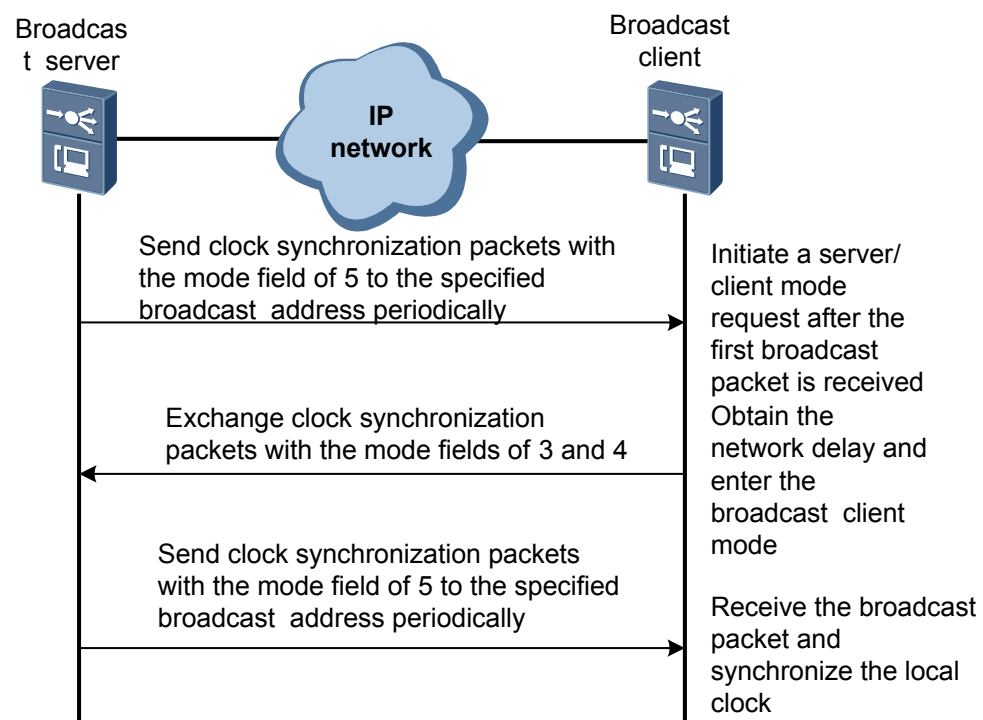
Prerequisites

The network interface and the routing protocol of the AC have been configured so that the server and the client can communicate at the network layer.

Context

In broadcast mode, the server periodically sends clock synchronization packets to the broadcast address 255.255.255.255, with the mode field set to 5 (indicating the broadcast mode). The client listens to the broadcast packets sent from the server. After receiving the first broadcast packet, the client exchanges NTP packets with the server to obtain a network delay between the client and the server. The client then enters the broadcast client mode and synchronizes the local clock according to the incoming broadcast packets, as shown in [Figure 2-1](#).

Figure 2-1 NTP broadcast mode



Precautions

1. In broadcast mode, configure both the NTP server and the NTP client.
2. The clock stratum of the client must be less than or equal to that of the server. Otherwise, clock synchronization fails.

Procedure

- Configure the NTP broadcast server.
 1. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
 2. (Optional) Configure NTP authentication.

On NTP-enabled networks demanding high security, NTP authentication is required. The NTP configuration of the server must be the same as that of the client.

 - a. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - b. Run the **ntp-service authentication-keyid** command to configure an NTP authentication key.
 - c. Run the **ntp-service reliable authentication-keyid** command to declare the key as reliable.
 3. Configure a VLANIF interface.
 - a. Run the **vlan** command to create a VLAN.
 - b. Run the **port vlan** command to add an uplink port to the VLAN so that the user packets with the VLAN tag are transmitted through the uplink port.
 - c. Run the **interface vlanif** command to create a VLANIF interface.
 - d. Run the **ip address** command to configure an IP address and a subnet mask for the VLANIF interface so that IP packets in the VLAN can be forwarded at Layer 3.
 4. Run the **ntp-service broadcast-server** command to configure the NTP broadcast server mode of the host, and specify the key ID for the server to send packets to the client.
- Configure the NTP broadcast client.
 1. (Optional) Configure NTP authentication.

On NTP-enabled networks demanding high security, NTP authentication is required. The NTP configuration of the server must be the same as that of the client.

 - a. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - b. Run the **ntp-service authentication-keyid** command to configure an NTP authentication key.
 - c. Run the **ntp-service reliable authentication-keyid** command to declare the key as reliable.
 2. Configure a VLANIF interface.
 - a. Run the **vlan** command to create a VLAN.
 - b. Run the **port vlan** command to add an uplink port to the VLAN so that the user packets with the VLAN tag are transmitted through the uplink port.
 - c. Run the **interface vlanif** command to create a VLANIF interface.
 - d. Run the **ip address** command to configure an IP address and a subnet mask for the VLANIF interface so that IP packets in the VLAN can be forwarded at Layer 3.
 3. Run the **ntp-service broadcast-client** command to configure the local device as the NTP broadcast client.

----End

Example

Configure AC_S to use the local clock as the master NTP clock, set the clock stratum to 2, use the NTP broadcast mode, and configure VLANIF 2 at 10.10.10.10/24 to periodically broadcast clock synchronization packets. Configure AC_C as the NTP client and enable the client to listen to the broadcast packets sent from the server through VLANIF 2 at 10.10.10.10/24 and synchronize with the clock of the broadcast server.

1. Configure AC_S:

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service broadcast-server
huawei(config-if-vlanif2)#quit
```
2. Configure AC_C:

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service broadcast-client
huawei(config-if-vlanif2)#quit
```

2.1.3 Configuring the NTP Multicast Mode

This section describes how to configure the AC (NTP client) to synchronize the clock in NTP multicast mode. After the configuration is complete, the server periodically multicasts clock synchronization packets through a specified port, and the client synchronizes the local clock according to the received multicast packets.

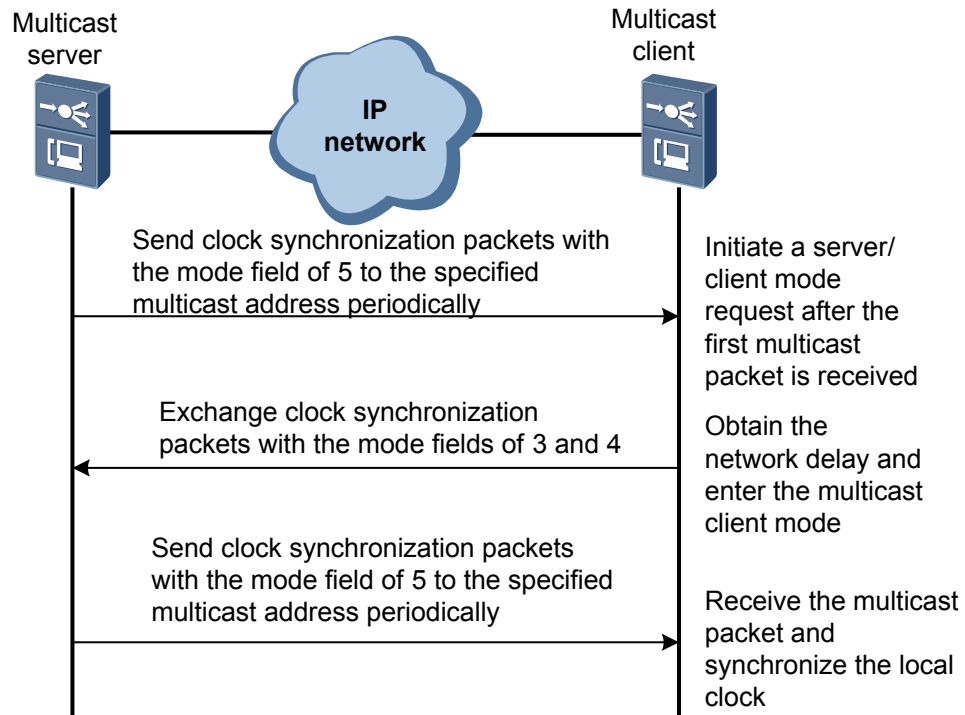
Prerequisites

The network interface and the routing protocol of the AC have been configured so that the server and the client can communicate at the network layer.

Context

In multicast mode, the server periodically sends clock synchronization packets to the specified multicast address. The default NTP multicast address 224.0.1.1 is used if no multicast address is configured. The mode field of a clock synchronization packet is set to 5 (multicast mode). The client listens to the multicast packets sent from the server. After receiving the first multicast packet, the client exchanges NTP packets with the server to obtain a network delay. The client then enters the multicast client mode and synchronizes the local clock according to multicast packets received from the server, as shown in [Figure 2-2](#).

Figure 2-2 NTP multicast mode



Precautions

1. In multicast mode, configure both the NTP server and the NTP client.
2. The clock stratum of the client must be less than or equal to that of the server. Otherwise, clock synchronization fails.

Procedure

- Configure the NTP multicast server.
 1. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
 2. (Optional) Configure NTP authentication.
On NTP-enabled networks demanding high security, NTP authentication is required. The NTP configuration of the server must be the same as that of the client.
 - a. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - b. Run the **ntp-service authentication-keyid** command to configure an NTP authentication key.
 - c. Run the **ntp-service reliable authentication-keyid** command to declare the key as reliable.
 3. Configure a VLANIF interface.
 - a. Run the **vlan** command to create a VLAN.

- b. Run the **port vlan** command to add an uplink port to the VLAN so that the user packets with the VLAN tag are transmitted through the uplink port.
 - c. Run the **interface vlanif** command to create a VLANIF interface.
 - d. Run the **ip address** command to configure an IP address and a subnet mask for the VLANIF interface so that IP packets in the VLAN can be forwarded at Layer 3.
 4. Run the **ntp-service multicast-server** command to configure the NTP multicast server mode, and specify the key ID for the server to send packets to the client.
 - Configure the NTP multicast client.
 1. (Optional) Configure NTP authentication.

On NTP-enabled networks demanding high security, NTP authentication is required. The NTP configuration of the server must be the same as that of the client.

 - a. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - b. Run the **ntp-service authentication-keyid** command to configure an NTP authentication key.
 - c. Run the **ntp-service reliable authentication-keyid** command to declare the key as reliable.
 2. Configure a VLANIF interface.
 - a. Run the **vlan** command to create a VLAN.
 - b. Run the **port vlan** command to add an uplink port to the VLAN so that the user packets with the VLAN tag are transmitted through the uplink port.
 - c. Run the **interface vlanif** command to create a VLANIF interface.
 - d. Run the **ip address** command to configure an IP address and a subnet mask for the VLANIF interface so that IP packets in the VLAN can be forwarded at Layer 3.
 3. Run the **ntp-service multicast-client** command to configure the local device as the NTP multicast client.

----End

Example

Configure AC_S to use the local clock as the master NTP clock, set the clock stratum to 2, use the NTP multicast mode, and configure VLANIF 2 at 10.10.10.10/24 to periodically multicast clock synchronization packets. Configure AC_C as the NTP client and enable the client to listen to the multicast packets sent from the server through VLANIF 2 at 10.10.10.10/24 and synchronize with the clock of the multicast server.

1. Configure AC_S:

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service multicast-server
huawei(config-if-vlanif2)#quit
```
2. Configure AC_C:

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
```

```
huawei(config-if-vlanif2)#ntp-service multicast-client  
huawei(config-if-vlanif2)#quit
```

2.1.4 Configuring the NTP Client/Server Mode

This section describes how to configure the AC as the NTP client to synchronize the clock with the NTP server.

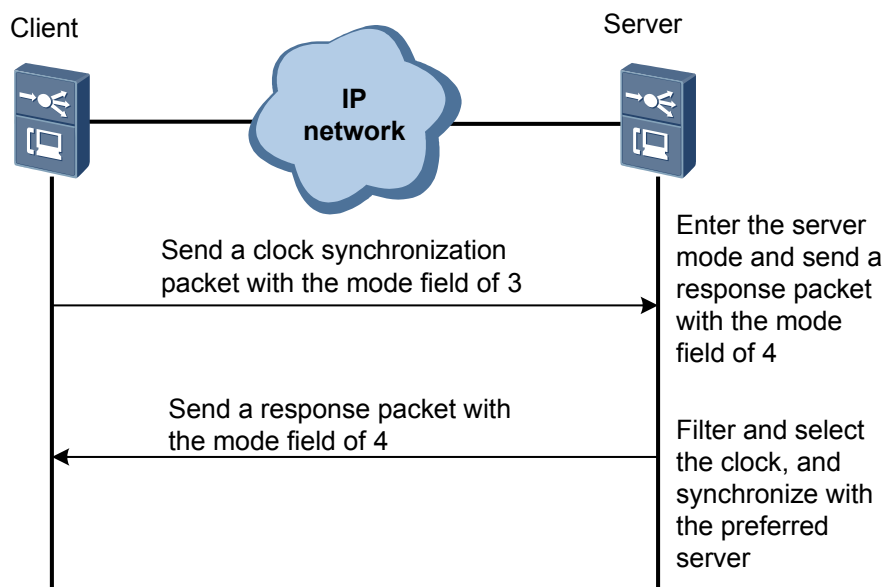
Prerequisites

The network interface and the routing protocol of the AC have been configured so that the server and the client can communicate at the network layer.

Context

In client/server mode, the client sends a synchronization packet to the server, with the mode field of 3 (client mode). After receiving the packet, the server automatically enters the server mode and sends a response packet with the mode field of 4 (server mode). After receiving the response from the server, the client filters and selects the clock, and synchronizes with the preferred server, as shown in [Figure 2-3](#).

Figure 2-3 NTP client/server mode



Precautions

1. In client/server mode, you need to configure only the client.
2. The clock stratum of the client must be less than or equal to that of the server. Otherwise, clock synchronization fails.

Procedure

Step 1 Configure a VLANIF interface.

1. Run the **vlan** command to create a VLAN.
2. Run the **port vlan** command to add an uplink port to the VLAN so that the user packets with the VLAN tag are transmitted through the uplink port.
3. Run the **interface vlanif** command to create a VLANIF interface.
4. Run the **ip address** command to configure an IP address and a subnet mask for the VLANIF interface so that IP packets in the VLAN can be forwarded at Layer 3.

Step 2 Run the **ntp-service unicast-server** command to configure the NTP unicast server mode, and specify the IP address of the remote server that functions as the local timer server and the interface for transmitting and receiving NTP packets.

 **NOTE**

- In this command, *ip-address* must be a unicast address. It cannot be a broadcast address, a multicast address, or the IP address of a local clock.
- After the source interface of the NTP packets is specified by *source-interface*, the source IP address of the NTP packets is configured as the primary IP address of the specified interface.
- A server can function as a time server to synchronize other devices only after its clock is synchronized.
- When the clock stratum of the server is higher than or equal to that of the client, the client does not synchronize with the server.
- You can run the **ntp-service unicast-server** command multiple times to configure multiple servers. Then the client selects the best server according to clock priorities.

Step 3 (Optional) Configure an ACL rule.

To filter the packets that pass through the Layer 3 interface and allow only IP packets from the clock server to pass through the Layer 3 interface, configure an ACL.

1. Run the **acl adv-acl-number** command to create an ACL.
2. Run the **rule** command to allow or reject data packets according to the source IP address, destination IP address, type of the protocol over IP, and features or protocol of the packet.
3. Run the **packet-filter** command to configure an ACL filtering rule for a specified port, and make the configuration take effect.

----End

Example

Configure the NTP client/server mode.

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#acl 3010
huawei(config-acl-adv-3010)#rule deny ip source any destination 10.10.10.10
0.0.0.0
huawei(config-acl-adv-3010)#rule permit ip source 10.20.20.20 0.0.0.0 destination
10.10.10.10 0.0.0.0
huawei(config-acl-adv-3010)#quit
huawei(config)#packet-filter inbound ip-group 3010 port 0/2/24
```

2.2 Configuring System Security

This section describes how to configure system security to protect the system against malicious attacks.

Context

The security feature protects the WS6603 against attacks initiated by invalid packets so that the device can run stably. The WS6603 provides the following security functions:

- ACL/Packet filtering firewall
- Blacklist
- Anti-DoS attack
- Anti-ICMP/IP attack
- Source route filtering
- Source MAC address filtering
- User-side ring network detection
- Permitted or denied IP address segments

Table 2-2 lists the default settings of system security.

Table 2-2 Default settings of system security

Item	Default Setting
Blacklist	Disabled
Anti-DoS attack	Disabled
Anti-ICMP attack	Disabled
Anti-IP attack	Disabled
Source route filtering	Disabled
User-side ring network detection	Disabled

2.2.1 Configuring the Firewall

You can configure the system firewall to control packets passing through the management port of the WS6603 so that unauthorized operators cannot access the system in inband or outband mode.

Context

The firewall has the following functions:

- **Blacklist:** The blacklist function filters out the packets sent from a specific IP address. Blacklist entries can be added or deleted dynamically. When the firewall detects a possible attack from a specific IP address according to the characteristics of packets, the firewall adds a blacklist entry and then filters out the packets from this IP address.
- **ACL/Packet filtering:** To configure a port to allow only one type of packets to go through, use an ACL to filter packets.

For example, to allow only the packets from source IP address 1.1.1.1 to pass through a port, perform the following operations:

1. Configure ACL rule 1 to allow the packets with source IP address 1.1.1.1 to pass through.
2. Configure ACL rule 2 to reject all packets.
3. Run the **firewall packet-filter** command to bind ACL rule 2 first and then ACL rule 1 to the inbound direction.

 **NOTE**

On the AC, an ACL can be activated in two modes. In the two modes, the sequence in which rules in the ACL take effect are different.

- Run the **firewall packet-filter** command to activate the ACL. This mode is applied to the NMS. The software determines the sequence in which ACL rules take effect. The rule that was configured first takes effect first.
- Run the **packet-filter** command to activate the ACL. The hardware determines the sequence in which ACL rules take effect. The rule that was configured last takes effect first.



CAUTION

To ensure device security, configure the firewall to control packets passing through the management port of the WS6603.

Procedure

- Configure the blacklist.

You can configure the blacklist in two modes: using ACLs and adding source IP addresses of untrusted packets. You can choose either mode, or both.

When two modes are configured at the same time, source IP addresses in the blacklist take precedence over ACLs. The system matches the packets with source IP addresses in the blacklist first, and then with the ACL.

 **NOTE**

The blacklist function takes effect only for user-side packets.

- To configure the blacklist function by using advanced ACLs, perform the following operations:
 1. Run the **acl** command to create an ACL. Only advanced ACLs can be used for the blacklist function. The number of an advanced ACL ranges from 3000 to 3999.
 2. Run the **rule(adv acl)** command to create an advanced ACL rule.
 3. Run the **quit** command to return to the global config mode.
 4. Run the **firewall blacklist enable acl-numberacl-number** command to enable the blacklist function.
- To configure the blacklist function by adding source IP addresses of untrusted packets, perform the following operations:
 1. Run the **firewall blacklist item** command to add source IP addresses of untrusted packets to the blacklist.
 2. Run the **firewall blacklist enable** command to enable the blacklist function.
- Configure the firewall (filtering packets based on the ACL).

1. Run the **acl** command to create an ACL. Only basic ACLs and advanced ACLs can be used when packet filtering firewall is configured. Therefore, the range of the ACL number is 2000-3999.
2. Run different rule commands to create different types of ACL rules.
 - Run the **rule (basic acl)** command to create a basic ACL rule.
 - Run the **rule (adv acl)** command to create an advanced ACL rule.
3. Run the **quit** command to return to the global config mode.
4. Run the **firewall enable** command to enable the blacklist function. By default, the blacklist function is disabled.
To filter the packets of a port based on the basic ACL, enable the blacklist function.
5. To configure a packet filtering rule for the MEth port, run the **interface meth** command to enter the MEth mode; to configure a packet filtering rule for the VLANIF interface, run the **interface vlanif** command to enter the VLANIF mode.
6. Run the **firewall packet-filter** command to apply packet filtering rules to the interface.

----End

Example

To add IP address 192.168.10.18 to the blacklist with the aging time of 100 minutes, run the following commands:

```
huawei (config) #firewall blacklist item 192.168.10.18 timeout 100
huawei (config) #firewall blacklist enable
```

Add the IP addresses on subnet 10.10.10.0 to the blacklist and bind ACL 3000 to these IP addresses.

```
huawei (config) #acl 3000
huawei (config-acl-adv-3000) #rule deny ip source 10.10.10.0 0.0.0.255 destination
10.10.10.20 0
huawei (config-acl-adv-3000) #quit
huawei (config) #firewall blacklist enable acl-number 3000
```

Prevent users on subnet 172.16.25.0 from accessing the maintenance network port of the AC at 172.16.25.28.

```
huawei (config) #acl 3001
huawei (config-acl-adv-3001) #rule 5 deny icmp source 172.16.25.0 0.0.0.255 destina
tion 172.16.25.28 0
huawei (config-acl-adv-3001) #quit
huawei (config) #firewall enable
huawei (config) #interface meth 0
huawei (config-if-meth0) #firewall packet-filter 3001 inbound
ACL applied successfully
```

2.2.2 Configuring Defense Against Malicious Attacks

Anti-DoS attack, anti-ICMP/IP attack, source route filtering, and source MAC address filtering prevent malicious attacks to ensure system security.

Context

The WS6603 provides the following measures to prevent malicious attacks to the system:

- Anti-DoS attack: enables the WS6603 to receive only authenticated protocol packets sent by users.
- Anti-ICMP attack: enables the WS6603 to discard Internet Control Message Protocol (ICMP) packets destined for the WS6603.
- Anti-IP attack: enables the WS6603 to discard IP packets destined for the WS6603.
- Source route filtering: enables the WS6603 to filter IP packets with source route options.

Procedure

- Configure anti-DoS attack.

Run the **security anti-dos enable** command to enable anti-DoS attack globally.

After anti-DoS attack is enabled globally, the WS6603 adds user ports carried in received attack packets to a blacklist. When anti-DoS attack is disabled, the system deletes the blacklist entry.

Application scenario: Two APs (AP1 and AP2) are connected to the network through the AC. If a malicious user (AP1) sends a large number of protocol packets to attack the CPU of the AC, the CPU usage of the AC will become too high, and then the AC is unable to process services of other APs such as AP2. To prevent DoS attacks, block the attack port or suppress its protocol packets sent from the attack port to protect the AC.

- Configure source route filtering.

Run the **security source-route enable** command to enable source route filtering. This function filters the packets that carry source route options and are reported to the Layer 3 network.

Application scenario: Routes are dynamic and applications do not control route selection. However, a malicious sender can add routing information to IP packets, select a specified route, and send these IP packets along the specified route on the network. To prevent malicious attacks, enable the source route filtering function. Then the AC performs validity check on IP packets and discards the packets that match source route options.

---End

Example

Enable anti-DoS attack globally.

```
huawei(config)#security anti-dos enable
```

2.2.3 Configuring a Permitted/Denied IP Address Segment

Only the users with IP addresses in the permitted IP address segment can access the AC, and users with IP addresses in the denied IP address segment cannot access the AC. This prevents users in invalid IP address segments from logging in to the system, ensuring system security.

Context

Each firewall can be configured with up to 10 address segments.

When you add an address segment, ensure that the start address of the address segment is unique.

The start address of the address segment is required when you delete the address segment.

Procedure

- Configure permitted and denied IP address segments for login through Telnet.
 1. Run the **sysman ip-access telnet** command to configure the permitted IP address segment for login through Telnet.



CAUTION

To ensure device security, comply with the least privilege principle. Configure the permitted IP address segment, and add only the necessary management IP address segment. Other IP addresses are not permitted to access the AC through the management port.

2. Run the **sysman ip-refuse telnet** command to configure a denied IP address segment for login through Telnet.



NOTE

The permitted address segment and the denied address segment cannot overlap. Only users whose IP addresses are in the permitted address segment are allowed to access the AC.

3. Run the **sysman firewall telnet enable** command to enable the firewall function for access through Telnet. By default, the firewall function of the system is disabled.

- Configure permitted and denied IP address segments for access through SSH.
 1. Run the **sysman ip-access ssh** command to configure a permitted IP address segment for login through SSH.



CAUTION

To ensure device security, comply with the least privilege principle. Configure the permitted IP address segment, and add only the necessary management IP address segment. Other IP addresses are not permitted to access the AC through the management port.

2. Run the **sysman ip-refuse ssh** command to configure a denied IP address segment for login through SSH.



NOTE

The permitted address segment and the denied address segment cannot overlap. Only users whose IP addresses are in the permitted address segment are allowed to access the AC.

3. Run the **sysman firewall ssh enable** command to enable the firewall function for login through SSH. By default, the firewall function of the system is disabled.

- Configure permitted and denied IP address segments for login through SNMP (from the NMS).
 1. Run the **sysman ip-access snmp** command to configure a permitted IP address segment for login through SNMP.

**CAUTION**

To ensure device security, comply with the least privilege principle. Configure the permitted IP address segment, and add only the necessary management IP address segment. Other IP addresses are not permitted to access the AC through the management port.

2. Run the **sysman ip-refuse snmp** command to configure a denied IP address segment for login through SNMP.

 **NOTE**

The permitted address segment and the denied address segment cannot overlap. Only users whose IP addresses are in the permitted address segment are allowed to access the AC.

3. Run the **sysman firewall snmp enable** command to enable the firewall function for login through SNMP. By default, the firewall function of the system is disabled.

---End

Example

Enable the firewall function for login through Telnet, and permit only users with the IP address segment 134.140.5.1-134.140.5.254 to log in to the AC through Telnet.

```
huawei(config)#sysman ip-access telnet 134.140.5.1 134.140.5.254  
huawei(config)#sysman firewall telnet enable
```

Enable the firewall function for login through SSH, and permit only users with the IP address segment 133.7.22.1-133.7.22.254 to log in to the device through SSH.

```
huawei(config)#sysman ip-access ssh 133.7.22.1 133.7.22.254  
huawei(config)#sysman firewall ssh enable
```

Enable the firewall function for login through SNMP, and permit only users with the IP address segment 10.10.20.1-10.10.20.254 to log in to the device through SNMP.

```
huawei(config)#sysman ip-refuse snmp 10.10.20.1 10.10.20.254  
huawei(config)#sysman firewall snmp enable
```

2.3 Configuring an ACL

This section describes access control list (ACL) types and rules.

Context

An ACL defines a series of rules and identifies the packets that need to be filtered. Then the ACL permits or denies the packets according to the configured policy. ACL-based traffic filtering is a prerequisite for quality of service (QoS) or user security.

[Table 2-3](#) lists the ACL types.

Table 2-3 ACL types

Type	Value Range	Description
Basic ACL	2000-2999	A basic ACL analyzes and processes a packet based on the source IP address.
Advanced ACL	3000-3999	An advanced ACL analyzes and processes a packet based on the source IP address, destination IP address, protocol type over IP, and protocol features, such as the TCP source and destination ports and ICMP type. Compared with a basic ACL, an advanced ACL supports more accurate, diverse, and flexible rules.
Link layer ACL	4000-4999	A link layer ACL analyzes and processes a Layer 2 frame based on the link layer information such as the source MAC address, VLAN ID, link layer protocol type, and destination MAC address.
User-defined ACL	5000-5999	A user-defined ACL analyzes and processes a Layer 2 frame according to any 32 bytes of the first 80 bytes in the Layer 2 frame.

When a packet matches two or more ACL rules, the matching order is as follows:

- If the rules of an ACL are activated simultaneously, the rule that was configured earlier takes effect first.
- If the rules of an ACL are activated one by one, the rule that is activated later takes effect first.
- If the rules belong to different ACLs, the rule that is activated later takes effect first.

Precautions

When configuring ACLs, pay attention to the following points:

- It is recommended that you define a common rule, such as permit any or deny any, in each ACL, so that any common packet can match the rule.
- Activated ACL rules share the limited hardware resources with protocol modules such as the DHCP module and IPoA module; therefore, hardware resources may be insufficient. To prevent a failure to enable service functions due to insufficient hardware resources, it is recommended that you enable a protocol module first and then activate the ACL rules during data configuration. If the protocol module cannot be enabled:
 1. Check whether ACL rules occupy too many resources.
 2. If ACL rules occupy too many resources, deactivate or delete unimportant or temporarily unused ACL rules, and then configure and enable the protocol module.

2.3.1 Configuring a Basic ACL

A basic ACL classifies traffic of packets based on source IP addresses.

Context

The number of a basic ACL ranges from 2000 to 2999.

A basic ACL analyzes and processes packets only based on source IP addresses.

Procedure

Step 1 (Optional) Configure a time range.

Run the **time-range** command to create a time range in which ACL rules take effect.

Step 2 Create a basic ACL.

Run the **acl** command to create a basic ACL and enter the ACL-basic mode.

Step 3 Configure a basic ACL rule.

In ACL-basic mode, run the **rule** command to create a basic ACL rule. The parameters are as follows:

- **rule-id**: specifies the ID of an ACL rule. To create an ACL rule with a specified ID, use this parameter.
- **permit**: permits packets that match ACL rules to pass through.
- **deny**: discards packets that match ACL rules.
- **time-range**: specifies the time range in which ACL rules take effect.

Step 4 Activate the ACL.

The ACL does not take effect immediately after being created. Run a command to activate the ACL and configure QoS. The following are examples:

- Run the **packet-filter** command to activate the ACL.
- Run the **firewall packet-filter** command to activate the ACL. For details, see [2.2.1 Configuring the Firewall](#).
- Configure QoS. For details, see [2.4.3 Configuring ACL-based Traffic Management](#).

----End

Example

Configure port 0/2/0 on the AC to receive only the packets from 2.2.2.2 and discard the packets from other addresses from 00:00 to 12:00 on Friday.

```
huawei (config) #time-range time1 00:00 to 12:00 fri
huawei (config) #acl 2000
huawei (config-acl-basic-2000) #rule permit source 2.2.2.2 0.0.0.0 time-range time1
huawei (config-acl-basic-2000) #rule deny time-range time1
huawei (config-acl-basic-2000) #quit
huawei (config) #packet-filter inbound ip-group 2000 port 0/2/0
huawei (config) #save
```

2.3.2 Configuring an Advanced ACL

An advanced ACL classifies traffic of data packets based on the source address, destination address, protocol type over IP, and protocol features, such as the TCP source and destination ports and ICMP type.

Context

The number of an advanced ACL ranges from 3000 to 3999.

An advanced ACL can classify traffic based on the following information:

- Protocol type
- Source IP address
- Destination IP address
- Source port number (source port of UDP or TCP packets)
- Destination port number (destination port of UDP or TCP packets)
- ICMP packet type
- Precedence value
- Type of Service (ToS) value
- Differentiated Services Code Point (DSCP) value

Procedure

Step 1 (Optional) Configure a time range.

Run the **time-range** command to create a time range in which ACL rules take effect.

Step 2 Create an advanced ACL.

Run the **acl** command to create an advanced ACL and then enter the ACL-adv mode.

Step 3 Configure an advanced ACL rule.

In ACL-adv mode, run the **rule** command to create an ACL rule. The parameters are as follows:

- **rule-id**: specifies the ID of an ACL rule. To create an ACL rule with a specified ID, use this parameter.
- **permit**: permits packets that match ACL rules to pass through.
- **deny**: discards packets that match ACL rules.
- **time-range**: specifies the time range in which ACL rules take effect.

Step 4 Activate the ACL.

The ACL does not take effect immediately after being created. Run a command to activate the ACL and configure QoS. The following are examples:

- Run the **packet-filter** command to activate the ACL.
- Run the **firewall packet-filter** command to activate the ACL. For details, see [2.2.1 Configuring the Firewall](#).
- Configure QoS. For details, see [2.4.3 Configuring ACL-based Traffic Management](#).

----End

Example

Example 1: On the AC, a VLAN is created and a VLANIF interface is specified. The IP address 10.10.10.101 is assigned to the VLANIF interface.

Perform the following operations to reject ICMP (such as ping packets) and Telnet packets on the VLANIF interface of the AC.

```
huawei (config) #acl 3001
huawei (config-acl-adv-3001) rule 1 deny icmp destination 10.10.10.101 0
```

```
huawei(config-acl-adv-3001)rule 2 deny tcp destination 10.10.10.101 0 destination-  
port eq telnet  
huawei(config-acl-adv-3001)quit  
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/2/0  
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/2/0  
huawei(config)#save
```

Example 2: On the AC, a VLAN is created and a VLANIF interface is specified. The IP address 10.10.10.101 is assigned to the VLANIF interface. Port 20 on the AC is connected to the AP at 10.10.10.20. Users connected to this AP can obtain IP addresses in the range of 192.168.1.1 to 192.168.1.254.

In the following example, only APs and terminals on the specified network segment can access the AC.

```
huawei(config)#acl 3001  
huawei(config-acl-adv-3001)rule 1 deny ip destination 10.10.10.101 0  
huawei(config-acl-adv-3001)rule 2 permit ip source 10.10.10.20 0 destination  
10.10.10.101 0  
huawei(config-acl-adv-3001)rule 3 permit ip source 192.168.1.0 0.0.0.255  
destination 10.10.10.101 0  
huawei(config-acl-adv-3001)quit  
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/2/20  
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/2/20  
huawei(config)#packet-filter inbound ip-group 3001 rule 3 port 0/2/20
```

2.3.3 Configuring a Link Layer ACL

A link layer ACL classifies traffic based on the link layer information such as the source MAC address, VLAN ID, Layer 2 protocol type, and destination MAC address.

Context

The number of a link layer ACL ranges from 4000 to 4999.

A link layer ACL can classify traffic based on the following link layer information:

- Type of the protocol over Ethernet
- 802.1p priority
- VLAN ID
- Source MAC address
- Destination MAC address

Procedure

Step 1 (Optional) Configure a time range.

Run the **time-range** command to create a time range in which ACL rules take effect.

Step 2 Create a link layer ACL.

Run the **acl** command to create a link layer ACL, and then enter the ACL-link mode.

Step 3 Configure a link layer ACL rule.

In ACL-link mode, run the **rule** command to create a link layer ACL rule. The parameters are as follows:

- **rule-id**: specifies the ID of an ACL rule. To create an ACL rule with a specified ID, use this parameter.
- **permit**: permits packets that match ACL rules to pass through.

- **deny**: discards packets that match ACL rules.
- **time-range**: specifies the time range in which ACL rules take effect.

Step 4 Activate the ACL.

The ACL does not take effect immediately after being created. Run a command to activate the ACL and configure QoS. The following are examples:

- Run the **packet-filter** command to activate the ACL.
- Configure QoS. For details, see [2.4.3 Configuring ACL-based Traffic Management](#).

----End

Example

Create a link layer ACL rule that allows data packets with protocol type 0x8863, VLAN ID 12, CoS 1, source MAC address 2222-2222-2222, and destination MAC address 00e0-fc11-4141 to pass through.

```

huawei (config) #acl 4001
huawei (config-acl-link-4001) rule 1 permit type 0x8863 cos 1 source 12
2222-2222-2222 0000-0000-0000 destination 00e0-fc11-4141 0000-0000-0000
huawei (config-acl-basic-4001) quit
huawei (config) #save
    
```

2.3.4 Configuring a User-defined ACL

A user-defined ACL classifies traffic based on any 32 bytes of the first 80 bytes in a Layer 2 frame.

Context

The number of a user-defined ACL ranges from 5000 to 5999.

A user-defined ACL rule can be created based on any 32 bytes of the first 80 bytes in the Layer 2 frame.

Figure 2-4 First 64 bytes of a frame

```

AA AA AA AA AA BB BB BB BB BB BB CC CC CC CC
DD DD EE FF GG GG HH HH II II JJ KK LL LL MM MM
MM MM NN NN NN OO OO PP PP QQ QQ QQ QQ RR RR
RR RR SS TT UU UU VV VV VV VV VV VV VV VV VV
    
```

[Table 2-4](#) describes the letters and lists their offset values.

Table 2-4 Letters and their offset values

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC address	0	L	IP checksum	28
B	Source MAC address	6	M	Source IP address	30

Letter	Meaning	Offset	Letter	Meaning	Offset
C	VLAN tag	12	N	Destination IP address	34
D	Protocol type	16	O	TCP source port	38
E	IP version number	18	P	TCP destination port	40
F	ToS	19	Q	Serial number	42
G	IP packet length	20	R	Acknowledgment field	46
H	ID	22	S	IP header length and reserved bit	50
I	Flags	24	T	Reserved bit and flags bit	51
J	TTL	26	U	Window size	52
K	Protocol ID (6 represents TCP and 17 represents UDP)	27	V	Others	54

 **NOTE**

The offset value of each field is the offset value in frame ETH II+VLAN tag. You can use the mask of a user-defined ACL rule and offset to extract any bytes from the first 80 bytes of frames, and then compare the extracted bytes with the user-defined ACL to filter matched frames for further processing.

Procedure

Step 1 (Optional) Configure a time range.

Run the **time-range** command to create a time range in which ACL rules take effect.

Step 2 Create a user-defined ACL.

Run the **acl** command to create a user-defined ACL, and then enter the ACL-user mode.

Step 3 Configure a user-defined ACL rule.

In ACL-user mode, run the **rule** command to create an ACL rule. The parameters are as follows:

- **rule-id**: specifies the ID of an ACL rule. To create an ACL rule with a specified ID, use this parameter.
- **permit**: permits packets that match ACL rules to pass through.
- **deny**: discards packets that match ACL rules.
- **rule-string**: specifies the character string of the user-defined rule. The character string is in hexadecimal notation. The number of characters in the string must be an even number.
- **rule-mask**: specifies the mask of the user-defined rule. It is a positive mask and used to perform the AND operation with packets for extracting the information from the packets.
- **offset**: specifies the offset from which the AND operation begins. It works with the rule mask to extract a character string from a packet.

- **time-range**: specifies the time range in which ACL rules take effect.

Step 4 Activate the ACL.

The ACL does not take effect immediately after being created. Run a command to activate the ACL and configure QoS. The following are examples:

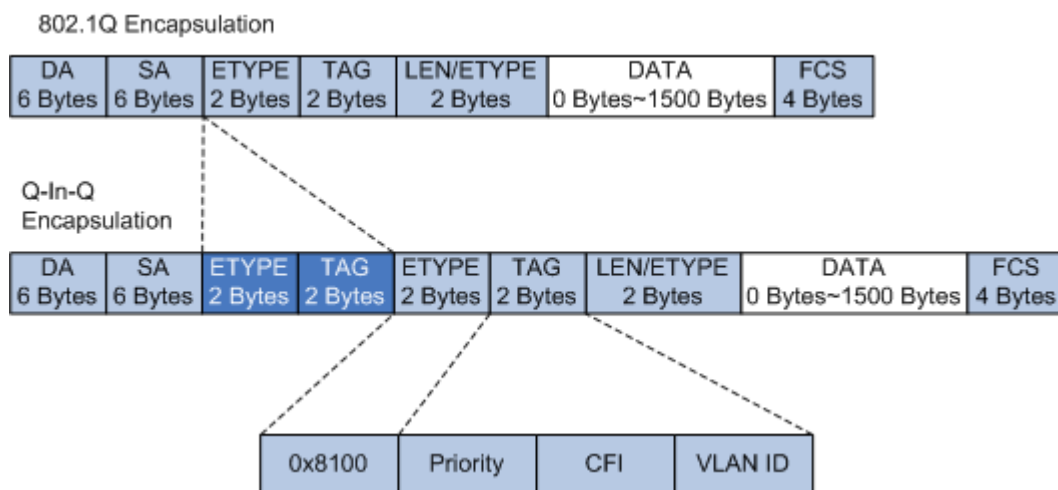
- Run the **packet-filter** command to activate the ACL.
- Configure QoS. For details, see [2.4.3 Configuring ACL-based Traffic Management](#).

----End

Example

Assume that a packet sent from port 0/2/0 to the AC is a QinQ packet. Change the CoS value in the outer VLAN tag (inner VLAN ID: 10) to 5.

Figure 2-5 QinQ packet format



```
huawei (config) #acl 5001
huawei (config-acl-user-5001) #rule 1 permit 8100 ffff 16
```

NOTE

The type value of a QinQ packet varies with different vendors. Huawei uses the default value 0x8100. As shown in [Figure 2-5](#), the offset of this type value is 16 bytes.

```
huawei (config-acl-user-5001) #rule 10 permit 0a ff 19
```

NOTE

"19" indicates that the user-defined ACL matches the packets from the nineteenth bytes of the Layer 2 header. "0a" refers to the value of the inner VLAN tag field in the QinQ packet. In this example, the second byte of the inner tag field is a part of the VLAN ID, which is exactly the inner VLAN ID (VLAN 10).

```
huawei (config-acl-user-5001) #quit
huawei (config) #traffic-priority inbound user-group 5001 cos 5 port 0/2/0
```

2.4 Configuring QoS

This section describes how to configure quality of service (QoS) on the AC.

Context

The QoS technology provides differentiated services.

The AC provides the following functions to implement QoS:

- Traffic management
Traffic management allows the AC to limit the traffic for a user service or a user port.
- Queue scheduling
After traffic management is performed for service packets, queue scheduling allows the AC to put service packets into queues with different priorities.

In addition to the preceding functions, the AC supports hierarchical quality of service (HQoS) and ACL-based traffic management.

- HQoS
The AC supports two levels of traffic management for HQoS users and HQoS user groups.
- ACL-based traffic management
If users need to flexibly implement QoS for service traffic, configure an ACL to classify the service traffic (see [2.3 Configuring an ACL](#)) and take QoS actions for the service traffic.

2.4.1 Configuring Traffic Management

This section describes how to configure traffic management on the AC.

Introduction to Traffic Management

The AC supports traffic management for incoming and outgoing traffic, and supports traffic management based on the combination of the port number and VLAN ID.

In addition, the AC supports rate limiting on an Ethernet port and traffic suppression for incoming broadcast packets and unknown multicast or unicast packets.

Configuring Rate Limiting on an Ethernet Port

This section describes how to configure rate limiting on a specified Ethernet port.

Prerequisite

- Rate limiting takes effect on only the Ethernet port.
- Traffic that exceeds the rate limit is discarded.

Procedure

Step 1 In global config mode, run the **line-rate** command to set the rate limit for incoming traffic on the specified Ethernet port.

Parameters are as follows:

- target-rate: specifies the rate limit on an Ethernet port, in kbit/s.
- port: indicates the shelf ID/slot ID/port number.

Step 2 Run the **display qos-info line-rate port** command to view the rate limit on the Ethernet port.

----End

Example

Set the rate limit on Ethernet port 0/2/0 to 6400 kbit/s.

```
huawei(config)#line-rate 6400 port 0/2/0
huawei(config)#display qos-info line-rate port 0/2/0

line-rate:
port 0/2/0:
  Line rate: 6400 Kbps
```

Configuring Traffic Suppression

The traffic suppression function suppresses the received broadcast, unknown multicast, and unknown unicast packets to ensure service processing.

Context

Traffic suppression can be configured on a board or a port on a board.

Procedure

- Step 1** Run the **interface scu** command to enter the SCU mode.
- Step 2** View the traffic suppression threshold.
Run the **display traffic-suppress all** command to view the traffic suppression threshold.
- Step 3** Run the **traffic-suppress** command to suppress traffic for a port on the SCU.
Parameters are as follows:
 - *broadcast*: suppresses broadcast traffic.
 - *multicast*: suppresses unknown multicast traffic.
 - *unicast*: suppresses unknown unicast traffic.
 - *value*: specifies the index of the traffic suppression level.

---End

Example

Configure suppression for broadcast packets according to traffic suppression level 8 on port 0 of the SCU.

```
huawei(config)#interface scu 0/2
huawei(config-if-scu-0/2)#display traffic-suppress all
```

Command:

```
display traffic-suppress all
```

Traffic suppression ID definition:

NO.	Min bandwidth(kbps)	Max bandwidth(kbps)	Package number(pps)
1	6	145	12
2	12	291	24
3	24	582	48
4	48	1153	95
5	97	2319	191
6	195	4639	382
7	390	9265	763
8	781	18531	1526

9	1562	37063	3052
10	3125	74126	6104
11	6249	148241	12207
12	12499	296483	24414
13	0	0	0

PortID	Broadcast_index	Multicast_index	Unicast_index
0	7	7	OFF
1	7	7	OFF
2	7	7	OFF
3	7	7	OFF

```

huawei(config-if-scu-0/2)#traffic-suppress all broadcast value 8
huawei(config-if-scu-0/2)#display traffic-suppress 0
Traffic suppression ID definition:

```

NO.	Min bandwidth(kbps)	Max bandwidth(kbps)	Package number(pps)
1	6	145	12
2	12	291	24
3	24	582	48
4	48	1153	95
5	97	2319	191
6	195	4639	382
7	390	9265	763
8	781	18531	1526
9	1562	37063	3052
10	3125	74126	6104
11	6249	148241	12207
12	12499	296483	24414
13	0	0	0

```

Current traffic suppression index of broadcast      : 8
Current traffic suppression index of multicast     : 7
Current traffic suppression index of unknown unicast : 7

```

2.4.2 Configuring Queue Scheduling

Queue scheduling ensures that packets of key services are processed in time when network congestion occurs.

Context

On the AC, congestion may occur in inbound and outbound directions. Packets of key services need to be processed first when congestion occurs. The AC supports Priority Queuing (PQ) and Weighted Round Robin (WRR).

Configuring the Queue Scheduling Mode

This section describes how to configure the queue scheduling mode to ensure that packets in high-priority queues are processed in time when congestion occurs.

Context

The AC supports PQ, WRR, and PQ+WRR.

- PQ

In PQ, packets are sent based on their queue priorities. Packets in the highest priority queue are sent first, and packets in lower priority queues are sent only when the queues with higher priorities are emptied.

By default, the system uses PQ.

- **WRR**

The system supports WRR for eight queues. Each queue has a weight value (w7, w6, w5, w4, w3, w2, w1, and w0 in descending order of priority). The weight value represents the percentage of obtaining resources. WRR schedules queues in turn, which ensures that each queue can be scheduled.

Table 2-5 lists the mapping between queue weights and actual queues.

Table 2-5 Mapping between queue weights and actual queues

Queue No.	Configured Weight	Actual Queue Weight (Port Supporting Eight Queues)	Actual Queue Weight (Port Supporting Four Queues)
7	W7	W7	-
6	W6	W6	-
5	W5	W5	-
4	W4	W4	-
3	W3	W3	W7+W6
2	W2	W2	W5+W4
1	W1	W1	W3+W2
0	W0	W0	W1+W0

Wn: indicates the weight of queue *n*. The weight sum of all queues must be 0 or 100 (excluding the queue with the weight of 255).

- **PQ+WRR**

- The system uses the combination of PQ and WRR to schedule queues. When the specified WRR value is 0, PQ is used.
- PQ schedules high-priority queues.
- The weight sum of the scheduled queues must be equal to 100.

Procedure

Step 1 Run the **queue-scheduler** command to configure the queue scheduling mode.

Step 2 Run the **display queue-scheduler** command to view the configuration of the queue scheduling mode.

----End

Example

Configure the WRR scheduling mode and set the weight values of the eight queues to 10, 10, 20, 20, 10, 10, 10, and 10.

```
huawei(config)#queue-scheduler wrr 10 10 20 20 10 10 10 10
huawei(config)#display queue-scheduler
Queue scheduler mode : WRR
-----
Queue  Scheduler Mode  WRR Weight
-----
  0   WRR                10
  1   WRR                10
  2   WRR                20
  3   WRR                20
  4   WRR                10
  5   WRR                10
  6   WRR                10
  7   WRR                10
-----
```

Configure the PQ+WRR scheduling mode and set the weight values of the six queues to 20, 20, 10, 30, 10, and 10.

```
huawei(config)#queue-scheduler wrr 20 20 10 30 10 10 0 0
huawei(config)#display queue-scheduler
Queue scheduler mode : WRR
-----
Queue  Scheduler Mode  WRR Weight
-----
  0   WRR                20
  1   WRR                20
  2   WRR                10
  3   WRR                30
  4   WRR                10
  5   WRR                10
  6   PQ                 --
  7   PQ                 --
-----
```

Configuring the Mapping Between Queues and 802.1p Priorities

This section describes how to configure the mapping between queues and 802.1p priorities so that packets with different 802.1p priorities are mapped to the specified queues based on the mapping.

Context

- The configuration is valid for all the service boards in the system.
- [Table 2-6](#) lists the default mapping between queues and 802.1p priorities.

Table 2-6 Mapping between queues and 802.1p priorities

Queue No.	Actual Queue Number (Port Supporting Eight Queues)	Actual Queue Number (Port Supporting Four Queues)	802.1p Priority
7	7	3	7
6	6	3	6

Queue No.	Actual Queue Number (Port Supporting Eight Queues)	Actual Queue Number (Port Supporting Four Queues)	802.1p Priority
5	5	2	5
4	4	2	4
3	3	1	3
2	2	1	2
1	1	0	1
0	0	0	0

Procedure

- Step 1** Run the **cos-queue-map** command to configure the mapping between 802.1p priorities and queues.
- Step 2** Run the **display cos-queue-map** command to view the mapping between 802.1p priorities and queues.

----End

Example

Map 802.1p priority 0 to queue 0, 802.1p priority 1 to queue 2, and other 802.1p priorities to queue 6.

```

huawei(config)#cos-queue-map cos0 0 cos1 2 cos2 6 cos3 6 cos4 6 cos5 6 cos6 6 cos7
6
huawei(config)#display cos-queue-map
CoS and queue map:
-----
CoS          Queue ID
-----
0            0
1            2
2            6
3            6
4            6
5            6
6            6
7            6
-----

```

2.4.3 Configuring ACL-based Traffic Management

You can configure an ACL to classify traffic flexibly. After traffic is classified, take QoS actions for service traffic.

Controlling the Traffic Matching an ACL Rule

This section describes how to control the traffic matching an ACL rule on a specified port, and process the excess traffic, such as adding the DSCP priority or discarding packets directly.

Prerequisite

The ACL and the ACL rule have been configured, and the port where rate limiting is configured is working properly.

Background

- You must configure permit rules in an ACL.
- The rate limit must be a multiple of 64 kbit/s.

Procedure

Step 1 Run the **traffic-limit** command to control the traffic matching an ACL rule on a specified port. You can run this command to configure either of the following actions to be taken when the traffic received on the port exceeds the rate limit:

- **drop**: discards the excess traffic.
- **remark-dscp value**: re-marks the excess traffic with the DSCP priority.

Step 2 Run the **display qos-info traffic-limit port** command to view the rate limit on the specified port.

---End

Example

Set the rate limit of the traffic that matches ACL 2001 received on port 0/2/0 to 512 kbit/s, and add the DSCP priority (af1) to packets that exceed the rate limit.

```
huawei(config)#traffic-limit inbound ip-group 2001 512 exceed remark-dscp af1 port 0/2/0 //af1 represents the DSCP type. Assured Forwarding 1 service (10)
huawei(config)#display qos-info traffic-limit port 0/2/0
traffic-limit:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5      running
    Target rate: 512 Kbps
    Exceed action: remark-dscp af1
```

Adding a Priority to the Traffic Matching an ACL Rule

This section describes how to add a ToS, DSCP, or 802.1p priority to the traffic matching an ACL rule on a specified port so that the traffic can obtain the corresponding service.

Prerequisite

The ACL and the ACL rule have been configured, and the port where the priority is re-marked is working properly.

Background

- You must configure permit rules in an ACL.
- The ToS and the DSCP priorities cannot be configured simultaneously.

Procedure

- Step 1** Run the **traffic-priority** command to add a priority to the traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-priority port** command to view the configured priority.

----End

Example

Add a priority to the traffic that matches ACL 2001 received on port 0/2/0, and set the DSCP priority to 10 (af1) and the local priority to 0.

```
huawei(config)#traffic-priority inbound ip-group 2001 dscp af1 local-precedence 0
port 0/2/0
huawei(config)#display qos-info traffic-priority port 0/2/0
traffic-priority:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5 running
    Priority action: dscp af1 local-precedence 0
```

Collecting Statistics on the Traffic Matching an ACL Rule

This section describes how to collect statistics on the traffic matching an ACL rule so that you can analyze and monitor the traffic.

Prerequisite

The ACL and the ACL rule have been configured, and the port where traffic statistics is configured is working properly.

Background

You must configure permit rules in an ACL.

Procedure

- Step 1** Run the **traffic-statistic** command to enable the statistics on traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-mirror port** command to view the statistics on the traffic matching an ACL rule on a specified port.

----End

Example

Collect statistics on the traffic matching ACL 2001 received on port 0/2/0.

```
huawei(config)#traffic-statistic inbound ip-group 2001 port 0/2/0
huawei(config)#display qos-info traffic-statistic port 0/2/0
traffic-statistic:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5 running
    0 packet
```

Mirroring the Traffic Matching an ACL Rule

This section describes how to mirror the traffic matching an ACL rule on a port to a specified port. Mirroring does not affect packet transmission on the source port. You can monitor the traffic of the source port by analyzing the traffic passing the destination port.

Prerequisite

The ACL and the ACL rule have been configured, and the port where traffic mirroring is configured is working properly.

Background

- You must configure permit rules in an ACL.
- The destination port cannot be an aggregation port.
- The system supports only one destination port for mirroring and the destination port must be the uplink port.

Procedure

Step 1 Run the **traffic-mirror** command to mirror the traffic matching an ACL rule on a specified port.

Step 2 Run the **display qos-info traffic-mirror port** command to view information about the mirrored traffic matching an ACL rule on a specified port.

----End

Example

Mirror the traffic that matches ACL 2001 received on port 0/2/0 to port 0/2/1.

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/2/0 to port 0/2/1
huawei(config)#display qos-info traffic-mirror port 0/2/0
traffic-mirror:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5      running
    Mirror to: port 0/2/1
```

Configuring Redirection for the Traffic Matching an ACL Rule

This section describes how to redirect the traffic matching an ACL rule on a specified port. After this operation is executed successfully, the specified port forwards the traffic.

Prerequisites

The ACL and the ACL rule have been configured, and the port where redirection is configured is working properly.

Context

- You must configure permit rules in an ACL.
- Currently, the system can only redirect the traffic matching the ACL rule from service ports to uplink ports, and redirect the traffic matching the ACL rule from uplink ports to ports on the board of the same type.

Procedure

- Step 1** Run the **traffic-redirect** command to redirect the traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-redirect port** command to view the redirection information about the traffic matching an ACL rule on a specified port.
- End

Example

Redirect the traffic that matches ACL 2001 received on port 0/2/0 to port 0/2/16.

```
huawei(config)#traffic-redirect inbound ip-group 2001 port 0/2/0 to port 0/2/1
huawei(config)#display qos-info traffic-redirect port 0/2/0
traffic-redirect:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5      running
    Redirected to: port 0/2/1
```

3 Configuring the WLAN Service

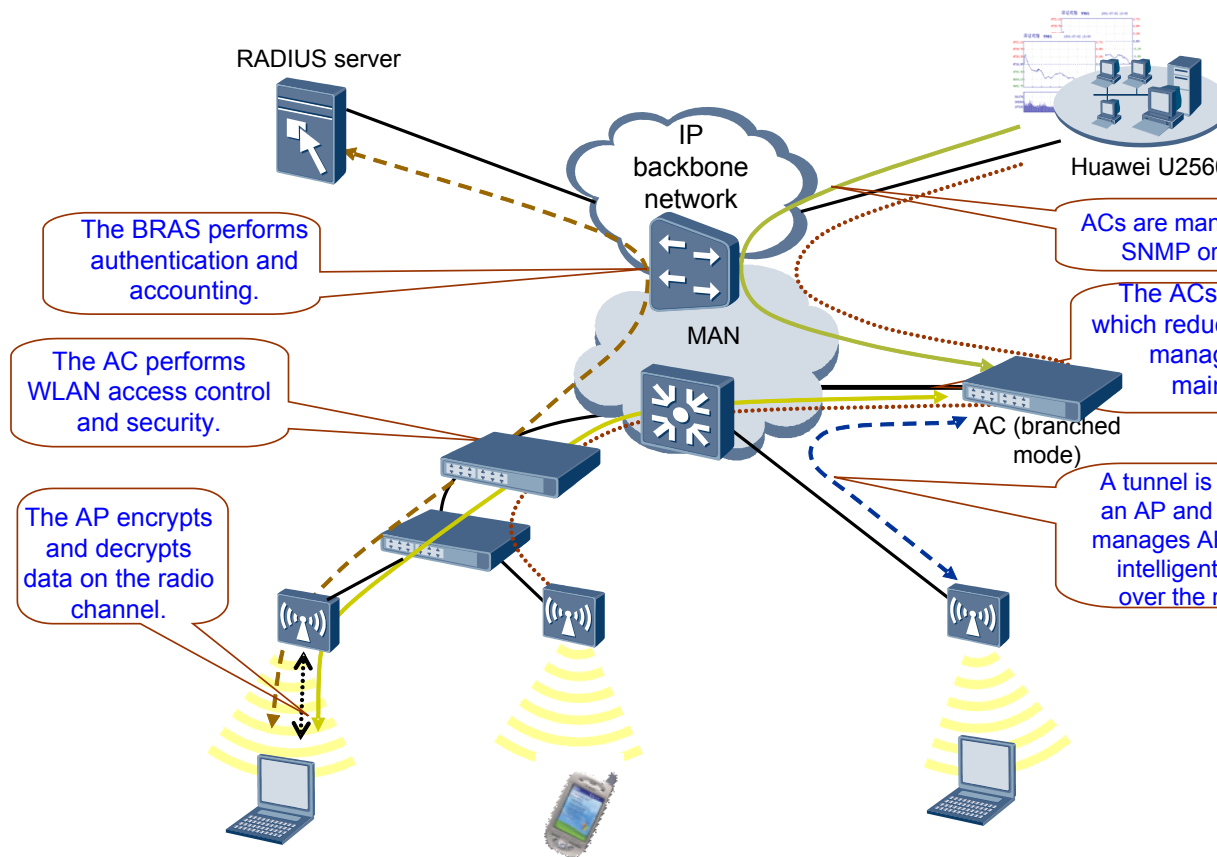
About This Chapter

This section describes how to configure the wireless local area network (WLAN) service in AC + fit AP networking mode. The following operations are performed on the AC system.

WLAN is developed based on computer networks and wireless telecommunications technologies. It implements the functions of a traditional wired LAN by using wireless multicast channels as transmission media and using electromagnetic waves for exchanging data.

Figure 3-1 shows an example network of a WLAN (AC + fit APs).

Figure 3-1 AC + fit AP networking mode



The data streams transferred to a wireless station (STA) from the Internet by using the WLAN access technologies are transmitted over two transmission media, namely, the wireless link between the STA and the AP and the wired link between the AP and the AC.

- The wired link between the AP and the AC is created in seven phases: the AP discovers the AC, the AP establishes a CAPWAP tunnel with the AC, the AP joins the AC, the AP updates its version, the AP updates its configuration, the AP checks its configuration, and the AP enters the running state. The phases are described as follows:
 1. After an AP is started, it can discover an AC in three modes: unicast, multicast, or broadcast. Generally, AC discovery by sending unicast packets can be implemented by DHCP discovery, DNS discovery, or static configuration.
 - DHCP mode: The AP obtains an IP address from the IP address pool of the AC by means of DHCP. The IP address allocated to the AP is carried in the Option 138, Option 43, or Option 189 field of a DHCP packet.
 - DNS mode: The AP obtains the IP address of the AC by means of DNS.
 - Static configuration: The IP address of the AC is configured statically on the AP.
 2. The AP negotiates with the AC according to the AC's IP address. After receiving the discovery response from the AC, the AP establishes a CAPWAP tunnel with the AC. The CAPWAP tunnel transmits UDP data packets by using the DTLS encryption.

3. After the CAPWAP tunnel is established, the AP negotiates with the AC by sending request and response messages. During the negotiation, the AC determines whether to allow the AP to join.
 4. According to the negotiated parameters, the AP checks whether its current version is the latest version. If the current version is not the latest one, the AP starts updating the software version on the CAPWAP tunnel. After updating the software version, the AP restarts, and performs AC discovery, establishes a CAPWAP tunnel, and joins the AC.
 5. After joining the AC, the AP sends a configuration status request to the AC, informing the AC of the current AP configuration (antenna, radio configuration, transmission rate, channel, and power). The AC replies with a configuration status response immediately to update the configuration requested by the AP.
 6. After the configuration is updated, the AP sends a status change request to inform the AC of the configuration update result. After learning about the configuration update result, the AC sends a response message to the AP.
 7. After the preceding steps are complete, the AP enters the normal state and starts working properly.
- The wireless link between the STA and the AP is created in three phases: the terminal scans the AP; the terminal is authenticated on the AP; the terminal is associated with the AP.
 1. Multiple APs on the WLAN periodically send Beacon frames. On each channel, the STA listens for the beacon frames sent by the APs and then selects an AP as its WLAN access device.
 2. After a STA is authenticated in 802.11 link authentication on the AP, it sends an association request to the AP. The AP forwards the association request to the AC. The AC determines whether to allow the STA to join and sends a site configuration request to the AP.
 3. The STA starts to dial up and gets 802.1x-authenticated, and then the STA associates with the AP.

3.1 Configuring an Carrier ID and an AC ID

To distinguish carriers and ACs, configure a unique ID for each carrier and AC.

3.2 Configuring the Layer 3 Interfaces

To ensure that an AP can communicate with an AC, you need to configure a VLAN interface, that is, a Layer 3 interface, on the AC to manage the AP.

3.3 Configuring the DHCP Server

If the IP address of an AP needs to be allocated by an AC, configure the DHCP server on the AC.

3.4 Configuring the Version Upgrade Mode for an AP

Before an AP starts working properly or after the AC version is changed, the AP and the AC negotiate the AP version that matches the current AC version. If the versions do not match, the AP starts an upgrade.

3.5 Configuring the Data Forwarding Mode

3.6 Adding an AP and Getting it Online

APs can be added offline, automatically, or manually.

3.7 Configuring a WLAN Radio

This section describes how to configure a WLAN radio. After an AP goes online, configure a radio profile for the AP.

[3.8 Configuring the ESS and VAP](#)

This section describes how to configure the extended service set (ESS) and virtual access point (VAP). After an AP goes online, you can set parameters for the VAP to complete the WLAN service configuration.

[3.9 Configuring a QoS Policy on a WLAN](#)

This section describes how to set QoS parameters for an AP and a STA on the AC so that the AC can provide differentiated services.

[3.10 Configuring a WLAN Security Policy](#)

This section describes how to configure a security policy for a WLAN network.

[3.11 Configuring 802.11n](#)

To increase the access rate for WLAN access users, you can configure 802.11n.

[3.12 Viewing AP Information](#)

This section describes how to view an AP's running status, authentication mode, and performance statistics.

3.1 Configuring an Carrier ID and an AC ID

To distinguish carriers and ACs, configure a unique ID for each carrier and AC.

Procedure

Step 1 Run the **wlan ac-global** command to number an AC for a carrier.

 **NOTE**

Currently, carriers are identified as cmcc (China Mobile), ctc (China Telecom), cuc (China Unicom), and other (other carriers).

---End

Example

Number an AC as 1 for China Telecom.

```
huawei (config) #wlan ac-global ac id 1 carrier id ctc
```

3.2 Configuring the Layer 3 Interfaces

To ensure that an AP can communicate with an AC, you need to configure a VLAN interface, that is, a Layer 3 interface, on the AC to manage the AP.

Context

If there are multiple management VLANs for APs, you need to configure multiple VLAN interfaces.

Procedure

Step 1 Run the **interface vlanif** command to create a VLANIF interface

Step 2 Run the **ip address** command to configure the IP address of the VLAN interface.

Step 3 Set the VLANIF interface as the source interface on the AC.

- If there is only one management VLAN, run the **wlan ac source interface vlanif** command to set the VLANIF interface as the source interface on the AC.

- If there are management VLANs, create a loopback interface to ensure that the APs connected to other VLAN IF interface can work normally when certain VLANIF interfaces are unavailable.

1. Run the **interface loopback** command to create a loopback interface,

2. Run the **ip address** command to configure the IP address of the Loopback interface.

3. Run the **wlan ac source interface loopback** command to set the loopback interface as the source interface on the AC.



CAUTION

The IP address of the loopback interface must use the 32-bit subnet mask and is used as the source IP address of the AC. This IP address is used for establishing a tunnel between the AP and the AC.

 **NOTE**

After the VLANIF interface and the loopback interface are bound successfully, packets sent to the loopback interface are forwarded to the device through the bound VLANIF interface.

---End

3.3 Configuring the DHCP Server

If the IP address of an AP needs to be allocated by an AC, configure the DHCP server on the AC.

Prerequisites

The DHCP server is configured on the VLANIF interface corresponding to the AP.

Procedure

Step 1 Run the **ip pool** command to create an IP address pool.

Step 2 Run the **gateway** command to configure the gateway address for the IP address pool. The gateway address must match the IP address of the VLANIF interface that manages the AP.

 **NOTE**

The gateway IP address in the IP address pool must be the same as the IP address of the VLANIF interface. After APs go online, they obtain IP addresses from this IP address pool.

Step 3 Run the **section** command to configure the address segment in the IP address pool.

Step 4 Run the **option** command to configure DHCP Option 60 and Option 43 to notify the AP of the AC's IP address by means of DHCP Option 43.



CAUTION

- If the AP needs to obtain the IP address of the AC, the Option field is optional for Layer 2 networking and mandatory for Layer 3 networking.
 - The text information must be **Huawei AP** for Option 60.
 - The text information must be **HuaweiAC-X.X.X.X** for Option 43. *X.X.X.X* indicates the IP address of the AC.
 - If multiple IP addresses are involved, separate the IP address in the text information for Option 43 by a comma, for example, **HuaweiAC-x.x.x.x,x.x.x.x**.
-

---End

Example

```
# Create an IP address pool, set its gateway address to 172.1.1.1/24 and its address segment from
172.1.1.2 to 172.1.1.124, and set the Option 43 field to HuaweiAC-172.1.1.1.
huawei(config)#ip pool ap-server
    It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.124
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-172.1.1.1
```

3.4 Configuring the Version Upgrade Mode for an AP

Before an AP starts working properly or after the AC version is changed, the AP and the AC negotiate the AP version that matches the current AC version. If the versions do not match, the AP starts an upgrade.

Context

An AP may be upgraded offline or online.

- Offline upgrade: When a newly registered AP detects that its version is earlier than the AP version on the AC or FTP server, it is upgraded automatically.
- Online upgrade: When a working AP detects that its version is earlier than the AP version on the AC or FTP server, it starts upgrade.

An AP supports two upgrade modes:

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

When configuring the version upgrade mode, pay attention to the following points:

- The AC or FTP upgrade mode must be preconfigured on the AC.
- In AC mode, a large number of version files can be configured on an AC for APs of the same type at a time, and a maximum of eight version files can be loaded at a time. In FTP mode, the number of version files loaded at a time is not limited.


NOTE

Currently, only version files can be loaded for only APs of the same type.

Procedure

- Configure the AC mode.
 1. In global config mode, run the **load file** command to load the upgrade file of the AP to the AC.
 2. In WLAN-AC mode, run the **ap-update mode** command to set the AP upgrade mode to **ac-mode**.
 3. In WLAN-AC mode, run the **ap-update update-filename** command to set the upgrade file name corresponding to the AP type.
 4. If an AP is upgraded online, you also need to perform the following operations:
 - a. Run the **ap-update multi-load** command to upgrade APs in batches according to the AP type.

- b. After the upgrade is complete, run the **ap-update multi-reset ap-type** command to reset the upgraded APs in batches.
- Configure the FTP mode.
 1. Run the **ap-update ftp-server** command to configure or change the IP address of the FTP server, and user name and password of the FTP client.

 **NOTE**
Save the upgrade file of the AP to a specified directory on the FTP server.
 2. In WLAN-AC mode, run the **ap-update mode** command to set the AP upgrade mode to **ftp-mode**.
 3. In WLAN-AC mode, run the **ap-update update-filename** command to set the upgrade file name corresponding to the AP type.
 4. If an AP is upgraded online, you also need to perform the following operations:
 - a. Run the **ap-update multi-load** command to upgrade APs in batches according to the AP type.
 - b. After the upgrade is complete, run the **ap-update multi-reset ap-type** command to reset the upgraded APs in batches.

----End

Example

On an AC, set the AP upgrade mode to **ac-mode** and the version file corresponding to AP WA601 to **ap_firmware.bin**.

```
huawei(config)#load file tftp 10.11.104.1 ap_firmware.bin
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-update mode ac-mode
huawei(config-wlan-ac-view)#ap-update update-filename ap_firmware.bin ap-type 0
huawei(config-wlan-ac-view)#ap-update multi-load ap-type 0
huawei(config-wlan-ac-view)#ap-update multi-reset ap-type 0
```

3.5 Configuring the Data Forwarding Mode

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Configure the data forwarding mode.

- Run the **forward-mode type { ess | ap }** command to set the forwarding mode to ESS-based or AP-based.
 - Run the **forward-mode ess *ssid* mode { direct-forward | tunnel }** command to set the data forwarding mode for the ESS to direct forwarding or tunnel forwarding.
 - Run the **forward-mode ap by-region *region* mode { direct-forward | tunnel }** command to set the data forwarding mode for the AP region to direct forwarding or tunnel forwarding.
 - Run the **forward-mode ap *apid-list* mode { direct-forward | tunnel }** command to set the data forwarding mode for the AP to direct forwarding or tunnel forwarding.

Step 3 Run the **display forward-mode** command to view the data frame forwarding mode of an AP or a service set.

----End

3.6 Adding an AP and Getting it Online

APs can be added offline, automatically, or manually.

Prerequisites

- The basic functions of the AC have been configured.
- The AP and the AC are connected properly.

Context

- Getting an AP online involves the following scenarios:
 - If the AP has been added offline, it can go online directly.
 - If the AP is not added offline but its authentication mode is "no-auth" or it is in the whitelist, the AP can be added automatically and go online.
 - If the AP is neither in the blacklist nor in the whitelist or AP list and its authentication mode is not "no-auth", the AP is not allowed to go online and it will be recorded in the list of unauthenticated APs. In this case, manually confirm the list of unauthenticated APs to add the AP.
- Requirements on the AP type:
 - The AP type must be unique and must be the same as the type of the actual AP; otherwise, the AP fails to go online.
 - When the AP is getting online, the AC checks whether the AP type is in the configured AP list. If the AP type is not in the list, the AP fails to go online.
- AP region:
 - To go online, an AP must be added to only one AP region.
 - By default, there is an AP region in the system. When an AP is getting online, it is automatically added to the default AP region. You can specify any existing region as the default region.
- AP profile: To go online, an AP must be bound to only one AP profile.

Procedure

Step 1 Add the AP type, that is, the type of the AP that is going online, to the AP type list on the AC.

1. Run the **wlan ac** command to enter the WLAN-AC mode.
2. Run the **display ap-type** command to check whether the type of the AP is in the AP type list.
3. If the AP type is not in the AP type list, run the **ap-type** command to add the AP type.

 **NOTE**

By default, the AP type list contains WA601, WA631, WA651, WA602, WA632, WA652, WA603SN, WA603DN, WA633SN, WA603DE, WA653DE and WA653SN.

Step 2 Add the AP.

- Offline:
 1. Run the **ap-auth-mode** command to specify that the AP is authenticated according to the MAC or SN when it is getting online.
 2. Run the **ap** command to add the AP offline. Set the AP ID according to the preset value and enter **mac-auth** or **sn-auth** according to the authentication mode.
 3. Get the AP online. The AP enters the **normal** state after it goes online.
- Automatically
 1. Run the **ap-auth-mode** command to specify that the AP is not authenticated when getting online, or run the **ap-whitelist** command to add the MAC address or SN of the AP to the whitelist if the AP is legal.
 2. Get the AP online. The AP enters the **normal** state after it goes online.

**NOTE**

If you do not want to get the AP online, run the **ap-blacklist** command to add the AP to the blacklist.

- Manually
 1. Run the **ap-confirm** command to confirm the AP in the unauthenticated AP list. If the AP is confirmed successfully, it enters the **normal** state.

Step 3 (Optional) Run the **ap-region** command to create an AP region to facilitate AP management. If no AP region is created, the system uses the default AP region. To add the AP to a specified region, run the **region-id** command.

Step 4 (Optional) Run the **ap-profile** command to create an AP profile and set parameters including the MTU, log server address, and backup mode in the AP profile. To bind the AP to a specified profile, run the **profile-id** command.

Step 5 Check whether the AP is added successfully.

Run the **display ap** command to view the status of the added AP.

```
huawei(config-wlan-ac-view)#display ap all
```

```
All AP information:
```

```
-----  
AP      AP      Profile  Region  AP  
ID      Type                               ID      ID      State  
-----  
0       WA631   0        0       fault  
1       WA601   1        101    normal  
2       WA601   0        102    normal  
3       WA632   0        0       fault  
-----
```

```
Total number: 4
```

----End

3.7 Configuring a WLAN Radio

This section describes how to configure a WLAN radio. After an AP goes online, configure a radio profile for the AP.

Context

After an AP goes online and starts working, the system creates radios for the AP by default. The system can create a maximum of four radios for an AP. Currently, the radio 0 is 2.4 GHz and the radio 1 is 5 GHz.

3.7.1 Configuring a Radio Profile

You need to bind a radio profile to a WMM profile and set parameters in the radio profile according to the configuration wizard.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Run the **radio-profile** command to create a radio profile.

 **NOTE**

After a radio profile is created, parameters in the radio profile are set to the default values.

Step 3 Run the **display radio-profile** command to view the parameters in the radio profile.

Create radio profile **radio-profile-1** and use default parameter settings.

```
huawei(config-wlan-ac-view)#radio-profile name radio-profile-1 id 1
huawei(config-wlan-radio-prof-radio-profile-1)#display radio-profile name radio-profile-1
```

```
-----
Profile ID                :1
Profile name              :radio-profile-1
Radio type                :802.11b/g
Rate mode                 :auto
Rate (Mbps)              :54
Channel mode              :auto
Power mode                :auto
Calibrate interval(min)  :720
PER threshold(%)         :30
Conflict rate threshold(%) :60
RTS/CTS threshold(Byte)  :2347
Fragmentation threshold(Byte) :2346
Short retry number limit  :7
Long retry number limit  :4
Support short preamble    :support
DTIM interval (Beacon interval numbers):3
Beacon interval (time unit) :1000
WMM profile ID           :-
WMM profile name         :-
Interference detect switch :disable
Calibrate switch         :enable
Common frequency disturb threshold(%) :50
Adjacent frequency disturb threshold(%) :50
Station disturb threshold :32
802.11n guard interval mode :normal
802.11n A-MPDU length limit :3
-----
```

Step 4 (Optional) Run the **radio-type** command to change the radio type in the radio profile.

 **NOTE**

- The default value of **radio-type** is **80211bg**.
- If the new radio type is not supported by a radio that is bound to the radio profile, the change fails.
- If the new radio type conflicts with the rate-specific parameters, the change fails. For example, if you change the radio type to 802.11b but the designated rate mode is used and the designated rate is 54 Mbit/s, the change fails.

Step 5 (Optional) Run the **rate auto max-rate rate-value** command to set rate-specific parameters in the radio profile.

 **NOTE**

To use the automatic rate mode and the maximum rate, run the **rate auto max-rate rate-value** command. In automatic rate mode, the radio bound to the profile can use any rate that does not exceed the maximum rate.

Step 6 (Optional) Run the **power-mode** command to configure the power mode in the radio profile.

 **NOTE**

The default value of **power-mode** is **auto**. In automatic power mode, the power is adjusted automatically according to the radio environment.

Step 7 (Optional) Run the **channel-mode** command to configure the channel mode in the radio profile.

 **NOTE**

The default value of **channel-mode** is **auto**. In automatic channel mode, the channel is adjusted automatically according to the radio environment. This mode is recommended.

Step 8 Run the **bind wmm-profile** command to bind a WMM profile to the radio profile.

Bind radio profile **radio-profile-1** to WMM profile **wmm-profile-1**.

```
huawei(config-wlan-radio-prof-radio-profile-1)#bind wmm-profile name wmm-profile-1
huawei(config-wlan-radio-prof-radio-profile-1)#display radio-profile name radio-
profile-1
```

```
-----
Profile ID                :1
Profile name              :radio-profile-1
.....
WMM profile ID           :1
WMM profile name         :wmm-profile-1
.....
-----
```

 **NOTE**

Before being bound to a radio, a radio profile must be bound to a WMM profile.

----End

3.7.2 Binding a Radio Profile to a Radio

When a radio is bound to a radio profile, it will use the settings in the profile.

Context

A radio profile includes the following parameters: radio type, radio rate, radio channel mode, radio power mode, radio calibration interval, packet loss threshold, error packet ratio threshold, conflict ratio threshold, segment threshold, RTS/CTS threshold, short/long frame retransmission threshold, short preamble status, DTIM period, Beacon frame period, and WMM parameter.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Run the **radio** command to enter the radio mode.

Step 3 Run the **bind radio-profile** command to bind a radio profile to the specified radio.

Step 4 Run the **display binding radio-profile** command to view the binding of the radio profile.

Display the binding status of radio profile **huawei**.

```
huawei(config-wlan-ac-view)#display binding radio-profile name radio-profile-1
```

```
-----
AP  RADIO
-----
1   0
-----
Total: 1
```

----End

Example

```
# Bind radio profile radio-profile-1 to radio 0 of AP1.
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #radio ap-id 1 radio-id 0
huawei (config-wlan-radio-1/0) #bind radio-profile name radio-profile-1
```

3.7.3 Configuring the Radio Calibration Function for an AP Region

To prevent radio signals in an AP region from deteriorating, configure the global radio calibration function for this region.

Context

The calibration function ensures that the transmit power of a radio does not interfere the transmit power of another radio.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Configure the radio calibration function.

- To enable global radio calibration for a specified region, run the **calibrate startup** command.
- To start radio calibration at scheduled time, run the **calibrate auto-startup** command.

 **NOTE**

To detect unauthorized neighbors during calibration, add the **listen-uncontrol-neighbor** parameter to the commands in step 2.

----**End**

Example

```
# Configure the system to start global radio calibration in AP region 3 at 2:00 a.m. every day
and to monitor unauthorized neighbors during global calibration.
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #calibrate auto-startup region 3 time 2:0:0 listen-
uncontrol-neighbor
```

3.7.4 (Optional) Configuring AP Radio Resource Management

AP radio resource management includes adjusting channels and transmit power and detecting and eliminating coverage holes.

Context

In auto mode, an AP automatically selects a channel or sets the transmit power for a radio based on the WLAN radio environment. The auto mode and manual mode are exclusive; therefore, you can select only one mode at a time.

Procedure

Step 1 If the AP is configured with a radio profile, run the **channel-mode auto** command to enable the automatic channel mode in the radio profile. In this mode, the AP can select a proper channel or adjust the current channel according to the radio environment. By default, the automatic channel mode is used.

 **NOTE**

An AC periodically instructs APs to check the network environment so that the APs can determine whether to adjust channels and how to adjust channels accordingly.

- Step 2** If the AP is configured with a radio profile, run the **power-mode auto** command to enable the automatic power mode. In this mode, the AP can select a proper power value or adjust the current power value according to the radio environment.

 **NOTE**

An AC periodically instructs APs to collect information about neighbors so that the APs can determine whether to adjust the transmit power to ensure that the entire WLAN area is covered.

- Step 3** A coverage hole is generated when an AP is removed or signals are blocked by an obstacle. An AC periodically checks for coverage holes. If the AC detects a coverage hole, it calibrates radios to eliminate the coverage hole.

----End

3.7.5 (Optional) Configuring an AP Load Balancing Group

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

Context

On a WLAN in centralized control mode, the association between a STA and an AP must be permitted by the corresponding AC. In practice, a STA scans APs and sends association requests to the APs. Regardless of the MAC address that is used, the APs forward the association requests to the AC. Then, according to the AC's policies, the AC will determine which AP is the best for the STA to associate with.

Procedure

- Step 1** Run the **wlan ac** command to enter the WLAN-AC mode.
- Step 2** Run the **load-balance group** command to create a load balancing group and enter the configuration view of the group.
1. Run the **member** command to add a radio to the load balancing group. When a STA wants to associate with the radio, the AC checks the traffic on this radio and other working radios in the group to determine whether the STA can be associated with the radio.
 2. (Optional) Run the **traffic gap** command to set the load balancing mode to traffic mode.
 3. (Optional) Run the **session gap** command to set the load balancing mode to session mode.
 4. Run the **associate-threshold** command to set the maximum number of association requests.

 **NOTE**

The default parameter settings are used for a new load balancing group unless they are modified by users.

----End

3.8 Configuring the ESS and VAP

This section describes how to configure the extended service set (ESS) and virtual access point (VAP). After an AP goes online, you can set parameters for the VAP to complete the WLAN service configuration.

3.8.1 Configuring an ESS

An ESS defines service parameters and VAP attributes. After an ESS is bound to the specified radio of an AP, all its service parameters are applied to the corresponding VAP.

Prerequisite

A security profile and a traffic profile have been configured.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Run the **ess** command to create an ESS.

```
# Create an ESS named huawei and set its SSID to huawei-1, IGMP mode to snooping, traffic profile to huawei, security profile to huawei, and other parameters to default settings.  
huawei(config-wlan-ac-view)#ess name huawei ssid huawei-1 traffic-profile huawei security-profile huawei igmp-mode snooping
```

Step 3 Run the **vlan-mapping** command to configure the VLAN mapping mode and the VLAN ID.

NOTE

- To configure the same VLAN ID for upstream service packets of the VAP bound to the ESS, set the ESS's service VLAN mode to **ess-mode**.
- To differentiate services by AP, set the ESS's service VLAN mode to **ap-mode**.
- To differentiate services by AP region, set the ESS's service VLAN mode to **region-mode**.

Step 4 Run the **display ess** command to check the attributes configured for the ESS.

```
# Display the attributes in ESS huawei.  
huawei(config-wlan-ac-view)#display ess name huawei  
-----  
ESS ID: 17  
ESS name: huawei  
SSID: huawei-1  
Hide SSID: disable  
User isolate: enable  
Type: service  
Maximum number of user: 32  
User association time out: 5 minutes  
Traffic profile name: huawei  
Security profile name: huawei  
IGMP mode: snooping  
-----
```

Step 5 Run the **display vlan-mapping ess** command to check the VLAN configured for the ESS.

```
huawei(config-wlan-ac-view)#display vlan-mapping ess name huawei  
-----  
ESS ID           : 17  
ESS Name         : huawei  
VLAN Mapping Mode : Region Mode  
Region ID to VLAN ID Mapping List:  
-----  
Region ID      VLAN ID  
101            101  
-----  
Total: 1  
Remark:Other Regions in this ESS use default VLAN ID 1
```

----End

Example

```
# Create an ESS named huawei, set its SSID to huawei-1, IGMP mode to snooping, traffic
profile to huawei, security profile to huawei, and VLAN mapping mode to AP region mapping,
and map AP region 101 to VLAN 101. Use the default settings for other parameters.
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ess name huawei ssid huawei-1 traffic-profile huawei
security-profile huawei igmp-mode snooping
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei type tag region 101 vlan
101
```

3.8.2 Configuring a VAP and Binding an ESS to the VAP

When a VAP is delivered to an AP, parameter settings in the ESS that is bound to the VAP are delivered to the AP as VAP parameters, which then provide services for users based on the VAP parameters.

Context

A VAP is a WLAN service entity. You can create a VAP on a radio by binding an ESS to the radio. Run the **commit** command to deliver VAP parameters to APs.

Prerequisite

- A radio profile has been bound to the specified radio according to [3.7.2 Binding a Radio Profile to a Radio](#).
- ESS parameters have been configured according to [3.8.1 Configuring an ESS](#).

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Create VAPs.

- Create a single VAP and bind an ESS to the VAP.
 1. Run the **vap ap** command to bind an ESS to a radio of an AP.
 2. Run the **commit** command to commit the configuration of the specified AP.
- Create VAPs in batches and bind an ESS to the VAPs.

NOTE

Pre-configuration can be regarded as offline configuration and batch configuration. You need to create all required profiles in the pre-configuration stage. The profiles will be bound to the VAPs subsequently created. The binding process is the same as the process of real-time online configuration. Because no AP entity exists in the case of offline configuration, you do not need to create VAPs here. After the preceding offline configuration is finished for the AP of the corresponding type, when the AP goes online, the AP will batch issue the VAP parameters according to the AP type, radio ID, radio profile, ESS profile, and AP domain.

Run the **service-batch ap-type** command to bind the radio profile and ESS to a specified radio of the APs of a specified type.

----End

Example

```
# Configure the VAP on AP1 and set the ESS name to huawei.
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei
huawei(config-wlan-ac-view)#commit ap 1
```

```
# Bind radio profile 1 and ESS 2 to the AP WA601.
huawei(config-wlan-ac-view)#service-batch ap-type name wa601 radio 0 radio-
profile
id 1 ess id 2
```

3.9 Configuring a QoS Policy on a WLAN

This section describes how to set QoS parameters for an AP and a STA on the AC so that the AC can provide differentiated services.

3.9.1 Configuring a Radio QoS Policy

To configure a QoS policy, create a WMM profile and bind the WMM profile to a radio profile.

Context

WMM provides QoS features for 802.11 networks and enables high-priority packets to be sent first, ensuring the quality of voice and video services on WLANs.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Run the **wmm-profile { id profile-id | name profile-name }** * command to create a WMM profile.

NOTE

After the WMM profile is created successfully, it uses the default parameter settings.

Step 3 Run the **display wmm-profile { all | id profile-id | name profile-name }** command to view the parameters in the WMM profile.

Create WMM profile **wmm-profile-1** and use default parameter settings.

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-profile-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)#display wmm-profile name wmm-profile-1
```

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


 **NOTE**

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

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

You can change the priorities of the queues by modifying the Enhanced Distributed Channel Access (EDCA) parameters, including the arbitration inter Frame spacing number (AIFSN), exponent form of CWmin (ECWmin), exponent form of CWmax (ECWmax), transmission opportunity limit (TXOPLimit), and ACK policy:

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

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

Step 4 (Optional) Run the **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw** **ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplmit** *txoplmit-value* } * command to set EDCA parameters for four WMM queues of a STA.

Step 5 (Optional) Run the **wmm edca ap** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw** **ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplmit** *txoplmit-value* | **ack-policy** { **normal** | **noack** } } * command to set EDCA parameters and ACK policies for four WMM queues of an AP.

----End

3.9.2 Configuring a VAP QoS Policy

To configure a QoS policy for a VAP, create a traffic profile.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Run the **traffic-profile** { **name** *profile-name* | **id** *profile-id* } * command to create a traffic profile.

 **NOTE**

After the traffic profile is created successfully, it uses the default parameter settings.

Step 3 (Optional) Run the **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* } command to configure an 802.1p priority for upstream 802.3 packets sent from an AP or map a user priority to an 802.1p priority.

Step 4 (Optional) Run the **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7* command to configure mappings from 802.1p priorities to user priorities.

Step 5 Run the **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the parameters in the traffic profile.

Display parameters in traffic profile **huawei**.

```

huawei(config-wlan-ac-view)#traffic-profile name huawei id 1
huawei(config-wlan-traffic-prof-huawei)#display traffic-profile name huawei
Profile ID                : 1
Profile name              : huawei
Client Limit Rate(up)    : -
VAP Limit Rate(up)       : -
Client Limit Rate(down)  : -
VAP Limit Rate(down)     : -
802.1p Mapping Mode      : mapping
-----
User-priority  802.1p
0               0
1               1
2               2
3               3
4               4
5               5
6               6
7               7
-----
802.1p to User-priority Mapping List:
-----
802.1p  User-priority
0        0
1        1
2        2
3        3
4        4
5        5
6        6
7        7
-----
Tunnel priority(up) Mapping Mode:tos(inner) to tos(outer)
-----
TOS(inner)    TOS(outer)
0              0
1              1
2              2
3              3
4              4
5              5
6              6
7              7
-----
Tunnel priority(down) Mapping Mode:tos(inner) to tos(outer)
-----
TOS(inner)    TOS(outer)
0              0
1              1
2              2
3              3
4              4
5              5
6              6
7              7
-----
    
```

 **NOTE**

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

When receiving an 802.3 packet from the Ethernet network, the AP converts the 802.3 packet to an 802.11 packet and forwards it to the STA. The user priority in the packet is determined based on the mappings between DSCP priorities and CoS values or the setting in a traffic classifier.

Step 6 (Optional) Run the **tunnel-priority { up | down } designate { tos | 8021p } priority-value** command to configure the upstream or downstream tunnel priority.

Step 7 (Optional) Run the **rate-limit { client | vap } { up | down } ratelimit-value** command to configure the upstream or downstream rate.

---End

3.10 Configuring a WLAN Security Policy

This section describes how to configure a security policy for a WLAN network.

Context

A WLAN security policy is used to:

- Control STAs' access to the WLAN network by means of open-system authentication or shared-key authentication.
- Secure the data transmission by using an encryption method such as static Wired Equivalent Privacy (WEP), 802.1X dynamic WEP, temporary key integrity protocol (TKIP), network-layer encryption protocol, and CTR with CBC-MAC Protocol (CCMP) in which CTR stands for counter mode, CBC stands for cipher-block chaining, and MAC stands for message authentication code.

To configure a security policy for a WLAN, you need to configure a security profile and make it referenced by an ESS to take effect.

Procedure

Step 1 Run the **wlan ac** command to enter the WLAN-AC mode.

Step 2 Run the **security-profile { id profile-id | name profile-name } *** command to configure a security profile.

After the profile is created, it uses the default policy settings, as shown in [Table 3-1](#).

Table 3-1 Default policy settings in a security profile

Security Policy	Authentication Mode	Encryption Mode
WEP	Open-system authentication	Null key
WPA1	802.1x+PEAP	TKIP
WPA2	802.1x+PEAP	CCMP
WAPI	WAI	WPI

Step 3 The specific configuration process is as follows:

- Open-system authentication:
 1. Run the **security-profile { id profile-id | name profile-name } *** command to enter the specified security profile mode.

2. Run the **authentication policy wep** command to specify WEP authentication for the security profile.
 3. Run the **policy wep open-system** command to specify Open-system authentication for the specified security profile mode.
- Shared key authentication:
 1. Run the **security-profile { id profile-id | name profile-name } *** command to enter the specified security profile mode.
 2. Run the **authentication policy wep** command to specify WEP authentication for the security profile.
 3. Run the **policy wep share-key** command to specify shared key authentication for the specified security profile mode.
 4. Run the **wep key { wep-40 | wep-104 } { pass-phrase | hex } key-id key-value** command to configure the WEP key.

 **NOTE**

In WEP-40 mode, a key consists of 10 hexadecimal characters or 5 ASCII characters. In WEP-104 mode, a key consists of 26 hexadecimal characters or 13 ASCII characters.

5. Run the **wep default-key key-id** command to configure the default key index.
- WPA1/WPA2 authentication:

 **NOTE**

Enable 802.1x and global MAC address-based control for 802.1x when WPA1/WPA2+PSK/802.1x authentication is used. In WPA1/WPA2+PSK authentication mode, the PSK must be transmitted in EAPoL packets. Therefore, 802.1x must be enabled.

1. Run the **dot1x enable** command to enable 802.1x.
 2. Run the **dot1x mac-control** command to enable global MAC address-based control for 802.1x.
 3. Run the **wlan ac** command to enter the WLAN-AC mode.
 4. Run the **security-profile { id profile-id | name profile-name } *** command to enter the specified security profile mode.
 5. Run the **authentication policy { wpa1 | wpa2 }** command to configure the access security profile as WPA1/WPA2 authentication.
 6. Configure the authentication and encryption modes for the WPA/WPA2 security policy:
 - If preshared key authentication is used, run: **policy { wpa1-psk | wpa2-psk } { tkip | ccmp } { pass-phrase | hex } <key>**
 - If 802.1x authentication is used, run: **policy { wpa1 | wpa2 } { tkip | ccmp } 802dot1x { peap | sim }**
- WAPI authentication:
 1. Run the **security-profile { id profile-id | name profile-name } *** command to enter the specified security profile mode.
 2. Run the **authentication policy wapi** command to specify WAPI authentication for the security profile.
 3. Configure the authentication and encryption modes for the WAPI security policy:
 - If preshared key authentication is used:
 - a. Run: **wapi wai psk { pass-phrase | hex } key**
 - If certificate authentication is used:

 **NOTE**

Before enabling certificate authentication, you need to download AC and AP certificate files.

- a. Run the **wapi wai certificate** command to configure the WAPI authentication mode and encryption mode.
- b. Run the **wapi certification { ac | asu | issuer } import file-name file_name** command to import the AC certificate file, AC private key file, and ASU certificate file to bind the certificate file and the security profile.
- c. (Optional) Run the **wapi private-key import file-name file_name** command to import the AC private key file if the AC certificate contains no key file.
- d. Run the **wapi asu-server ip ip-addr** command to configure an IP address for the ASU server so that an AC can send the certificate to the ASU server if WAPI certificate authentication is configured.

Step 4 Run the **display security-profile { all | { id profile-id | name profile-name } [detail] }** command to view the configured security profile.

----End

Example

```
# Specify WAPI authentication and the certificate authentication mode for security profile
security-5. Set the IP address of the ASU server to 10.10.10.1, AC authentication certificate to
huawei-ac.cer, ASU authentication certificate to huawei-asu.cer, private key file of the AC
certificate to ac-key.key, and authentication certificate of the issuer to huawei-issuer.cer.
huawei(config-wlan-ac-view)#security-profile name security-5
huawei(config-wlan-security-prof-security-5)#wapi wai certificate
huawei(config-wlan-security-prof-security-5)#wapi asu-server ip 10.10.10.1
huawei(config-wlan-security-prof-security-5)#wapi certificate ac import file-name
huawei
-ac.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate issuer import file-
name hua
wei-issuer.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate asu import file-name
huawe
i-asu.cer
huawei(config-wlan-security-prof-security-5)#wapi private-key import file-name ac-
key.key...//
huawei(config-wlan-security-prof-security-5)#authentication policy wapi
huawei(config-wlan-security-prof-security-5)#quit
```

3.11 Configuring 802.11n

To increase the access rate for WLAN access users, you can configure 802.11n.

Context

As a new member in the 802.11 protocol family, 802.11n supports 2.4 GHz and 5 GHz frequency bands and provides two methods of increasing the communication rate: increasing bandwidth and improving channel usage.

- Increasing bandwidth: 802.11n binds two 20 MHz channels to form a 40 MHz channel for doubling the transmission rate and improving the throughput of the wireless network. In actual applications, the two bound 20 MHz channels can also be used as two separate channels, one as the primary channel and the other as the secondary channel. Therefore,

either a 40 MHz channel or a single 20 MHz channel can be used for transmitting and receiving data.

- Increasing channel usage:
 1. 802.11n uses the Aggregated MAC Protocol Data Unit (A-MPDU) frame format and aggregates multiple MAC protocol data units (MPDU) to one A-MPDU, with only one PHY header retained. This reduces the transmission of additional information contained in PHY headers and the number of ACK frames. Therefore, it lightens the load of protocols and increases the network throughput.
 2. 802.11n optimizes resources at the physical layer and support the short guard interval (GI) function. A common GI is 800 ns; a short GI is 400 ns. Using the short GI can improve 802.11n transmission rate by 10%.

Procedure

- Step 1** Run the **wlan ac** command to enter the WLAN-AC mode.
- Step 2** Run the following command to create a radio profile: **radio-profile** { *id profile-id* | **name profile-name** } *
- Step 3** Run the following command to set the radio type: **radio-type** { **80211an** | **80211bgn** | **80211gn** | **80211n** }
- Step 4** Run the following command to configure the GI mode: **80211n guard-interval-mode** { **short** | **normal** }
- Step 5** Run the following command to configure the length of frames aggregated in an A-MPDU: **80211n a-mpdu max-length-exponent** *exponent-value*
- Step 6** Run the following command to quit the radio profile view: **quit**
- Step 7** Run the following command to enter the radio mode: **radio ap-id** *ap-id* **radio-id** *radio-id*
- Step 8** Run the following command to configure the channel and channel frequency of the AP: **channel** { **20MHz** | **40MHz-minus** | **40MHz-plus** } *channel*
- Step 9** Run the following command to configure the MCS value of the 802.11n radio: **80211n mcs** *mcs-value* is configured.
- Step 10** Run the **radio enable** command to enable the radio.
- End

3.12 Viewing AP Information

This section describes how to view an AP's running status, authentication mode, and performance statistics.

Context

During routine maintenance, you can run the following commands in any view to learn about the running status of an AP.

Procedure

- Run the **display ap** command to check the ID, MAC address, SN, and working status of the AP.
- Run the **display ap-auth-mode** command to check the authentication mode of the AP.
- Run the **display ap-performance-statistic** command to check the performance statistics on the AP.
- Run the **display ap-profile** command to check the configuration profile of the AP.
- Run the **display ap-region** command to check information about the AP region.
- Run the **display ap-run-info** command to check running information about the AP.
- Run the **display ap-type** command to check the type of the AP.

----End

4 Configuring WLAN Services

About This Chapter

This section describes how to configure QoS policies, security policies, and service parameters for different WLAN networking scenarios.

[4.1 WLAN Networking](#)

There are two typical networking modes for a WLAN: chain networking and branched networking.

[4.2 WLAN Service Configuration Procedure](#)

This section describes the procedure for configuring the basic WLAN services.

[4.3 Example for Configuring the WLAN Service](#)

This section provides examples of typical WLAN service configuration in AC + fit AP networking mode.

4.1 WLAN Networking

There are two typical networking modes for a WLAN: chain networking and branched networking.

Context

- In chain networking mode, there is a CAPWAP tunnel between an AC and AP; the AC is directly connected to a broadband remote access server (BRAS) and forwards and processes the management and service data of the AP.

In this mode, the AC has powerful forwarding capabilities and provides aggregation layer functions. The chain networking mode simplifies the network architecture and applies to scenario where a great number of APs are deployed in centralized manner.

- In branched networking mode, an AC is not directly connected to a BRAS. It only manages APs and does not forward the AP service data.

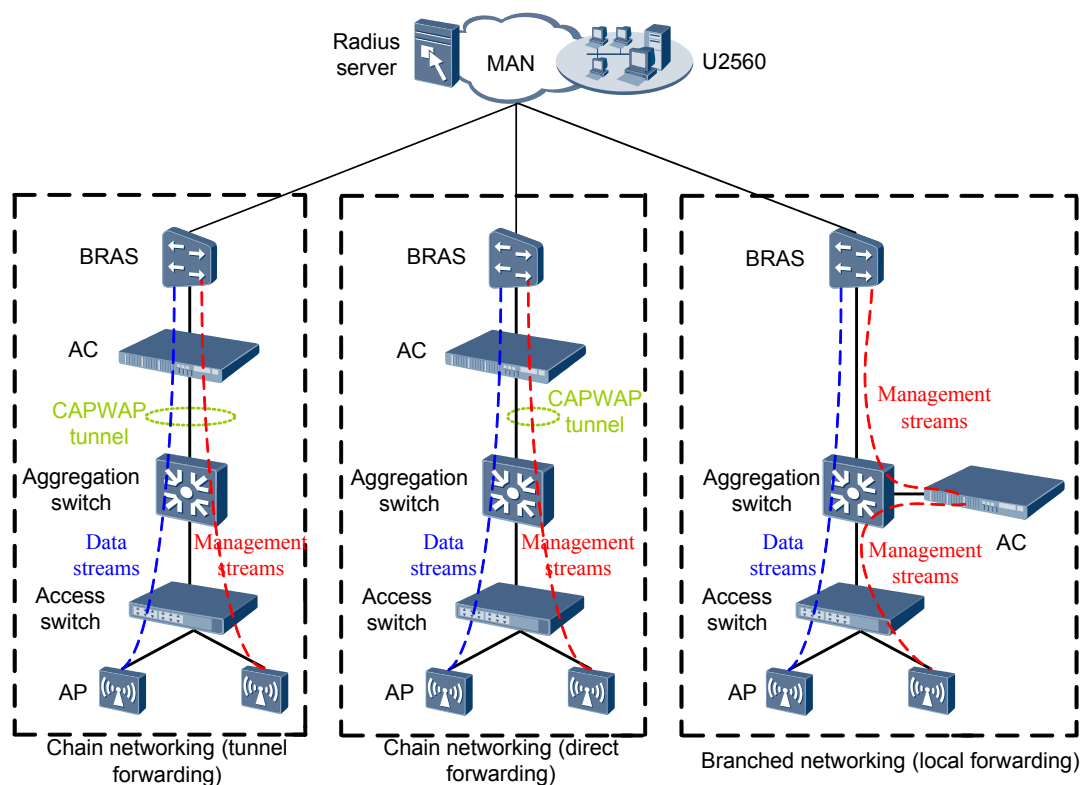
In this mode, the AC manages all APs connected to the BRAS. The branched networking mode is applicable to scenarios where APs are scattered in hot spots of a city.

Network Diagram

Figure 4-1 shows the typical WLAN network topologies.

- Chain networking (service data forwarded with a tunnel): Management and service data flows of an AP are encapsulated in the CAPWAP tunnel and forwarded by the AC. The service data flows are differentiated by VLAN IDs.
- Chain networking (direct forwarding): Management data flows of an AP are transmitted over the CAPWAP tunnel, but service data flows are sent to the AC directly, not through the tunnel.
- Branched networking (local forwarding): Management data flows of an AP must be processed by an AC. Service data flows of the AP, however, are directly sent to the BRAS without being forwarded by the AC.

Figure 4-1 Typical WLAN network topologies



4.2 WLAN Service Configuration Procedure

This section describes the procedure for configuring the basic WLAN services.

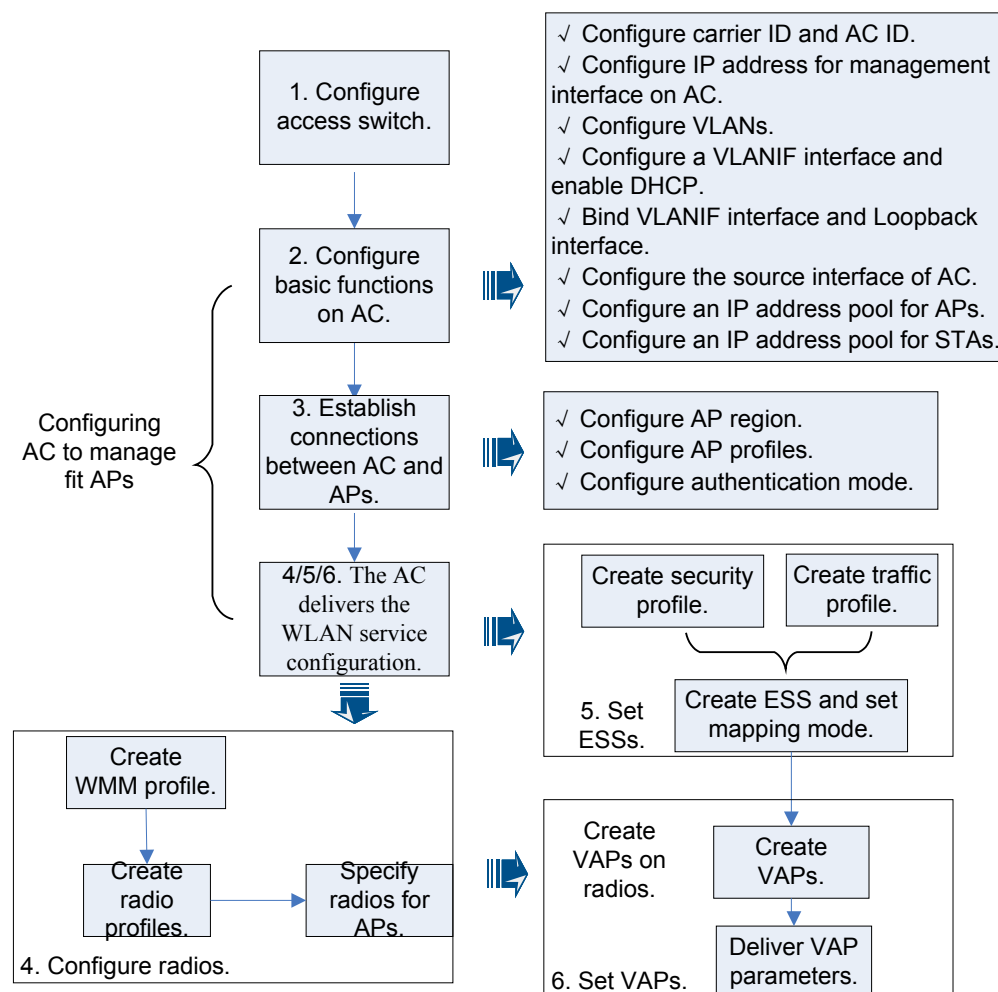
Procedure

Figure 4-2 shows the WLAN service configuration flowchart, which involves the following steps:

1. Configure the upper-layer switch connected to APs.
2. Configure basic functions on the AC.
3. Establish connections between the AC and the APs.
4. Configure radios for APs.
5. Configure ESSs for APs.
6. Configure VAPs for APs and deliver VAP parameters.

For detailed configuration, see the configuration examples.

Figure 4-2 WLAN service configuration flowchart



4.3 Example for Configuring the WLAN Service

This section provides examples of typical WLAN service configuration in AC + fit AP networking mode.

4.3.1 Example for Configuring Services for Layer 2 Chain Networking (Data Forwarded by Tunnel)

The chain networking mode simplifies the network architecture and applies to scenario where a great number of APs are deployed in centralized manner.

Service Requirements

On a WLAN network, an AC is at a lower layer and many APs are deployed in centralized manner.

The AC and APs are on the same LAN and belong to the same network segment.

All management and service data flows of the APs are transmitted over tunnels to the AC and then processed and forwarded by the AC.

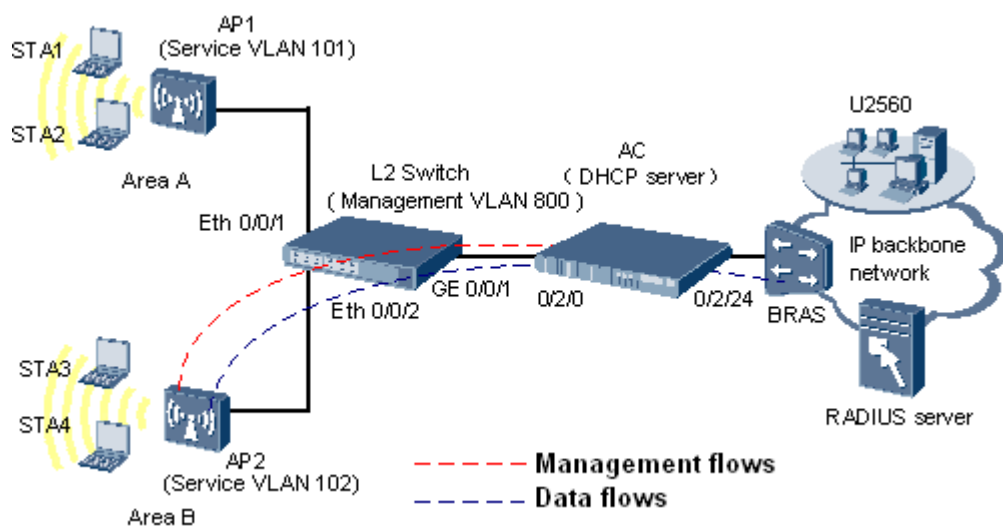
Networking

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

The Layer 2 chain networking mode is used for the AC and the APs, as shown in **Figure 4-3**. The AC delivers VLAN IDs for the service packets and the management and service packet are encapsulated into the CAPWAP tunnel. The Layer 2 switch adds VLAN tags to the management packets of the APs. When the AP management packets are transmitted to the AC, the AC removes the CAPWAP headers from the packets and forwards the service packets to the upper-layer device according to their VLAN IDs.

In the meantime, the AC functions as a DHCP server to allocate IP addresses to the APs and sends its IP address to the APs by means of DHCP Option 43.

Figure 4-3 Layer 2 chain networking (tunnel forwarding)



Prerequisite

- The APs, AC, and Layer 2 switch are functioning properly.
- The functions of the router, BRAS, and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.

Data Plan

Table 4-1 Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP security policy and OPEN-SYS authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 800 (added by the Layer 2 switch)
AP Region	AP1: 101
	AP2: 102
ESS	<ul style="list-style-type: none"> ● Name: huawei-1 ● SSID: huawei-F4 ● Mapping mode: AP region mapping ● Mapping VLAN ID: VLAN 101 ● Data forwarding mode: tunnel forwarding
	<ul style="list-style-type: none"> ● Name: huawei-2 ● SSID: huawei-F5 ● Mapping mode: AP region mapping ● Mapping VLAN ID: VLAN 102 ● Data forwarding mode: tunnel forwarding
Service VLAN ID: 100	STA1/STA2: VLAN 101 (delivered by the AC)
	STA3/STA4: VLAN 102 (delivered by the AC)
VLANs on the Layer 2 switch	Set the link type of the port connecting to the APs as Trunk and default VLAN ID as VLAN 800 . Set the link type of the port connecting to the AC as Trunk and enable the AC to support VLAN 800. The management and service VLAN IDs of the APs are all encapsulated in the CAPWAP tunnel.
Carrier ID/AC ID of the AC	CTC/1
IP address of the management interface on the AC (Meth 0)	10.11.104.2/24
IP address pool of the management interface on the AP	192.168.1.2-192.168.1.254/24
Gateway IP address of the management interface on the AP	192.168.1.1/24

Configuration Item	Data
IP address pool of sta1 and sta2	192.168.3.2 to 192.168.3.254/24
IP address pool of sta3 and sta4	192.168.4.2 to 192.168.4.254/24
DHCP server	AC

Procedure

Step 1 Configure the Layer 2 switch so that APs can communicate with the AC at Layer 2.

1. On the Layer 2 switch, set the link type of ports Eth 0/0/1 and Eth 0/0/2 connecting to APs to trunk and set the default VLAN to VLAN 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.



CAUTION

Isolate the ports of all the Layer 2 switches that connect to the downstream ports within the management and service VLANs of the APs. Otherwise, unnecessary broadcast packets exist on the VLAN or WLAN users of different APs cannot communicate with each other at Layer 2.

```
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. On the Layer 2 switch, set the link type of port GE 0/0/1 connecting to the AC to trunk and enable the port to transmit packets whose VLAN ID is 101, 102, or 800.

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

Step 2 Configure basic functions on the AC.

1. Set global AC parameters (carrier ID and global ID).
Set the carrier ID of the AC to CTC (China Telecom) and the global AC ID to 1.
huawei (config) #wlan ac-global carrier id ctc ac id 1
2. Configure VLANs for ports between the AC and the Layer 2 switch.
Create VLANs 101, 102, and 800.
huawei (config) #vlan 101
huawei (config) #vlan 102
huawei (config) #vlan 800

```
# Enable service port 0/2/0 to support VLAN ID 800.
huawei(config)#port vlan 800 0/2 0
```

3. Configure the uplink port on the AC.

```
# Add port 0/2/24 to VLANs 101 and 102.
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

4. Create a VLANIF interface on the AC.

```
# Set the IP address of VLANIF 800 to 192.168.1.1.
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 192.168.1.1 255.255.255.0
```

Enable DHCP on VLANIF 800 so that the AC also functions as the DHCP server to allocate IP address to the APs.

```
huawei(config-if-vlanif800)#dhcps enable
huawei(config-if-vlanif800)#quit
```

NOTE

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a broadband remote access server (BRAS), or a DHCP server.
- In this example, APs obtain IP addresses from the AC.

Enable DHCP on VLANIF 101 and VLANIF 102. Configure the AC as a DHCP server to allocate IP addresses to STAs.

```
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 192.168.3.1 255.255.255.0
```

```
huawei(config-if-vlanif101)#dhcps enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 192.168.4.1 255.255.255.0
```

```
huawei(config-if-vlanif102)#dhcps enable
huawei(config-if-vlanif102)#quit
```

5. Specify the source IP address for the AC.

```
# Configure VLANIF 800 as the source interface of the AC.
```

NOTE

You must specify the source IP address of an AC so that all APs connected to the AC can learn this IP address.

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

6. Configure an IP address pool for APs on the AC.

```
# Configure IP address pool ap-server on VLANIF 800.
```

NOTE

The gateway IP address in the IP address pool must be the same as the IP address of the VLANIF interface corresponding to management VLAN. After APs go online, they obtain IP addresses from this IP address pool.

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
```

```
huawei (config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei (config-ip-pool-ap-server)#quit
```

(Optional) Configure DHCP Option 60 and Option 43 to notify the APs of the AC's IP address by means of DHCP Option 43.

```
huawei (config-ip-pool-ap-server)#option 60 string Huawei AP
huawei (config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.1.1
huawei (config-ip-pool-ap-server)#quit
```

 **NOTE**

- The text information must be **Huawei AP** for Option 60.
- The text information must be **HuaweiAC-*X.X.X.X*** for Option 43. *X.X.X.X* indicates the IP address of the AC.

7. Configure an IP address pool for STAs on the AC.

```
huawei (config)#ip pool sta1-server
It's successful to create an IP address pool
huawei (config-ip-pool-sta1-server)#gateway 192.168.3.1 255.255.255.0
huawei (config-ip-pool-sta1-server)#section 0 192.168.3.2 192.168.3.254
huawei (config-ip-pool-sta1-server)#quit
huawei (config)#ip pool sta2-server
It's successful to create an IP address pool
huawei (config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0
huawei (config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254
huawei (config-ip-pool-sta2-server)#quit
```

Step 3 Connect the AC to APs.

1. Set the authentication mode of the APs to **sn-auth**.

```
huawei (config)#wlan ac
huawei (config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. Add APs offline.

Query the AP device type.

```
huawei (config-wlan-ac-view)#display ap-type all
All AP types
information:
```

```
-----
ID
Type
-----
0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN
```



```

-----
Total number: 12
# Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID
(0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002

# Get the AP online. The AP enters the normal state after it goes online.
huawei(config-wlan-ac-view)#display ap all
All AP information:
-----
AP      AP      Profile  Region  AP
ID      Type                               ID      ID      State
-----
1       WA601   0        0       normal
2       WA601   0        0       normal
-----
Total number: 2

```

3. Configure AP regions.

```

# Set AP region IDs to 101 and 102.
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit

```

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

```

huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:

Command:
    ap id 1

huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:

Command:
    ap id 2

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit

```

Step 4 Configure radios for APs.

1. Create a WMM profile named **wmm-1** and use default parameter settings for the profile.

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit

```

2. Create a radio profile named **radio-1** and bind it to WMM profile **wmm-1**.

```

huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit

```

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

```

huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit

```

 **NOTE**

You can specify different radio profiles for an AP or specify the same radio profile for multiple APs.

Step 5 Configure ESSs for APs.


1. Create a security profile.


```
# Create a security profile named security-1 in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.
huawei (config-wlan-ac-view) #security-profile name security-1
huawei (config-wlan-security-prof-security-1) #authentication policy wep
huawei (config-wlan-security-prof-security-1) #policy wep open-system
huawei (config-wlan-security-prof-security-1) #quit
```
2. Create a traffic profile (QoS profile).


```
# Create a traffic profile named traffic-1 and use default parameter settings for the profile.
huawei (config-wlan-ac-view) #traffic-profile name traffic-1
huawei (config-wlan-traffic-prof-traffic-1) #quit
```
3. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.


```
# Create an ESS named huawei-1, specify SSID huawei-F4 for it, and bind traffic profile traffic-1 and security profile security-1 to it.
huawei (config-wlan-ac-view) #ess name huawei-1 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1

# Create an ESS named huawei-2, specify SSID huawei-F5 for it, and bind traffic profile traffic-1 and security profile security-1 to it.
huawei (config-wlan-ac-view) #ess name huawei-2 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
```

 **NOTE**

An ESS defines service parameters and VAP attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.
4. Configure mappings between VLANs and APs in each ESS.


```
# Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 mode region
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 type tag region 101
vlan 101
Success: 1
Failure: 0
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 mode region
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 type tag region 102
vlan 102
Success: 1
Failure: 0
```

Step 6 Configure the data forwarding mode.

- ```
Set the data forwarding mode to ESS-based forwarding.
huawei (config-wlan-ac-view) #forward-mode type ess

Enable the ESSs named huawei-1 and huawei-2 to use the tunnel forwarding mode.
huawei (config-wlan-ac-view) #forward-mode ess 0 mode tunnel
huawei (config-wlan-ac-view) #forward-mode ess 1 mode tunnel
```

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

1. Create VAPs for AP1 and AP2 and specify radios and ESSs.
 

```
huawei (config-wlan-ac-view) #vap ap 1 radio 0 ess name huawei-1
huawei (config-wlan-ac-view) #vap ap 2 radio 0 ess name huawei-2
```

 **NOTE**

- A VAP is the binding between an AP, a radio, and an ESS profile. When an ESS profile is bound to a radio of an AP, a VAP is generated in the system.
  - The VAP functions as a radio instance of the ESS profile on the AP, has all attributes of the ESS profile, and uses the radio hardware of the AP.
2. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

----End

## Result

Wireless access users on AP1 and AP2 can discover WLANs with SSIDs huawei-F4 and huawei-F5 and then enjoy the WLAN Internet access service without authentication.

## Configuration Files

The configuration file on the AC in this configuration example is as follows:

```
#
[vlan-config]
<vlan-config>
vlan 800
vlan 101 to 102
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
port vlan 800 0/2 0
#
[vlanif]
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
<vlanif800>
interface vlanif 800
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
```

```
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode tunnel
forward-mode ess 1 mode tunnel
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-
server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.1.1
#
<ip-pool-sta1-server>
ip pool sta1-
server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip-pool-sta2-
server
gateway 192.168.4.1 255.255.255.0
section 0 192.168.4.2 192.168.4.254
#
return
```

## 4.3.2 Example for Configuring VLAN Services in a Layer 2 Branched Networking (Direct Forwarding)

The branched networking mode is applicable to scenarios where APs are scattered in hot spots of a city.

### Service Requirements

On a WLAN network, the AC is at a lower layer and APs are scattered.

The AC and APs are on the same LAN and belong to the same network segment.

Data flows and management flows of APs are directly forwarded, which requires lower AC performance.

### Networking

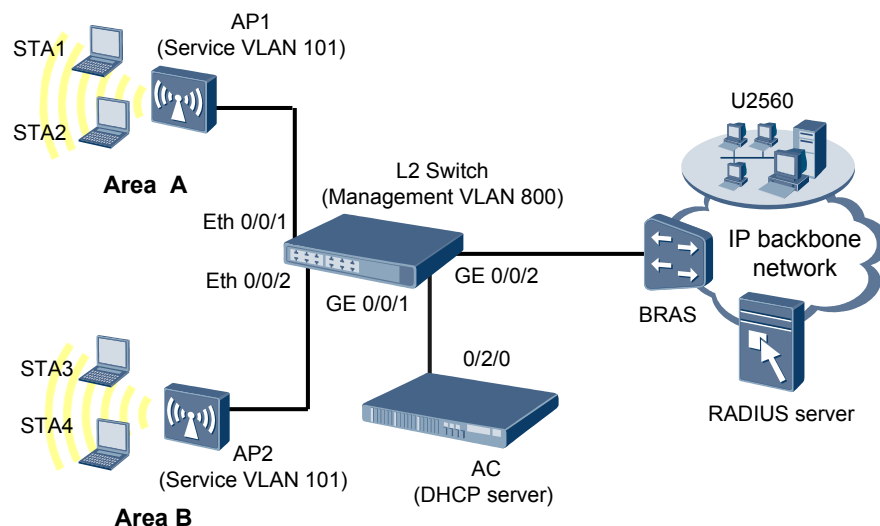
An Internet service provider (ISP) provides the WLAN service for two neighboring regions A and B. AP1 provides the WLAN service for region A, and AP2 provides the WLAN service for region B.

The AC is connected to a Layer 2 switch in branched mode, as shown in [Figure 4-4](#). The AC delivers service VLANs. The Layer 2 switch transparently transmits service VLANs and adds

VLAN tags to the AP management packets. The AC also functions as a DHCP server to allocate IP addresses to the APs and sends its IP address to the APs using Option 43.

The service data of AP1 and AP2 is forwarded directly and the AC only manages APs.

**Figure 4-4** Layer 2 branched networking (direct forwarding)



## Prerequisites

- The AP, AC, and Layer 2 switch are working properly.
- The functions of the router, broadband remote access server (BRAS), and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.

## Data Plan

**Table 4-2** Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP authentication policy and Open-system authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 800 (with VLAN tags added by the Layer 2 switch)
AP Region	AP1: 101
	AP2: 102

Configuration Item	Data
ESS	<ul style="list-style-type: none"> <li>● Name: huawei-1</li> <li>● SSID: huawei-F4</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 101</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
	<ul style="list-style-type: none"> <li>● Name: huawei-2</li> <li>● SSID: huawei-F5</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 102</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
VLAN IDs in the packets of the Internet access service	STA1/STA2: VLAN 101 (delivered by the AC)
	STA3/STA4: VLAN 102 (delivered by the AC)
VLANs on the Layer 2 switch	<ul style="list-style-type: none"> <li>● Port (Eth 0/0/1) connecting to AP1: Its link type is Trunk and default VLAN ID is 800; it transmits packets whose VLAN ID is 101 or 800.</li> <li>● Port (Eth 0/0/2) connecting to AP2: Its link type is Trunk and default VLAN ID is 800; it transmits packets whose VLAN ID is 102 or 800.</li> <li>● Port (GE 0/0/1) connecting to the AC: Its link type is Trunk and it transmits packets whose VLAN ID is 800.</li> <li>● Port (GE 0/0/2) connecting to the BRAS: Its link type is Trunk and it transmits packets whose VLAN ID is 101 or 102.</li> </ul>
AC Carrier ID/AC ID	CTC/1
IP address of the management interface (Meth 0) on the AC	10.11.104.2/24
IP address pool of APs	192.168.1.2 to 192.168.1.254/24
Gateway IP address for APs	192.168.1.1/24
IP address pool of sta1 and sta2	192.168.3.2 to 192.168.3.254/24
IP address pool of sta3 and sta4	192.168.4.2 to 192.168.4.254/24
DHCP server	AC functioning as the DHCP server to allocate IP addresses to APs

## Procedure

**Step 1** Configure the Layer 2 switch so that APs can communicate with the AC at Layer 2.

1. Set the link type of ports ETH 0/0/1 and ETH 0/0/2 on the Layer 2 switch to Trunk and VLAN ID to VLAN 800 to ensure that the ports can transmit packets whose VLAN ID is 101, 102, or 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.



**CAUTION**

Configure port isolation on all downstream ports of the Layer 2 switching in the management VLANs and service VLANs. If the ports are not isolated, unnecessary broadcast packets may exist on the VLAN or WLAN users of different APs may be unable to communicate with each other at Layer 2.

```
[huawei]vlan 101
[huawei-vlan101]quit
[huawei]vlan 102
[huawei-vlan102]quit
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. Configure the link type of port GE 0/0/1 on the Layer 2 switch connected to the AC as Trunk and VLAN ID as VLAN 800.

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

3. Configure the link type of ports GE 0/0/2 on the Layer 2 switch connected to the BRAS as Trunk and VLAN ID as VLAN 101 and VLAN 102.

```
[huawei]interface GigabitEthernet 0/0/2
[huawei-GigabitEthernet0/0/2]port link-type trunk
[huawei-GigabitEthernet0/0/2]port trunk allow-pass vlan 101
[huawei-GigabitEthernet0/0/2]port trunk allow-pass vlan 102
[huawei-GigabitEthernet0/0/2]quit
```

**Step 2** Configure basic functions on the AC.

1. Set global AC parameters (carrier ID and global ID).  
# Set the carrier ID of the AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.  
huawei (config) #wlan ac-global carrier id ctc ac id 1
2. Configure VLANs for ports between the AC and the Layer 2 switch.  
# Create VLAN 800, VLAN 101, VLAN 102.  
huawei (config) #vlan 800  
huawei (config) #vlan 101 to 102  
# Add service port 0/2/0 to VLAN 800.

```
huawei(config)#port vlan 800 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
```

3. Create a VLANIF interface on the AC.

# Configure an IP address 192.168.1.1 for VLANIF 800 so that data packets are forwarded at Layer 3 through VLANIF 800.

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.1 255.255.255.0
```

# Enable the DHCP function for VLANIF 800 so that the AC can function as the DHCP server to allocate IP addresses to the APs.

```
huawei(config-if-vlanif800)#dhcps enable
huawei(config-if-vlanif800)#quit
```

 **NOTE**

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
- In this example, APs obtain IP addresses from the AC.

Enable DHCP on VLANIF 101 and VLANIF 102. Configure the AC as a DHCP server to allocate IP addresses to STAs.

```
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.3.1 255.255.255.0
huawei(config-if-vlanif101)#dhcps enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.4.1 255.255.255.0
huawei(config-if-vlanif102)#dhcps enable
huawei(config-if-vlanif102)#quit
```

4. Specify the source IP address for the AC.

# Specify VLANIF 800 as the source interface for the AC.

 **NOTE**

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

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

5. Configure an IP address pool for APs on the AC.

# Map the IP address pool **ap-server** to VLAN 800.

 **NOTE**

The gateway IP address in the IP address pool must be the same as the IP address of the VLANIF interface corresponding to management VLAN. After APs go online, they obtain IP addresses from this IP address pool.

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

# (Optional) Configure DHCP Option 60 and Option 43 so that APs can learn the AC's IP address using Option 43.



```

huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.1.1
huawei(config-ip-pool-ap-server)#quit

```

 **NOTE**

- The text information must be **Huawei AP** for Option 60.
- The text information must be **HuaweiAC-X.X.X.X** for Option 43. X.X.X.X indicates the IP address of the AC.

6. Configure an IP address pool for STAs on the AC.

```

huawei(config)#ip pool sta1-server
It's successful to create an IP address pool
huawei(config-ip-pool-sta1-server)#gateway 192.168.3.1 255.255.255.0
huawei(config-ip-pool-sta1-server)#section 0 192.168.3.2 192.168.3.254
huawei(config-ip-pool-sta1-server)#quit
huawei(config)#ip pool sta2-server
It's successful to create an IP address pool
huawei(config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0
huawei(config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254
huawei(config-ip-pool-sta2-server)#quit

```

**Step 3** Connect the AC to APs.

1. Set the authentication mode of the APs to **sn-auth**.

```

huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth

```

2. Add APs offline.

# Query the AP device type.

```

huawei(config-wlan-ac-view)#display ap-type all
All AP types
information:

```

```

ID
Type

0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN

Total number: 12

```

# Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.

```

huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002

Enable the AP to get online. The AP enters the normal state after it goes online.
huawei(config-wlan-ac-view)#display ap all

```

All AP information:

```

AP AP Profile Region AP
ID Type ID ID State

1 WA601 0 0 normal
2 WA601 0 0 normal

```

Total number: 2

### 3. Configure AP regions.

```

Set AP region IDs to 101 and 102.
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit

```

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

```

huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> } :

```

Command:  
ap id 1

```

huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> } :

```

Command:  
ap id 2

```

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit

```

## Step 4 Configure radios for APs.

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

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit

```

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

```

huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit

```

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

```

huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit

```

#### NOTE

You can specify different radio profiles for an AP or specify the same radio profile for multiple APs.

## Step 5 Configure ESSs for APs.

### 1. Create a security profile.

```

Create a security profile named security-1 in which WEP authentication, OPEN-SYS
authentication, and non-encryption are used.

```

```

huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep

```

```
huawei (config-wlan-security-prof-security-1) #policy wep open-system
huawei (config-wlan-security-prof-security-1) #quit
```

2. Create a traffic profile (QoS profile).

```
Create a traffic profile named traffic-1 and retain the default parameter settings.
huawei (config-wlan-ac-view) #traffic-profile name traffic-1
huawei (config-wlan-traffic-prof-traffic-1) #quit
```

3. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.

```
Create an ESS named huawei-1, specify SSID huawei-F4 for it, and bind traffic profile traffic-1 and security profile security-1 to it.
```

```
huawei (config-wlan-ac-view) #ess name huawei-1 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
```

```
Create an ESS named huawei-2, specify SSID huawei-F5 for it, and bind traffic profile traffic-1 and security profile security-1 to it.
```

```
huawei (config-wlan-ac-view) #ess name huawei-2 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
```

 **NOTE**

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

4. Configure mappings between VLANs and APs in each ESS.

```
Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101.
Map AP region 102 to VLAN 102.
```

```
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 mode region
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 type tag region 101
vlan 101
```

```
Success: 1
```

```
Failure: 0
```

```
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 mode region
```

```
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 type tag region 102
vlan 102
```

```
Success: 1
```

```
Failure: 0
```

### Step 6 Configure the data forwarding mode.

- # Set the data forwarding mode to ESS-based forwarding.

```
huawei (config-wlan-ac-view) #forward-mode type ess
```

- # Configure ESSs named **huawei-1** and **huawei-2** to use direct forwarding.

```
huawei (config-wlan-ac-view) #forward-mode ess 0 mode direct-forward
```

```
huawei (config-wlan-ac-view) #forward-mode ess 1 mode direct-forward
```

### Step 7 Configure VAPs for APs and deliver WLAN services.

1. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei (config-wlan-ac-view) #vap ap 1 radio 0 ess name huawei-1
```

```
huawei (config-wlan-ac-view) #vap ap 2 radio 0 ess name huawei-2
```

 **NOTE**

- A VAP is the binding between an AP, a radio, and an ESS profile. When an ESS profile is bound to a radio of an AP, a VAP is generated.
- The VAP functions as a radio instance of the ESS profile on the AP, has all attributes of the ESS profile, and uses the radio hardware of the AP.

2. Deliver VAP parameters to APs.

```
huawei (config-wlan-ac-view) #commit ap 1
```

```
huawei (config-wlan-ac-view) #commit ap 2
```

```
huawei (config-wlan-ac-view) #quit
```

----End

## Result

Wireless access users on AP1 and AP2 can discover WLANs with SSIDs **huawei-F4** and **huawei-F5** and then enjoy the WLAN Internet access service without authentication.

## Configuration Files

Configuration file of the AC:

```
#
[vlan-config]
<vlan-config>
vlan 800
vlan 101 to 102
port vlan 101 to 102 0/2 0
port vlan 800 0/2 0
#
[vlanif]
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
<vlanif800>
interface vlanif 800
ip address 192.168.1.1 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
```

```
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode direct-
forward
forward-mode ess 1 mode direct-forward
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-
server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.1.1
#
<ip-pool-sta1-server>
ip pool sta1-
server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip-pool-sta2-
server
gateway 192.168.4.1 255.255.255.0
section 0 192.168.4.2 192.168.4.254
#
return
```

### 4.3.3 Example for Configuring VLAN Services in a Layer 3 Chain Networking (Direct Forwarding)

The chain networking mode simplifies the network architecture and is applicable to large-scale and centralized WLANs.

#### Service Requirements

On a WLAN network, the AC is at a higher layer and APs are deployed in centralized mode.

The data flows of APs are directly forwarded, which requires mode requires lower AC performance but complex configurations (configure the service gateway from APs to the AC and STA).

#### Networking

An Internet service provider (ISP) provides the WLAN service for two regions (A and B) that are deployed distantly. AP1 provides the WLAN service for region A, and AP2 provides the WLAN service for region B. Users in the regions are charged by traffic.

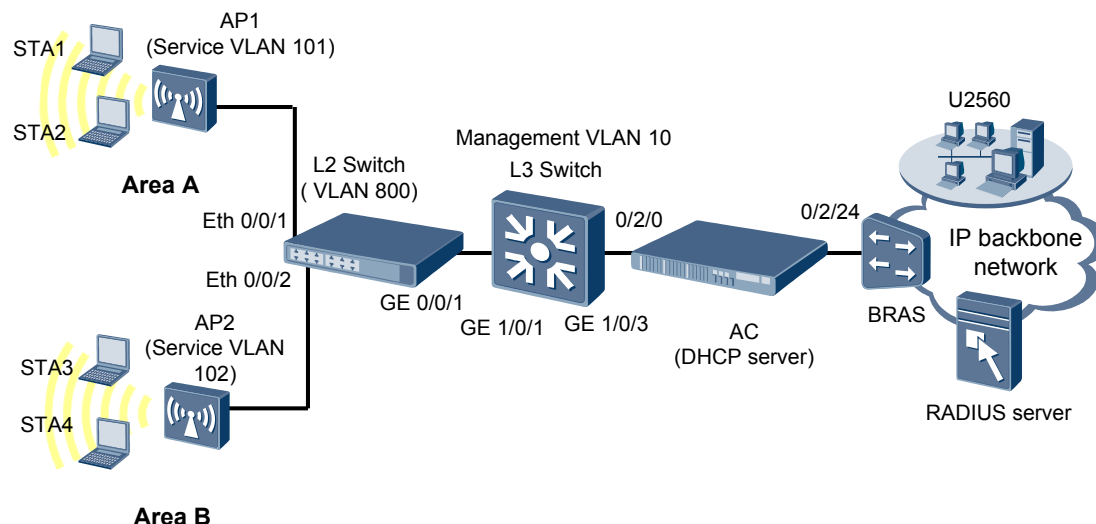
The AC is connected to a Layer 3 switch in chain mode, as shown in [Figure 4-5](#). The AC delivers service VLANs. The Layer 2 switch transparently transmits service VLANs and adds management VLAN tags to the AP management packets.

The AC also functions as a DHCP server to allocate IP addresses to the APs and advertises its IP address using Option 43.

The service data of AP1 and AP2 is forwarded directly and the AC only manages APs. AP management data is encapsulated into the CAPWAP tunnel and delivered to the AC. AP service

data is not encapsulated. Instead, it is sent from APs directly to the Layer 3 switch and then transparently transmitted to the upper-layer device.

**Figure 4-5** Layer 3 chain networking (direct forwarding)



## Prerequisites

- The AP, AC, Layer 2 switch, and Layer 3 switch are working properly and VLANs have been created on the switches.
- The functions of the router, broadband remote access server (BRAS), and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.

## Data Plan

**Table 4-3** Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP authentication policy and Open-system authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 10
AP Region	AP1: 101
	AP2: 102

Configuration Item	Data
ESS	<ul style="list-style-type: none"> <li>● Name: huawei-1</li> <li>● SSID: huawei-F4</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 101</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
	<ul style="list-style-type: none"> <li>● Name: huawei-2</li> <li>● SSID: huawei-F5</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 102</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
VLAN IDs in the packets of the Internet access service	STA1/STA2: VLAN 101 (delivered by the AC)
	STA3/STA4: VLAN 102 (delivered by the AC)
VLANs on the Layer 2 switch	<ul style="list-style-type: none"> <li>● Port (Eth 0/0/1) connecting to AP1: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 101 or 800 to pass through.</li> <li>● Port (Eth 0/0/2) connecting to AP2: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 102 or 800 to pass through.</li> <li>● Port (GE 0/0/1) connecting to the Layer 3 switch: Its link type is Trunk and it allows packets from VLAN 101, 102, or 800 to pass through.</li> </ul>
VLANs on the Layer 3 switch	<ul style="list-style-type: none"> <li>● Port (GE 1/0/1) connecting to the Layer 2 switch: Its link type is Trunk and it allows packets from VLAN 101, 102, or 800 to pass through.</li> <li>● Port (GE 1/0/3) connecting to the AC: Its link type is Hybrid and it allows packets from VLAN 101, 102, or 800 to pass through.</li> </ul>
AC Carrier ID/AC ID	CTC/1
IP address of the management interface on the AC	192.168.1.1/32
IP address pool of sta1 and sta2	192.168.3.2 to 192.168.3.254/24
IP address pool of sta3 and sta4	192.168.4.2 to 192.168.4.254/24
IP address pool of APs	192.168.1.2 to 192.168.1.254/24
Gateway IP address for APs	192.168.1.1/24 (on the Layer 3 switch)
DHCP server	AC functioning as the DHCP server to allocate IP addresses to APs

## Procedure

### Step 1 Configure switches so that APs can communicate with the AC.

1. Set the link type of ports ETH 0/0/1 and ETH 0/0/2 on the Layer 2 switch to Hybrid and VLAN ID to VLAN 800 to ensure that the ports can transmit packets whose VLAN ID is 101, 102, or 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.



### CAUTION

Configure port isolation on all downstream ports of the Layer 2 switching in the management VLANs and service VLANs. If the ports are not isolated, unnecessary broadcast packets may exist on the VLAN or WLAN users of different APs may be unable to communicate with each other at Layer 2.

---

```
[huawei]vlan batch 101 102 800
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. On the Layer 2 switch, enable GE port 0/0/1 connecting to the Layer 3 switch to transparently transmit packets with management VLANs and service VLANs.

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

3. On the Layer 3 switch, enable GE port 1/0/1 connecting to the Layer 2 switch to transparently transmit packets with management VLANs and service VLANs.

 **NOTE**

In this example, Huawei S9300 is used. If a switch of other series is used, see the relevant command reference.

```
[huawei]vlan batch 101 102 800
[huawei]interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1]port link-type trunk
[huawei-GigabitEthernet1/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet1/0/1]quit
```

4. On the Layer 3 switch, enable GE port 1/0/3 connecting to the AC to transparently transmit packets with management VLANs.

```
[huawei]vlan 10
[huawei-vlan10]quit
[huawei]interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3]port link-type hybrid
[huawei-GigabitEthernet1/0/3]port hybrid tagged vlan 10 101 102
[huawei-GigabitEthernet1/0/3]quit
```

5. Configure the DHCP relay function on the Layer 3 switch.

```
[huawei]dhcp enable
[huawei]interface Vlanif 800
```



```
[huawei-Vlanif103]ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif103]dhcp select relay
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.2
[huawei-Vlanif103]quit
```

6. Create VLAN 10 and set the IP address of VLANIF 10 to 192.168.2.1 as a Layer 3 interface that connects to the AC.

```
[huawei]interface Vlanif 10
[huawei-Vlanif10]ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif10]quit
```

## Step 2 Configure basic functions on the AC.

1. Set global AC parameters (carrier ID and global ID).

# Set the carrier ID of the AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.

```
huawei (config)#wlan ac-global carrier id ctc ac id 1
```

2. Configure VLANs for ports between the AC and the Layer 2 switch.

# Create VLANs 101, 102, and 10.

```
huawei (config)#vlan 101
huawei (config)#vlan 102
huawei (config)#vlan 10
```

# Add service port 0/2/0 to VLAN 10.

```
huawei (config)#port vlan 10 0/2 0
```

3. Create VLANIF10 interface on the AC.

# Set the IP address of the VLANIF 10 to 192.168.2.2 as a Layer 3 interface that connects to the AC.

```
huawei (config)#interface vlanif 10
huawei (config-if-vlanif10)#ip address 192.168.2.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.2.2 255.255.255.0
```

```
huawei (config)#quit
```

Enable DHCP on VLANIF 101 and VLANIF 102. Configure the AC as a DHCP server to allocate IP addresses to STAs.

```
huawei (config)#interface vlanif 101
huawei (config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.3.1 255.255.255.0
```

```
huawei (config)#quit
```

```
huawei (config)#interface vlanif 102
```

```
huawei (config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.4.1 255.255.255.0
```

```
huawei (config)#quit
```

Enable the DHCP function on the VLANIF interface so that the AC can allocate IP addresses to the APs and STA.

```
huawei (config)#interface vlanif 10
huawei (config-if-vlanif10)#dhcpc enable
huawei (config-if-vlanif10)#quit
huawei (config)#interface vlanif 101
huawei (config-if-vlanif101)#dhcpc enable
huawei (config-if-vlanif101)#quit
huawei (config)#interface vlanif 102
huawei (config-if-vlanif102)#dhcpc enable
huawei (config-if-vlanif102)#quit
```

 **NOTE**

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
  - In this example, APs and STA obtain IP addresses from the AC.
4. Configure the IP address of the vlanif interface as the source IP address of the AC to create tunnels between APs and the AC.
  5. Specify the source IP address for the AC.  
# Configure the vlanif interface as the source interface for the AC.

 **NOTE**

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

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

6. Configure an IP address pool for APs on the AC.

# Map the IP address pool **ap-server** to vlanif 10.

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

# Configure DHCP Option 60 and Option 43 so that APs can learn the AC's IP address using Option 43.

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.2.2
huawei(config-ip-pool-ap-server)#quit
```

 **NOTE**

- The text information must be **Huawei AP** for Option 60.
  - The text information must be **HuaweiAC-X.X.X.X** for Option 43. X.X.X.X indicates the IP address of the AC.
7. Configure an IP address pool for STAs on the AC.  
huawei(config)#ip pool sta1-server  
It's successful to create an IP address pool  
huawei(config-ip-pool-sta1-server)#gateway 192.168.3.1 255.255.255.0  
huawei(config-ip-pool-sta1-server)#section 0 192.168.3.2 192.168.3.254  
huawei(config-ip-pool-sta1-server)#quit  
huawei(config)#ip pool sta2-server  
It's successful to create an IP address pool  
huawei(config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0  
huawei(config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254  
huawei(config-ip-pool-sta2-server)#quit
  8. Configure the route from the AC to 192.168.1.0.  
huawei(config)#ip route-static 192.168.1.0 255.255.255.0 192.168.2.1

**Step 3** Connect the AC to APs.

1. Set the authentication mode of the APs to **sn-auth**.  
huawei(config)#wlan ac  
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth  
huawei(config-wlan-ac-view)#quit
2. Add APs offline.  
# Query the AP device type.  
huawei(config-wlan-ac-view)#display ap-type all  
All AP types  
information:

```

 ID
 Type

 0
 WA601
 1
 WA631
 2
 WA651
 3
 WA602
 4
 WA632
 5
 WA652
 6
 WA603SN
 7
 WA603DN
 8
 WA633SN
 11
 WA603DE
 12
 WA653DE
 14
 WA653SN

```

-----  
 Total number: 12

# Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.

```

huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002

```

# Enable the AP to get online. The AP enters the **normal** state after it goes online.

```

huawei(config-wlan-ac-view)#display ap all

```

All AP information:

```

 AP AP Profile Region AP
 ID Type ID ID State

 1 WA601 0 0 normal
 2 WA601 0 0 normal

```

-----  
 Total number: 2

### 3. Configure AP regions.

# Set AP region IDs to 101 and 102.

```

huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
`12huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit

```

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

```

huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }

```

Command:  
 ap id 1

```

huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }

```

Command:

```
ap id 2
```

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

#### Step 4 Configure radios for APs.

1. Create a WMM profile named **wmm-1** and use default parameter settings for the profile.

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. Create a radio profile named **radio-1** and bind it to WMM profile **wmm-1**.

```
huawei(config-wlan-ac-view)#radio-profile name radio-1 id 1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

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

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

#### NOTE

You can specify different radio profiles for an AP or specify the same radio profile for multiple APs.

#### Step 5 Configure ESSs for APs.

1. Create a security profile.

# Create a security profile named **security-1** in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.

```
huawei(config-wlan-ac-view)#security-profile name security-1 id 1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. Create a traffic profile (QoS profile).

# Create a traffic profile named **traffic-1** and retain the default parameter settings.

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1 id 1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.

# Create an ESS named **huawei-1**, specify SSID **huawei-F4** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
tra
ffic-1 security-profile security-1
```

# Create an ESS named **huawei-2**, specify SSID **huawei-F5** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile
tra
ffic-1 security-profile security-1
```

#### NOTE

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

4. Configure mappings between VLANs and APs in each ESS.

# Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101
vlan 101
Success: 1
```

```
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102
vlan 102
Success: 1
Failure: 0
```

### Step 6 Configure the data forwarding mode.

```
Set the data forwarding mode to ESS-based forwarding.
huawei(config-wlan-ac-view)#forward-mode type ess

Configure ESSs named huawei-1 and huawei-2 to use direct forwarding.
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

### Step 7 Configure VAPs for APs and deliver WLAN services.

1. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1 wlan 1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2 wlan 1
```

#### NOTE

- A VAP is the binding between an AP, a radio, and an ESS profile. When an ESS profile is bound to a radio of an AP, a VAP is generated.
- The VAP functions as a radio instance of the ESS profile on the AP, has all attributes of the ESS profile, and uses the radio hardware of the AP.

2. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

----End

## Result

Wireless access users on AP1 and AP2 can discover WLANs with SSIDs **huawei-F4** and **huawei-F5** and then enjoy the WLAN Internet access service without authentication.

## Configuration Files

Configuration file of the AC:

```
#
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 0
port vlan 101 to 102 0/2 0
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
```

```

dhcps enable
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode direct-
forward
forward-mode ess 1 mode direct-forward
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-
server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.2
#
<ip-pool-sta1-server>
ip pool sta1-
server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip pool-sta2-

```

```
server
 gateway 192.168.4.1 255.255.255.0
 section 0 192.168.4.2 192.168.4.254
#
return
```

### 4.3.4 Example for Configuring VLAN Services in a Layer 3 Branched Networking (Tunnel Forwarding)

The branched networking mode is applicable to scenarios where APs are scattered in hot spots of a city.

#### Service Requirements

On a WLAN network, the AC is at a higher layer and APs are scattered.

The data flows of APs are transmitted to the AC over tunnels, and then processed and forwarded by the AC. This mode requires higher AC performance but simple configurations (configure the service gateway only from the AC to the STA).

#### Networking

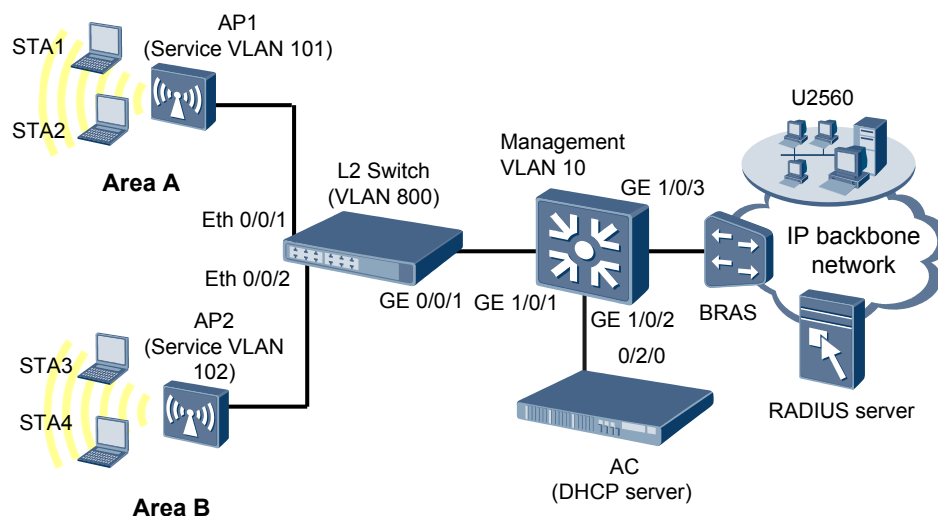
An Internet service provider (ISP) provides the WLAN service for two regions (A and B) that are deployed distantly. AP1 provides the WLAN service for region A, and AP2 provides the WLAN service for region B. Users in the regions are charged by traffic.

The AC is connected to a Layer 3 switch in branched mode, as shown in [Figure 4-6](#). The AC delivers service VLANs. The Layer 2 switch transparently transmits service VLANs and adds management VLAN tags to the AP management packets.

The AC also functions as a DHCP server to allocate IP addresses to the APs and advertises its IP address using Option 43.

Service data on AP1 and AP2 are forwarded over through channels.

**Figure 4-6** Layer 3 branched networking (tunnel forwarding)



## Prerequisites

- The AP, AC, Layer 2 switch, and Layer 3 switch are working properly and VLANs have been created on the switches.
- The functions of the router, broadband remote access server (BRAS), and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.

## Data Plan

**Table 4-4** Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP authentication policy and Open-system authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 10
AP Region	AP1: 101
	AP2: 102
ESS	<ul style="list-style-type: none"> <li>● Name: huawei-1</li> <li>● SSID: huawei-F4</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 101</li> <li>● Data forwarding mode: tunnel forwarding</li> </ul>
	<ul style="list-style-type: none"> <li>● Name: huawei-2</li> <li>● SSID: huawei-F5</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 102</li> <li>● Data forwarding mode: tunnel forwarding</li> </ul>
VLAN IDs in the packets of the Internet access service	STA1/STA2: VLAN 101 (delivered by the AC)
	STA3/STA4: VLAN 102 (delivered by the AC)
VLANs on the Layer 2 switch	<ul style="list-style-type: none"> <li>● Port (Eth 0/0/1) connecting to AP1: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 101 or 800 to pass through.</li> <li>● Port (Eth 0/0/2) connecting to AP2: Its link type is Trunk and default VLAN ID is 801; it allows packets from VLAN 102 or 801 to pass through.</li> <li>● Port (GE 0/0/1) connecting to the Layer 3 switch: Its link type is Trunk and it allows packets from VLAN 101, 102, 800, or 801 to pass through.</li> </ul>



Configuration Item	Data
VLANs on the Layer 3 switch	<ul style="list-style-type: none"> <li>● Port (GE 1/0/1) connecting to the Layer 2 switch: Its link type is Trunk and it allows packets from VLAN 101, 102, 103, 800, or 801 to pass through.</li> <li>● Port (GE 1/0/2) connecting to the AC: Its link type is Hybrid and it allows packets from VLAN 103, 800, or 801 to pass through.</li> <li>● Port (GE 1/0/3) connecting to the BRAS: Its link type is Trunk and it allows packets from VLAN 101 or 102 to pass through.</li> </ul>
AC Carrier ID/AC ID	CTC/1
IP address of the management interface on the AC	192.168.1.1/32
IP address pool of APs	192.168.1.2 to 192.168.1.254/24
Gateway IP address for APs	192.168.1.1/24 (on the Layer 3 switch)
IP address pool of sta1 and sta2	192.168.3.2 to 192.168.3.254/24
IP address pool of sta3 and sta4	192.168.4.2 to 192.168.4.254/24
DHCP server	AC functioning as the DHCP server to allocate IP addresses to APs

## Procedure

### Step 1 Configure switches so that APs can communicate with the AC.

1. Set the link type of ports ETH 0/0/1 and ETH 0/0/2 on the Layer 2 switch to Hybrid and VLAN ID to VLAN 800 to ensure that the ports can transmit packets whose VLAN ID is 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.



### CAUTION

Configure port isolation on all downstream ports of the Layer 2 switching in the management VLANs and service VLANs. If the ports are not isolated, unnecessary broadcast packets may exist on the VLAN or WLAN users of different APs may be unable to communicate with each other at Layer 2.

```
[huawei]vlan batch 800
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
```

```
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. On the Layer 2 switch, enable GE port 0/0/1 connecting to the Layer 3 switch to transparently transmit packets with management VLANs.

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

3. On the Layer 3 switch, enable GE port 1/0/1 connecting to the Layer 2 switch to transparently transmit packets with management VLANs and service VLANs.

 **NOTE**

In this example, Huawei S9300 is used. If a switch of other series is used, see the relevant command reference.

```
[huawei]vlan batch 800
[huawei]interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1]port link-type trunk
[huawei-GigabitEthernet1/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet1/0/1]quit
```

4. On the Layer 2 switch, enable GE port 1/0/2 connected to the AC to transparently transmit packets with management VLANs.

```
[huawei]vlan 10
[huawei-vlan10]quit
[huawei]interface GigabitEthernet 1/0/2
[huawei-GigabitEthernet1/0/2]port link-type hybrid
[huawei-GigabitEthernet1/0/2]port hybrid tagged vlan 10
[huawei-GigabitEthernet1/0/2]quit
```

5. On the Layer 3 switch, enable GE port 1/0/3 connecting to the BRAS to transparently transmit packets with service VLANs.

```
[huawei]interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3]port link-type trunk
[huawei-GigabitEthernet1/0/3]port trunk allow-pass vlan 101 102
[huawei-GigabitEthernet1/0/3]quit
```

6. Configure the DHCP relay function on the Layer 3 switch.

```
[huawei]dhcp enable
[huawei]interface Vlanif 800
[huawei-Vlanif103]ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif103]dhcp select relay
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.2
[huawei-Vlanif103]quit
```

7. Create VLAN 10 and set the IP address of VLANIF 10 to 192.168.2.1 as a Layer 3 interface that connects to the AC.

```
[huawei]interface Vlanif 10
[huawei-Vlanif1]ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif1]quit
```

## Step 2 Configure basic functions on the AC.

1. Set global AC parameters (carrier ID and global ID).

```
Set the carrier ID of the AC to cmcc (for China Mobile), ctc (for China Telecom), cuc
(for China Unicom), or other (for other carriers). Set the global AC ID to 1.
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

2. Configure VLANs for ports between the AC and the Layer 2 switch.

```
Create VLANs 101, 102, 800, and 801.
huawei(config)#vlan 101
huawei(config)#vlan 102
huawei(config)#vlan 10
```

```
Add service port 0/2/0 to VLAN 10 ,vlan 101 and VLAN 102.
```

```
huawei(config)#port vlan 10 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
```

3. Create a VLANIF interface on the AC.

```
Set the IP address of the VLANIF 10 to 192.168.2.2 as a Layer 3 interface that connects to the AC.
```

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif1)#ip address 192.168.2.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.2.2 255.255.255.0
huawei(config)#quit
```

Enable DHCP on VLANIF 101 and VLANIF 102. Configure the AC as a DHCP server to allocate IP addresses to STAs.

```
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.3.1 255.255.255.0
huawei(config)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.4.1 255.255.255.0
huawei(config)#quit
```

Enable the DHCP function on the VLANIF interface so that the AC can allocate IP addresses to the APs and STA.

```
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#dhcpcps enable
huawei(config-if-vlanif10)#quit
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#dhcpcps enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#dhcpcps enable
huawei(config-if-vlanif102)#quit
```

 **NOTE**

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
- In this example, APs and sta obtain IP addresses from the AC.

4. Specify the source IP address for the AC.

```
Configure the vlanif interface as the source interface for the AC.
```

 **NOTE**

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

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

5. Configure an IP address pool for APs on the AC.

```
Map the IP address pool ap-server to vlanif 10.
```

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
```

```
huawei (config-ip-pool-ap-server) #quit
□
Configure DHCP Option 60 and Option 43 so that APs can learn the AC's IP address
using Option 43.
huawei (config-ip-pool-ap-server) #option 60 string Huawei AP
huawei (config-ip-pool-ap-server) #option 43 string HuaweiAC-192.168.2.2
huawei (config-ip-pool-ap-server) #quit
```

 **NOTE**

- The text information must be **Huawei AP** for Option 60.
- The text information must be **HuaweiAC-X.X.X.X** for Option 43. X.X.X.X indicates the IP address of the AC.

6. Configure an IP address pool for STAs on the AC.

```
huawei (config) #ip pool sta1-server
It's successful to create an IP address pool
huawei (config-ip-pool-sta1-server) #gateway 192.168.3.1 255.255.255.0
huawei (config-ip-pool-sta1-server) #section 0 192.168.3.2 192.168.3.254
huawei (config-ip-pool-sta1-server) #quit
huawei (config) #ip pool sta2-server
It's successful to create an IP address pool
huawei (config-ip-pool-sta2-server) #gateway 192.168.4.1 255.255.255.0
huawei (config-ip-pool-sta2-server) #section 0 192.168.4.2 192.168.4.254
huawei (config-ip-pool-sta2-server) #quit
```

7. Configure the route from the AC to 192.168.1.0.

```
huawei (config) #ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

### Step 3 Connect the AC to APs.

1. Set the authentication mode of the APs to **sn-auth**.

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #ap-auth-mode sn-auth
huawei (config-wlan-ac-view) #quit
```

2. Add APs offline.

# Query the AP device type.

```
huawei (config-wlan-ac-view) #display ap-type all
All AP types
information:
```

```

ID
Type

```

```
0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
```

```
WA653DE
 14
WA653SN
```

```

Total number: 12
```

# Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

# Enable the AP to get online. The AP enters the **normal** state after it goes online.

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

```

AP AP Profile Region AP
ID Type ID ID State

1 WA601 0 0 normal
2 WA601 0 0 normal

```

```
Total number: 2
```

### 3. Configure AP regions.

# Set AP region IDs to 101 and 102.

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

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

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
 ap id 1
```

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
 ap id 2
```

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

## Step 4 Configure radios for APs.

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

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

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

```
huawei(config-wlan-ac-view)#radio-profile name radio-1 id 1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

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

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

 **NOTE**

You can specify different radio profiles for an AP or specify the same radio profile for multiple APs.

**Step 5** Configure ESSs for APs.

1. Create a security profile.

# Create a security profile named **security-1** in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.

```
huawei (config-wlan-ac-view) #security-profile name security-1 id 1
huawei (config-wlan-security-prof-security-1) #authentication policy wep
huawei (config-wlan-security-prof-security-1) #policy wep open-system
huawei (config-wlan-security-prof-security-1) #quit
```

2. Create a traffic profile (QoS profile).

# Create a traffic profile named **traffic-1** and retain the default parameter settings.

```
huawei (config-wlan-ac-view) #traffic-profile name traffic-1 id 1
huawei (config-wlan-traffic-prof-traffic-1) #quit
```

3. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.

# Create an ESS named **huawei-1**, specify SSID **huawei-F4** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei (config-wlan-ac-view) #ess name huawei-1 ssid huawei-F4 traffic-profile
tra
ffic-1 security-profile security-1
```

# Create an ESS named **huawei-2**, specify SSID **huawei-F5** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei (config-wlan-ac-view) #ess name huawei-2 ssid huawei-F5 traffic-profile
tra
ffic-1 security-profile security-1
```

 **NOTE**

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

4. Configure mappings between VLANs and APs in each ESS.

# Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.

```
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 mode region
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 type tag region 101
vlan 101
Success: 1
Failure: 0
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 mode region
huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 type tag region 102
vlan 102
Success: 1
Failure: 0
```

**Step 6** Configure the data forwarding mode.

# Set the data forwarding mode to ESS-based forwarding.

```
huawei (config-wlan-ac-view) #forward-mode type ess
```

# Configure ESSs named **huawei-1** and **huawei-2** to use tunnel forwarding.

```
huawei (config-wlan-ac-view) #forward-mode ess 0 mode tunnel
huawei (config-wlan-ac-view) #forward-mode ess 1 mode tunnel
```

**Step 7** Configure VAPs for APs and deliver WLAN services.

1. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei (config-wlan-ac-view) #vap ap 1 radio 0 ess name huawei-1 wlan 1
huawei (config-wlan-ac-view) #vap ap 2 radio 0 ess name huawei-2 wlan 1
```

 **NOTE**

- A VAP is the binding between an AP, a radio, and an ESS profile. When an ESS profile is bound to a radio of an AP, a VAP is generated.
- The VAP functions as a radio instance of the ESS profile on the AP, has all attributes of the ESS profile, and uses the radio hardware of the AP.

## 2. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

----End

## Result

Wireless access users on AP1 and AP2 can discover WLANs with SSIDs **huawei-F4** and **huawei-F5** and then enjoy the WLAN Internet access service without authentication.

## Configuration Files

Configuration file of the AC:

```
#
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 13
port vlan 101 to 102 0/2 13
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
```

```
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode tunnel
forward-mode ess 1 mode tunnel
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-
server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.2
#
<ip-pool-sta1-server>
ip pool sta1-
server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip-pool-sta2-
server
gateway 192.168.4.1 255.255.255.0
section 0 192.168.4.2 192.168.4.254
#
return
```

### 4.3.5 Example for Configuring VLAN Services in a Layer 2 Chain Networking (Two-Node Hot Backup)

On a WLAN network, an AC usually manages more than one thousand APs. To ensure non-stop service transmission on the WLAN, you can configure active and standby ACs to provide two-node hot backup.

#### Service Requirements

The active and standby ACs protect each other when they are not directly connected.

The active and standby ACs communicate with the APs at the same time.



When the system detects a link failure between an AP and the active AC, it triggers the active/standby switchover without affecting the services.

The priority of the active AC is higher than the standby AC. When the active AC recovers, the services are switched from the standby AC to the active AC.

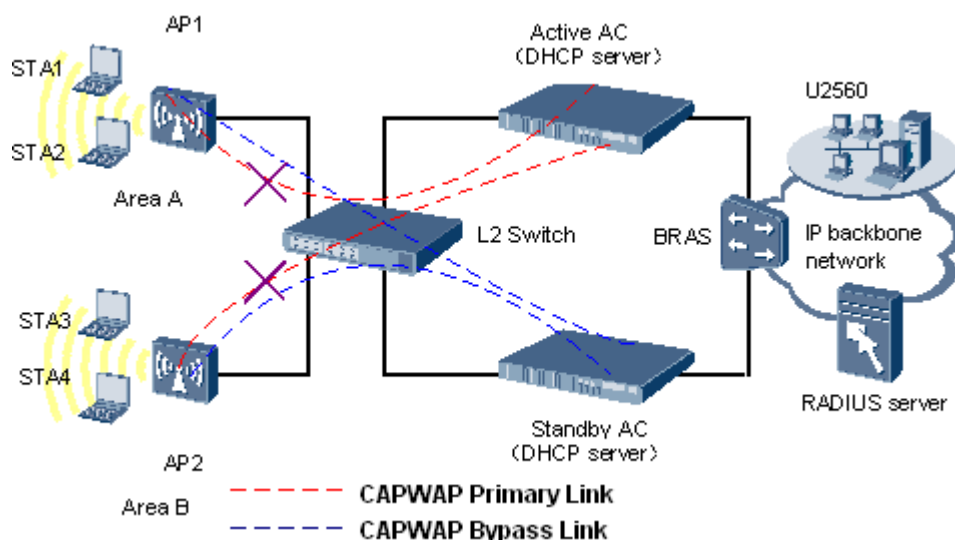
## Networking

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

The ACs and the APs are connected by a Layer 2 switch, as shown in [Figure 4-7](#). The service configurations are the same on the active and standby ACs.

IP addresses of STAs are allocated by the Layer 2 switch and the IP addresses of APs are allocated by ACs.

**Figure 4-7** Layer 2 chain networking (active/standby ACs)



## Configuration Principle

- Ensure that the APs can communicate with the active and standby ACs. The AP and the active and standby ACs must belong to the same VLAN and their IP addresses must belong to the same network segment.
- Use the following method to allocate an IP address to an AP:  
Enable the DHCP server function and configure IP address pools that do not overlap (including the gateway address, Option 43, Option 60, and sections) on the active and standby ACs so that an IP address is automatically allocated to the AP. Prevent IP address pools configured on the active and standby ACs from overlapping.
- Specify the source interface for the ACs. Only the VLANIF interface sharing the same network segment with the APs can be used as the source interface.
- Configure WLAN data:

- Enable two-node hot backup function on the active and standby ACs and set priorities for the two ACs.
- Configure the same data on the ACs.



### CAUTION

- The carrier ID cannot be **other**. If the carrier ID is configured as **other**, STAs fail to be authenticated using WPA or WAPI after an active/standby switchover is performed.
- An AC cannot allocate IP addresses to STAs or function as the gateway of STAs.

## Prerequisites

- The APs, AC, and Layer 2 switch are functioning properly.
- The functions of the router, broadband remote access server (BRAS), and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.
- You have logged in to the AC system by using a maintenance terminal.

## Data Plan

Table 4-5 Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP authentication policy and Open-system authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 800/801 (with VLAN tags added by the Layer 2 switch)
AP region	AP1: 101
	AP2: 102
ESS	<ul style="list-style-type: none"> <li>● Name: huawei-1</li> <li>● SSID: huawei-F4</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 101</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
	<ul style="list-style-type: none"> <li>● Name: huawei-2</li> <li>● SSID: huawei-F5</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 102</li> <li>● Data forwarding mode: direct forwarding</li> </ul>

Configuration Item	Data
VLAN IDs in the packets of the Internet access service	STA1/STA2: VLAN 101 (delivered by the AC)
	STA3/STA4: VLAN 102 (delivered by the AC)
VLANs on the Layer 2 switch	<ul style="list-style-type: none"> <li>● Port (Eth 0/0/1) connecting to AP1: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 800 and VLAN 101 to pass through.</li> <li>● Port (Eth 0/0/2) connecting to AP2: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 800 and VLAN 102 to pass through.</li> <li>● Port (GE 0/0/1) connecting to the active AC: Its link type is Trunk and it allows packets from VLAN 800 ,VLAN 101 and VLAN 102 to pass through.</li> <li>● Port (GE 0/0/2) connecting to the standby AC: Its link type is Trunk and it allows packets from VLAN 800 ,VLAN 101 and VLAN 102 to pass through.</li> </ul>
AC Carrier ID/AC ID	CTC/1
IP address pool of APs	192.168.1.3 to 192.168.1.254/24
Gateway IP address for APs	192.168.1.1/24
IP address pool of STA1 and STA2	192.168.5.2 to 192.168.5.254
IP address pool of STA3 and STA4	192.168.6.2 to 192.168.6.254
IP address of active and standby ACs	Active AC: 192.168.1.1/24 Standby AC: 192.168.1.2/24
Priorities of active and standby ACs	Active AC: 1 Standby AC: 2
DHCP server	AC functioning as the DHCP server to allocate IP addresses to APs.Layer 2 switch functioning as the DHCP server to allocate IP addresses to STAs

## Procedure

- Configure the Layer 2 switch so that APs can communicate with the ACs at Layer 2.
  1. Set the link type of ports ETH 0/0/1 and ETH 0/0/2 on the Layer 2 switch to Trunk and VLAN ID to VLAN 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.

**CAUTION**

Configure port isolation on all downstream ports of the Layer 2 switching in the management VLANs and service VLANs. If the ports are not isolated, unnecessary broadcast packets may exist on the VLAN or WLAN users of different APs may be unable to communicate with each other at Layer 2.

```
[huawei]vlan batch 101 102 800
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. Set the link type of ports GE 0/0/1 and GE 0/0/2 on the Layer 2 switch to Trunk and VLAN ID to VLAN 101, VLAN 102, VLAN 800.

- Connect the active AC to the Layer 2 switch.

```
[huawei]interface gigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

- Connect the standby AC to the Layer 2 switch.

```
[huawei]interface gigabitEthernet 0/0/2
[huawei-GigabitEthernet0/0/2]port link-type trunk
[huawei-GigabitEthernet0/0/2]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/2]quit
```

Configure IP address pools for the STAs.

```
[huawei] interface Vlanif 101
[huawei-Vlanif101] ip address 192.168.5.1 255.255.255.0
[huawei-Vlanif101] dhcp select interface
[huawei-Vlanif101] quit
[huawei] interface Vlanif 102
[huawei-Vlanif102] ip address 192.168.6.1 255.255.255.0
[huawei-Vlanif102] dhcp select interface
[huawei-Vlanif102] quit
```

- Configure basic functions on the ACs.

1. Set global AC parameters (carrier ID and global ID).

- Active AC

# Set the carrier ID of the active AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

- Standby AC

# Set the carrier ID of the standby AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

 **NOTE**

Ensure that the IDs of active and standby ACs are the same with the carrier ID. If they are different, service switching may fail after the active and standby AC switchover.

2. Configure VLANs for ports between the ACs and the Layer 2 switch.
  - Active AC

Create VLAN 101, VLAN 102, VLAN 800 on the active AC, add it to service port 0/2/0, and configure the port isolation function.

```
huawei(config)#vlan 101 to 102
huawei(config)#vlan 800
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#port vlan 800 0/2 0
huawei(config)#isolate port 0/2/0
```

- Standby AC

Create VLAN 101, VLAN 102, VLAN 800 on the standby AC, add it to service port 0/2/0, and configure the port isolation function.

```
huawei(config)#vlan 101 to 102
huawei(config)#vlan 800
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#port vlan 800 0/2 0
huawei(config)#isolate port 0/2/0
```

3. Configure the upstream port of the ACs.
  - Active AC

# Add VLAN 101 and VLAN 102 to upstream port 0/2/24.

```
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

- Standby AC

# Add VLAN 101 and VLAN 102 to upstream port 0/2/24.

```
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

4. Create a VLANIF interface on the AC.
  - Active AC

# Set the IP address of VLANIF 800 to 192.168.1.1.

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.1 255.255.255.0
```

# Enable the DHCP function for VLANIF 800 so that the AC can function as the DHCP server to allocate IP addresses to the APs.

```
huawei(config-if-vlanif800)#dhcps enable
huawei(config-if-vlanif800)#quit
```

- Standby AC

# Set the IP address of VLANIF 800 to 192.168.1.2.

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.2 255.255.255.0
```

```
Enable the DHCP function for VLANIF 800 so that the AC can function as the
DHCP server to allocate IP addresses to the APs.
```

```
huawei (config-if-vlanif800) #dhcps enable
huawei (config-if-vlanif800) #quit
```

 **NOTE**

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
- In this example, APs obtain IP addresses from the AC.

5. Specify the source IP address for the ACs.

- Active AC

```
Specify VLANIF 800 as the source interface for the AC.
```

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #wlan ac source interface vlanif 800
huawei (config-wlan-ac-view) #quit
```

- Standby AC

```
Specify VLANIF 800 as the source interface for the AC.
```

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #wlan ac source interface vlanif 800
huawei (config-wlan-ac-view) #quit
```

 **NOTE**

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

6. Configure an IP address pool for APs on the AC.

- Active AC

```
Map the IP address pool ap-server to VLAN 800.
```

```
huawei (config) #ip pool ap-server
It's successful to create an IP address pool
huawei (config-ip-pool-ap-server) #gateway 192.168.1.1 255.255.255.0
huawei (config-ip-pool-ap-server) #section 0 192.168.1.3 192.168.1.128
```

- Standby AC

```
Map the IP address pool ap-standby to VLAN 800.
```

```
huawei (config) #ip pool ap-standby
It's successful to create an IP address pool
huawei (config-ip-pool-ap-server) #gateway 192.168.1.2 255.255.255.0
huawei (config-ip-pool-ap-server) #section 0 192.168.1.129 192.168.1.254
```

● Connect the ACs to APs.

1. Set the authentication mode of the APs to **sn-auth**.

- Active AC

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #ap-auth-mode sn-auth
```

- Standby AC

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #ap-auth-mode sn-auth
```

2. Add APs offline.

- Active AC

```
Query the AP device type.
```

```
huawei (config-wlan-ac-view) #display ap-type all
All AP types
information:
```

-----  
---

```

ID
Type

0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN

```

```


Total number: 12
Add AP1 and AP2 of the WA601 type offline according to the obtained device type
ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
Enable the AP to get online. The AP enters the normal state after it goes online.
huawei(config-wlan-ac-view)#display ap all
All AP information:

```

```

-

```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

```

-

```

```

Total number: 2
- Standby AC

```

 **NOTE**

Because only one link is established, the AP cannot go online from the standby AP after it goes online from the active AC.

To enable the AP to go online from the standby AP, disconnect the primary link. Perform the following operations.

```

Query the AP device type.
huawei(config-wlan-ac-view)#display ap-type all
All AP types
information:

```

```

ID
Type

0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN

```

```

Total number: 12
Add AP1 and AP2 of the WA601 type offline according to the obtained device type
ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
Enable the AP to get online. The AP enters the normal state after it goes online.
huawei(config-wlan-ac-view)#display ap all
All AP information:

```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

```

-
Total number: 2

```

3. Configure AP regions.

- Active AC

```

Set AP region IDs to 101 and 102.
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit

```

- Standby AC

```

Set AP region IDs to 101 and 102.
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit

```



```
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

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

- Active AC

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
ap id 1
```

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
ap id 2
```

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

- Standby AC

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
ap id 1
```

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
ap id 2
```

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

● Configure radios for APs.

- Active AC

1. Create a WMM profile named **wmm-1** and use default parameter settings for the profile.

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. Create a radio profile named **radio-1** and bind it to WMM profile **wmm-1**.

```
huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

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

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

- Standby AC

1. Create a WMM profile named **wmm-1** and use default parameter settings for the profile.

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. Create a radio profile named **radio-1** and bind it to WMM profile **wmm-1**.

```
huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

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

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

 **NOTE**

You can specify different radio profiles for an AP or specify the same radio profile for multiple APs.

- Configure ESSs for APs.

- Active AC

1. Create a security profile.

# Create a security profile named **security-1** in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. Create a traffic profile (QoS profile).

# Create a traffic profile named **traffic-1** and retain the default parameter settings.

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.

# Create an ESS named **huawei-1**, specify SSID **huawei-F4** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-
profile
traffic-1 security-profile security-1
```

# Create an ESS named **huawei-2**, specify SSID **huawei-F5** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-
profile
traffic-1 security-profile security-1
```

 **NOTE**

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

4. Configure mappings between VLANs and APs in each ESS.

# Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag
region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag
region 102 vlan 102
Success: 1
Failure: 0
```

- Standby AC

1. Create a security profile.  
 # Create a security profile named **security-1** in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.  

```

 huawei (config-wlan-ac-view) #security-profile name security-1
 huawei (config-wlan-security-prof-security-1) #authentication policy wep
 huawei (config-wlan-security-prof-security-1) #policy wep open-system
 huawei (config-wlan-security-prof-security-1) #quit

```
2. Create a traffic profile (QoS profile).  
 # Create a traffic profile named **traffic-1** and retain the default parameter settings.  

```

 huawei (config-wlan-ac-view) #traffic-profile name traffic-1
 huawei (config-wlan-traffic-prof-traffic-1) #quit

```
3. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.  
 # Create an ESS named **huawei-1**, specify SSID **huawei-F4** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.  

```

 huawei (config-wlan-ac-view) #ess name huawei-1 ssid huawei-F4 traffic-profile
 traffic-1 security-profile security-1

```

 # Create an ESS named **huawei-2**, specify SSID **huawei-F5** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.  

```

 huawei (config-wlan-ac-view) #ess name huawei-2 ssid huawei-F5 traffic-profile
 traffic-1 security-profile security-1

```

 **NOTE**

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

4. Configure mappings between VLANs and APs in each ESS.  
 # Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.  

```

 huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 mode region
 huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-1 type tag
 region 101 vlan 101
 Success: 1
 Failure: 0
 huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 mode region
 huawei (config-wlan-ac-view) #vlan-mapping ess name huawei-2 type tag
 region 102 vlan 102
 Success: 1
 Failure: 0

```

- Configure the data forwarding mode.

- Active AC

```

Set the data forwarding mode to ESS-based forwarding.
huawei (config-wlan-ac-view) #forward-mode type ess

Configure ESSs named huawei-1 and huawei-2 to use direct forwarding.
huawei (config-wlan-ac-view) #forward-mode ess 0 mode direct-forward
huawei (config-wlan-ac-view) #forward-mode ess 1 mode direct-forward

```

- Standby AC

```

Set the data forwarding mode to ESS-based forwarding.
huawei (config-wlan-ac-view) #forward-mode type ess

Configure ESSs named huawei-1 and huawei-2 to use direct forwarding.
huawei (config-wlan-ac-view) #forward-mode ess 0 mode direct-forward
huawei (config-wlan-ac-view) #forward-mode ess 1 mode direct-forward

```

- Configure VAPs for APs and deliver WLAN services.

- Active AC

1. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

2. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

- Standby AC

 **NOTE**

Because only one link is established, the AP cannot go online from the standby AP after it goes online from the active AC.

To enable the AP to go online from the standby AP, disconnect the primary link. Perform the following operations.

1. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

 **NOTE**

- A VAP is the binding between an AP, a radio, and an ESS profile. When an ESS profile is bound to a radio of an AP, a VAP is generated.
- The VAP functions as a radio instance of the ESS profile on the AP, has all attributes of the ESS profile, and uses the radio hardware of the AP.

2. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

 **NOTE**

After the configuration is delivered to the AP, both the primary and secondary links must be connected.

- Enable the two-node hot backup protection function on the ACs.

- Active AC

Enable the two-node hot backup protection function on the active AC. Set the IP address of the standby AC to 192.168.1.2/24 and the priority of the active AC to 1.

 **NOTE**

The active and standby ACs are determined by the configured priorities. The AC with a higher priority works as the active AC, and the AC with a lower priority works as the standby AC. A smaller priority value indicates a higher priority. When the two ACs have the same priority, the one with lighter load becomes the active AC. If the loads on the ACs are also the same, the AC with a smaller IP address becomes the active AC.

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.1.2
priority 1
```

- Standby AC

Enable the two-node hot backup protection function on the standby AC. Set the IP address of the standby AC to 192.168.1.1/24 and the priority of the standby AC to 2.

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.1.1
priority 2
```

----End

## Result

When the system detects a link failure between an AP and the active AC, it triggers the active/standby switchover without affecting the services. When the active AC recovers, the services are switched over to the active AC.

## Configuration Files

Configuration file of the active AC:

```
#
[vlan-config]
<vlan-config>
vlan 101 to 102
vlan 800
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
port vlan 800 0/2 0
#
[vlanif]
<vlanif800>
interface vlanif 800
ip address 192.168.1.1 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.1.2 priority 1
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
```

```

#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-
server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.3 192.168.1.128
#
return
Configuration file of the standby AC:
#
[vlan-config]
<vlan-config>
vlan 101 to 102
vlan 800
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
port vlan 800 0/2 0
#
[vlanif]
<vlanif800>
interface vlanif 800
ip address 192.168.1.2 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.1.1 priority 2
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1

```

```
#
[ip-pool]
<ip-pool-ap-standby>
ip pool ap-
standby
 gateway 192.168.1.2 255.255.255.0
 section 0 192.168.1.129 192.168.1.254
#
```

```
return
```

Configuration file of the layer 2 Switch:

```
#
vlan batch 101 102 800
#
interface Vlanif101
 ip address 192.168.5.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.6.1 255.255.255.0
 dhcp select interface
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk pvid vlan 800
 port trunk allow-pass vlan 101 800
 port-isolate enable group 1
#
interface Ethernet0/0/2
 port link-type trunk
 port trunk pvid vlan 800
 port trunk allow-pass vlan 102 800
 port-isolate enable group 1
#
interface
GigabitEthernet0/0/1
 port hybrid tagged vlan 101 to 102 800
#
interface
GigabitEthernet0/0/2
 port hybrid tagged vlan 101 to 102 800
#
return
```

### 4.3.6 Example for Configuring VLAN Services in a Layer 3 Branched Networking (Two-Node Hot Backup)

On a WLAN network, an AC usually manages more than one thousand APs. To ensure non-stop service transmission on the WLAN, you can configure active and standby ACs to provide two-node hot backup.

#### Service Requirements

The active and standby ACs protect each other when they are not directly connected.

The active and standby ACs communicate with the APs at the same time.

When the system detects a link failure between an AP and the active AC, it triggers the active/standby switchover without affecting the services.

The priority of the active AC is higher than the standby AC. When the active AC recovers, the services are switched from the standby AC to the active AC.

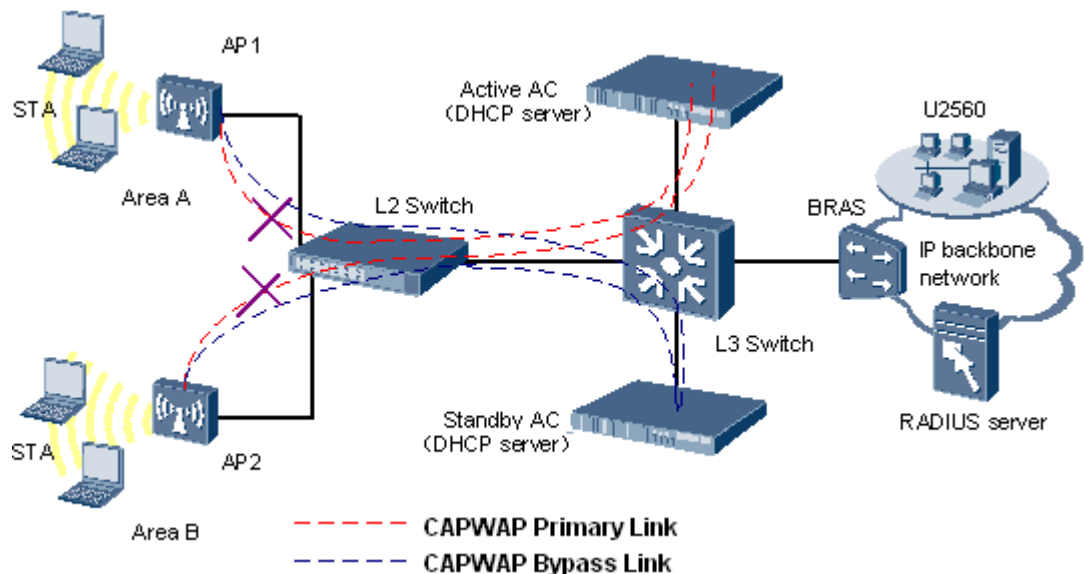
## Networking

An Internet service provider (ISP) provides the WLAN service for two regions (A and B) that are deployed distantly. AP1 provides the WLAN service for region A, and AP2 provides the WLAN service for region B. Users in the regions are charged by traffic.

The ACs are connected by a Layer 3 switch and communicate with APs through a Layer 2 switch, as shown in **Figure 4-8**. The service configurations are the same on the active and standby ACs.

IP addresses of STAs are allocated by the Layer 3 Switch and the IP addresses of APs are allocated by ACs.

**Figure 4-8** Layer 3 branched networking (active/standby ACs)



## Configuration Principle

- Ensure that the APs can communicate with the active and standby ACs.
- Use the following method to allocate an IP address to an AP:
  - Enable the DHCP server function and configure IP address pools that do not overlap (including the gateway address, Option 43, Option 60, and sections) on the active and standby ACs so that an IP address is automatically allocated to the AP. Prevent IP address pools configured on the active and standby ACs from overlapping.
- Specify the source interface for the ACs. Only the VLANIF or loopback interface sharing the same network segment with the APs can be used as the source interface.
- Configure WLAN data:
  - Enable two-node hot backup function on the active and standby ACs and set priorities for the two ACs.
  - Configure the same data on the ACs.





## CAUTION

- The carrier ID cannot be **other**. If the carrier ID is configured as **other**, STAs fail to be authenticated using WPA or WAPI after an active/standby switchover is performed.
- An AC cannot allocate IP addresses to STAs or function as the gateway of STAs.

## Prerequisites

- The AP, AC, Layer 2 switch, and Layer 3 switch are working properly and VLANs have been created on the switches.
- The functions of the router, broadband remote access server (BRAS), and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.
- You have logged in to the AC system by using a maintenance terminal.

## Data Plan

Table 4-6 Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP authentication policy and Open-system authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 10
AP Region	AP1: 101
	AP2: 102
ESS	<ul style="list-style-type: none"> <li>● Name: huawei-1</li> <li>● SSID: huawei-F4</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 101</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
	<ul style="list-style-type: none"> <li>● Name: huawei-2</li> <li>● SSID: huawei-F5</li> <li>● Mapping mode: AP region mapping</li> <li>● Mapping VLAN ID: 102</li> <li>● Data forwarding mode: direct forwarding</li> </ul>
VLAN IDs in the packets of the Internet access service	STA1/STA2: VLAN 101 (delivered by the AC)
	STA3/STA4: VLAN 102 (delivered by the AC)

Configuration Item	Data
VLANs on the Layer 2 switch	<ul style="list-style-type: none"> <li>● Port (Eth 0/0/1) connecting to AP1: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 800 or 101 to pass through.</li> <li>● Port (Eth 0/0/2) connecting to AP2: Its link type is Trunk and default VLAN ID is 800; it allows packets from VLAN 800 or 102 to pass through.</li> <li>● Port (GE 0/0/1) connecting to the Layer 3 switch: Its link type is Trunk and it allows packets from VLAN 800 or 101 or 102 to pass through.</li> </ul>
VLANs on the Layer 3 switch	<ul style="list-style-type: none"> <li>● Port (GE 1/0/1) connecting to the Layer 2 switch: Its link type is Trunk and it allows packets from VLAN 101, 102, or 800 to pass through.</li> <li>● Port (GE 1/0/2) connecting to the active AC: Its link type is Hybrid and it allows packets from VLAN 10, 101, or 102 to pass through.</li> <li>● Port (GE 1/0/4) connecting to the standby AC: Its link type is Hybrid and it allows packets from VLAN 10, 101, or 102 to pass through.</li> <li>● Port (GE 1/0/3) connecting to the BRAS: Its link type is Trunk and it allows packets from VLAN 101 or 102 to pass through.</li> </ul>
AC Carrier ID/AC ID	CTC/1
IP address pool of APs	192.168.1.2 to 192.168.1.254/24
Gateway IP address for APs	192.168.1.1/24 (on the Layer 3 switch)
IP address pool of STA1	192.168.5.2 to 192.168.5.254/24
IP address pool of STA3	192.168.6.2 to 192.168.6.254/24
DHCP server	AC functioning as the DHCP server to allocate IP addresses to APs
IP address of active and standby ACs	Active AC: 192.168.2.2/24 Standby AC: 192.168.2.3/24
Priorities of active and standby ACs	Active AC: 1 Standby AC: 2
Dynamic IP address of an AP.	192.168.1.2 to 192.168.1.254/24

## Procedure

- Configure switches so that APs can communicate with the AC.
  1. Set the link type of ports ETH 0/0/1 and ETH 0/0/2 on the Layer 2 switch to Hybrid and VLAN ID to VLAN 800 to ensure that the ports can transmit packets whose VLAN ID is 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.



**CAUTION**

Configure port isolation on all downstream ports of the Layer 2 switching in the management VLANs and service VLANs. If the ports are not isolated, unnecessary broadcast packets may exist on the VLAN or WLAN users of different APs may be unable to communicate with each other at Layer 2.

```
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. On the Layer 2 switch, enable GE port 0/0/1 connecting to the Layer 3 switch to transparently transmit packets with management VLANs and service VLANs.

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

3. On the Layer 3 switch, enable GE port 1/0/1 connecting to the Layer 2 switch to transparently transmit packets with management VLANs and service VLANs.

 **NOTE**

In this example, Huawei S9300 is used. If a switch of other series is used, see the relevant command reference.

```
[huawei]vlan batch 10 101 102 800
[huawei]interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1]port link-type trunk
[huawei-GigabitEthernet1/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet1/0/1]quit
```

4. On the Layer 2 switch, enable GE port 1/0/2 connecting to the active AC to transparently transmit packets with management VLANs.

```
[huawei-vlan10]quit
[huawei]interface GigabitEthernet 1/0/2
[huawei-GigabitEthernet1/0/2]port link-type hybrid
[huawei-GigabitEthernet1/0/2]port hybrid tagged vlan 10 101 102
[huawei-GigabitEthernet1/0/2]quit
```

5. On the Layer 4 switch, enable GE port 1/0/4 connecting to the standby AC to transparently transmit packets with management VLANs.

```
[huawei-vlan11]quit
[huawei]interface GigabitEthernet 1/0/4
[huawei-GigabitEthernet1/0/4]port link-type hybrid
[huawei-GigabitEthernet1/0/4]port hybrid tagged vlan 10 101 102
[huawei-GigabitEthernet1/0/4]quit
```

6. On the Layer 3 switch, enable GE port 1/0/3 connecting to the BRAS to transparently transmit packets with service VLANs.

```
[huawei]interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3]port link-type trunk
[huawei-GigabitEthernet1/0/3]port trunk allow-pass vlan 101 102
[huawei-GigabitEthernet1/0/3]quit
```

7. Configure the DHCP relay function on the Layer 3 switch.

```
[huawei]dhcp enable
[huawei]interface Vlanif 800
[huawei-Vlanif103]ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif103]dhcp select relay
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.2
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.3
[huawei-Vlanif103]quit
```

8. # Set the IP address of the VLANIF 10 to 192.168.2.1 as a Layer 3 interface that connects to the active AC and standby AC.

```
[huawei]interface Vlanif 10
[huawei-Vlanif10]ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif10]quit
```

Configure IP address pools for the STAs.

```
[huawei]interface Vlanif 101
[huawei-Vlanif101]ip address 192.168.5.1 255.255.255.0
[huawei-Vlanif101]dhcp select interface
[huawei-Vlanif101]quit
[huawei]interface Vlanif 102
[huawei-Vlanif102]ip address 192.168.6.1 255.255.255.0
[huawei-Vlanif102]dhcp select interface
[huawei-Vlanif102]quit
```

- Configure basic functions on the ACs.

1. Set global AC parameters (carrier ID and global ID).

- Active AC

# Set the carrier ID of the active AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

- Standby AC

# Set the carrier ID of the standby AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

#### NOTE

Ensure that the IDs of active and standby ACs are the same with the carrier ID. If they are different, service switching may fail after the active and standby AC switchover.

2. Configure VLANs for ports between the ACs and the Layer 3 switch.

- Active AC

Create VLAN 10, VLAN 101 and VLAN 102 on the active AC, add it to service port 0/2/0, and configure the port isolation function.

```
huawei(config)#vlan 10
huawei(config)#vlan 101 to 102
huawei(config)#port vlan 10 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#isolate port 0/2/0
```

- Standby AC

Create VLAN 10, VLAN 101 and VLAN 102 on the standby AC, add it to service port 0/2/0, and configure the port isolation function.

```
huawei(config)#vlan 10
huawei(config)#vlan 101 to 102
huawei(config)#port vlan 10 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#isolate port 0/2/0
```

3. Create a VLAN and VLANIF interface on the AC.

- Active AC

Set the IP address of the VLANIF 10 to 192.168.2.2 as a Layer 3 interface that connects to the AC.

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 192.168.2.2 255.255.255.0
{ <cr>|description<K>|sub<K> } :
Command:
ip address 192.168.2.2 255.255.255.0
```

Enable the DHCP function on the VLANIF interface so that the AC can allocate IP addresses to the APs.

```
huawei(config-if-vlanif10)#dhcps enable
huawei(config-if-vlanif10)#quit
```

 NOTE

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
- In this example, APs obtain IP addresses from the AC.

- Standby AC

Set the IP address of the VLANIF 10 to 192.168.2.3 as a Layer 3 interface that connects to the AC.

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif11)#ip address 192.168.2.3 255.255.255.0
{ <cr>|description<K>|sub<K> } :

Command:
ip address 192.168.2.3 255.255.255.0
```

Enable the DHCP function on the VLANIF interface so that the AC can allocate IP addresses to the APs.

```
huawei(config-if-vlanif11)#dhcps enable
huawei(config-if-vlanif11)#quit
```

 NOTE

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
- In this example, APs obtain IP addresses from the AC.

4. Specify the source IP address for the ACs.

- Active AC

Configure the VLANIF interface as the source interface for the active AC.

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

- Standby AC

Configure the VLANIF interface as the source interface for the standby AC.

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #wlan ac source interface vlanif 10
huawei (config-wlan-ac-view) #quit
```

 **NOTE**

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

5. Configure an IP address pool for APs on the AC.
  - Active AC

Map the IP address pool **ap-server** to vlanif 10.

```
huawei (config) #ip pool ap-server
 It's successful to create an IP address pool
huawei (config-ip-pool-ap-server) #gateway 192.168.1.1 255.255.255.0
huawei (config-ip-pool-ap-server) #section 0 192.168.1.2 192.168.1.128
huawei (config-ip-pool-ap-server) #quit
```

# Configure DHCP Option 60 and Option 43 so that APs can learn the AC's IP address using Option 43.

```
huawei (config-ip-pool-ap-server) #option 60 string Huawei AP
huawei (config-ip-pool-ap-server) #option 43 string
HuaweiAC-192.168.2.2,192.168.2.3
huawei (config-ip-pool-ap-server) #quit
```

- Standby AC

Map the IP address pool **ap-standby** to vlanif 10.

```
huawei (config) #ip pool standby
 It's successful to create an IP address pool
huawei (config-ip-pool-ap-server) #gateway 192.168.1.1 255.255.255.0
huawei (config-ip-pool-ap-server) #section 0 192.168.1.129 192.168.1.254
huawei (config-ip-pool-ap-server) #quit
```

# Configure DHCP Option 60 and Option 43 so that APs can learn the AC's IP address using Option 43.

```
huawei (config-ip-pool-ap-server) #option 60 string Huawei AP
huawei (config-ip-pool-ap-server) #option 43 string
HuaweiAC-192.168.2.3,192.168.2.2
huawei (config-ip-pool-ap-server) #quit
```

 **NOTE**

- The text information must be **Huawei AP** for Option 60.
- The text information must be **HuaweiAC-X.X.X.X** for Option 43. *X.X.X.X* indicates the IP address of the AC.

1. Configure the route from the AC to 192.168.1.0.
  - Active AC

```
huawei (config) #ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

- Standby AC

```
huawei (config) #ip route-static 192.168.1.0 255.255.255.0 192.168.3.1
```

1. Connect the ACs to APs.

- a. Set the authentication mode of the APs to **sn-auth**.

- Active AC

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #ap-auth-mode sn-auth
```

- Standby AC

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #ap-auth-mode sn-auth
```

b. Add APs offline.

- Active AC

# Query the AP device type.

```
huawei (config-wlan-ac-view) #display ap-type all
All AP types
information:
```

```


ID
Type
```

```


0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN
```

```


Total number: 12
```

# Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.

```
huawei (config-wlan-ac-view) #ap id 1 type-id 0 sn SN000001
huawei (config-wlan-ac-view) #ap id 2 type-id 0 sn SN000002
```

# Enable the AP to get online. The AP enters the **normal** state after it goes online.

```
huawei (config-wlan-ac-view) #display ap all
All AP information:
```

```


AP AP Profile Region AP
ID Type ID ID State

1 WA601 0 0 normal
2 WA601 0 0 normal
```

```


Total number: 2
```

- Standby AC

 **NOTE**

Because only one link is established, the AP cannot go online from the standby AP after it goes online from the active AC.

To enable the AP to go online from the standby AP, disconnect the primary link. Perform the following operations.

**# Query the AP device type.**

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types
information:
```

```


ID
Type

```

```


0
WA601
1
WA631
2
WA651
3
WA602
4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN

```

```


Total number: 12
```

**# Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID (0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.**

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

**# Enable the AP to get online. The AP enters the normal state after it goes online.**

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

```


AP AP Profile Region AP
ID Type ID ID State

1 WA601 0 0 normal
2 WA601 0 0 normal

```

```


Total number: 2
```



c. Configure AP regions.

- Active AC

# Set AP region IDs to 101 and 102.

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

- Standby AC

# Set AP region IDs to 101 and 102.

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

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

- Active AC

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:  
ap id 1

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:  
ap id 2

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

- Standby AC

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:  
ap id 1

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:  
ap id 2

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

2. Configure radios for APs.

- Active AC

a. Create a WMM profile named **wmm-1** and use default parameter settings for the profile.

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

b. Create a radio profile named **radio-1** and bind it to WMM profile **wmm-1**.

```
huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

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

```

huawei (config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei (config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei (config-wlan-radio-1/0)#quit
huawei (config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei (config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei (config-wlan-radio-2/0)#quit

```

– Standby AC

- a. Create a WMM profile named **wmm-1** and use default parameter settings for the profile.

```

huawei (config-wlan-ac-view)#wmm-profile name wmm-1
huawei (config-wlan-wmm-prof-wmm-profile-1)#quit

```

- b. Create a radio profile named **radio-1** and bind it to WMM profile **wmm-1**.

```

huawei (config-wlan-ac-view)#radio-profile name radio-1
huawei (config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei (config-wlan-radio-prof-radio-1)#quit

```

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

```

huawei (config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei (config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei (config-wlan-radio-1/0)#quit
huawei (config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei (config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei (config-wlan-radio-2/0)#quit

```

 **NOTE**

You can specify different radio profiles for an AP or specify the same radio profile for multiple APs.

3. Configure ESSs for APs.

– Active AC

- a. Create a security profile.

# Create a security profile named **security-1** in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.

```

huawei (config-wlan-ac-view)#security-profile name security-1
huawei (config-wlan-security-prof-security-1)#authentication policy
wep
huawei (config-wlan-security-prof-security-1)#policy wep open-system
huawei (config-wlan-security-prof-security-1)#quit

```

- b. Create a traffic profile (QoS profile).

# Create a traffic profile named **traffic-1** and retain the default parameter settings.

```

huawei (config-wlan-ac-view)#traffic-profile name traffic-1
huawei (config-wlan-traffic-prof-traffic-1)#quit

```

- c. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.

# Create an ESS named **huawei-1**, specify SSID **huawei-F4** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```

huawei (config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-
profile
traffic-1 security-profile security-1

```

# Create an ESS named **huawei-2**, specify SSID **huawei-F5** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```

huawei (config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-
profile
traffic-1 security-profile security-1

```

 **NOTE**

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

- d. Configure mappings between VLANs and APs in each ESS.

# Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode
region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag
region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode
region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag
region 102 vlan 102
Success: 1
Failure: 0
```

- Standby AC

- a. Create a security profile.

# Create a security profile named **security-1** in which WEP authentication, OPEN-SYS authentication, and non-encryption are used.

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy
wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

- b. Create a traffic profile (QoS profile).

# Create a traffic profile named **traffic-1** and retain the default parameter settings.

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

- c. Create ESSs for AP1 and AP2 and bind them to the traffic profile and security profile.

# Create an ESS named **huawei-1**, specify SSID **huawei-F4** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-
profile
traffic-1 security-profile security-1
```

# Create an ESS named **huawei-2**, specify SSID **huawei-F5** for it, and bind traffic profile **traffic-1** and security profile **security-1** to it.

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-
profile
traffic-1 security-profile security-1
```

 **NOTE**

An ESS defines service parameters and virtual AP (VAP) attributes. When an ESS is bound to a specified radio of an AP, all the ESS parameters are applied to a WLAN service entity, a VAP. The AP provides differentiated wireless functions for users based on these parameters.

- d. Configure mappings between VLANs and APs in each ESS.

# Set the VLAN mapping mode to AP region mapping. Map AP region 101 to VLAN 101. Map AP region 102 to VLAN 102.

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode
region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag
region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode
region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag
region 102 vlan 102
Success: 1
Failure: 0
```

## 4. Configure the data forwarding mode.

## - Active AC

# Set the data forwarding mode to ESS-based forwarding.

```
huawei(config-wlan-ac-view)#forward-mode type ess
```

# Configure ESSs named **huawei-1** and **huawei-2** to use direct forwarding.

```
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward
```

```
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

## - Standby AC

# Set the data forwarding mode to ESS-based forwarding.

```
huawei(config-wlan-ac-view)#forward-mode type ess
```

# Configure ESSs named **huawei-1** and **huawei-2** to use direct forwarding.

```
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward
```

```
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

## 5. Configure VAPs for APs and deliver WLAN services.

## - Active AC

## a. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
```

```
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

## b. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
```

```
huawei(config-wlan-ac-view)#commit ap 2
```

```
huawei(config-wlan-ac-view)#quit
```

## - Standby AC

 **NOTE**

Because only one link is established, the AP cannot go online from the standby AP after it goes online from the active AC.

To enable the AP to go online from the standby AP, disconnect the primary link. Perform the following operations.

## a. Create VAPs (or WLAN services) for AP1 and AP2 and specify radios and ESSs.

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
```

```
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

 **NOTE**

- A VAP is the binding between an AP, a radio, and an ESS profile. When an ESS profile is bound to a radio of an AP, a VAP is generated.
- The VAP functions as a radio instance of the ESS profile on the AP, has all attributes of the ESS profile, and uses the radio hardware of the AP.

## b. Deliver VAP parameters to APs.

```
huawei(config-wlan-ac-view)#commit ap 1
```

```
huawei(config-wlan-ac-view)#commit ap 2
```

```
huawei(config-wlan-ac-view)#quit
```

 **NOTE**

After the configuration is delivered to the AP, both the primary and secondary links must be connected.

## ● Enable the two-node hot backup protection function on the ACs.

## - Active AC

## 1. Enable the two-node hot backup protection function on the active AC. Set the IP address of the standby AC to 192.168.3.2/24 and the priority of the active AC to 1.

 **NOTE**

The active and standby ACs are determined by the configured priorities. The AC with a higher priority works as the active AC, and the AC with a lower priority works as the standby AC. A smaller priority value indicates a higher priority. When the two ACs have the same priority, the one with lighter load becomes the active AC. If the loads on the ACs are also the same, the AC with a smaller IP address becomes the active AC.

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.3.2
priority 1
```

**- Standby AC**

1. Enable the two-node hot backup protection function on the standby AC. Set the IP address of the standby AC to 192.168.2.2/24 and the priority of the standby AC to 2.

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.2.2
priority 2
```

----End

## Result

When the system detects a link failure between an AP and the active AC, it triggers the active/standby switchover without affecting the services. When the active AC recovers, the services are switched over to the active AC.

## Configuration Files

Configuration file of the active AC:

```
#
[board-bind]
<board-bind>
isolate port 0/2/0
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 0
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.2 255.255.255.0
dhcps enable
#
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.2.3 priority 1
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
```

```

ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
 region-id 102
 quit
wmm-profile name wmm-1 id 1
 quit
traffic-profile name traffic-1 id
1
 quit
security-profile name security-1 id
1
 quit
radio-profile name radio-1 id 1
 bind wmm-profile id 1
 quit
radio ap-id 1 radio-id 0
 bind radio-profile id 1
 quit
radio ap-id 2 radio-id 0
 bind radio-profile id 1
 quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-
server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.3 192.168.1.128
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.2,192.168.2.3
#
return

```

**Configuration file of the standby AC:**

```

#
[board-bind]
<board-bind>
isolate port 0/2/0
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 0
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.3 255.255.255.0
dhcp enable
#
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.2.2 priority 2

```

```

wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id
1
quit
security-profile name security-1 id
1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile
security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile
security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
#
[ip-pool]
<ip-pool-standby>
ip pool standby
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.129 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.3,192.168.2.2
#
return

```

**Configuration file of the Layer 2 Switch:**

```

#
vlan batch 101 102 800
#
interface Ethernet0/0/1
port link-type trunk
port trunk pvid vlan 800
port trunk allow-pass vlan 101
800
port-isolate enable group 1
#
interface Ethernet0/0/2
port link-type trunk
port trunk pvid vlan 800
port trunk allow-pass vlan 102
800
port-isolate enable group 1
#
interface GigabitEthernet0/0/1
port link-type trunk

```

```
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 101 102
800
#
return
Configuration file of the Layer 3 Switch:
#
vlan batch 10 101 102 800
#
interface Vlanif10
ip address 192.168.2.1 255.255.255.0
#
interface Vlanif101
ip address 192.168.5.1 255.255.255.0
dhcp select interface
#
interface Vlanif102
ip address 192.168.6.1 255.255.255.0
dhcp select interface
#
interface Vlanif800
ip address 192.168.1.1 255.255.255.0
dhcp select relay
dhcp relay server-ip 192.168.2.2
dhcp relay server-ip 192.168.2.3
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 101 102 800
#
interface GigabitEthernet0/0/2
port hybrid tagged vlan 10 101 to 102
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 101 102
#
interface
GigabitEthernet0/0/4

port hybrid tagged vlan 10 101 to 102
#
return
```

### 4.3.7 Configuring QoS Policies for APs

When multiple APs are deployed in a region, you can configure different QoS policies for the APs to provide differentiated services.

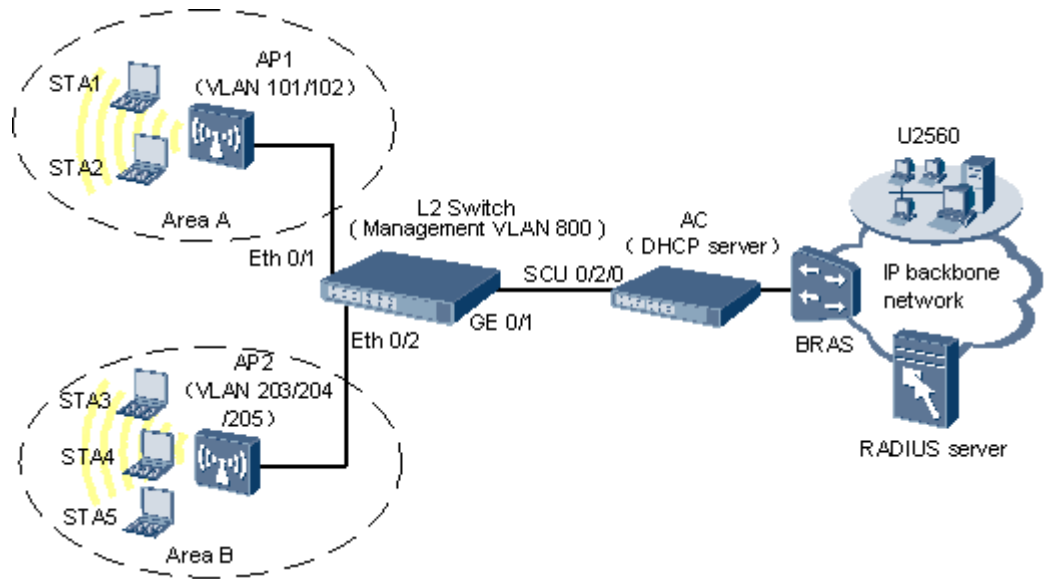
#### Networking Requirements

As shown in [Figure 4-9](#), STA1 and STA2 are connected to the Internet through AP1, and STA3, STA4, and STA5 are connected to the Internet through AP2. STA5 is a VIP user.

Voice data is processed first on AP1 and video data is processed first on AP2. When the network bandwidth is insufficient, the data of the VIP user must be processed first.



**Figure 4-9** Network topology for configuring QoS policies



**Table 4-7** Data plan

Configuration Item	Data
WLAN service	SSID: huawei-1 Traffic profile: huawei VLAN: 101 VLAN priority: 4
	SSID: huawei-2 Traffic profile: huawei VLAN: 102 VLAN priority: 5
	SSID: huawei-3 Traffic profile: huawei VLAN: 203 VLAN priority: 4
	SSID: huawei-4 Traffic profile: huawei-vip VLAN: 204 VLAN priority: 6

Configuration Item	Data
	SSID: huawei-5 Traffic profile: huawei-vip VLAN: 205 VLAN priority: 5
Radio profiles of APs	AP1 radio profile (huawei) and WMM profile (huawei)
	AP2 radio profile (huawei-vi) and WMM profile (huawei-vi)
Management VLAN ID for APs	VLAN 800 allocated by the Layer 2 switch
AP region	AP1: 101
	AP2: 102
Service VLAN ID for APs	AP1: VLAN 101 and VLAN 102
	AP2: VLAN 203, VLAN 204, and VLAN 205
VLAN IDs on the access switch	VLAN 800/101/102/203/204/205
Carrier ID/AC ID of the AC	CTC/1

## Data Preparation

- The CAPWAP tunnels between the AC and APs have been created.
- The AC can communicate with the APs.
- The APs support the WMM function.
- In tunnel forwarding mode, port 1 and port 2 of the switch cannot be added to service VLANs. In direct forwarding mode, port 1 and port 2 of the switch must be added to service VLANs. That is, the ports must allow all VLANs to pass.

## Procedure

### Step 1 Establish connections between the AC and the APs.

#### 1. Create VLANs.

```
Create VLANs 101, 102, 203, 204, 205, and 800.
```

```
huawei(config)#vlan 101 to 102
```

```
huawei(config)#vlan 203 to 205
```

```
huawei(config)#vlan 800
```

```
Map VLAN 101 and VLAN 203 to priority 4, VLAN 102 and VLAN 205 to priority 5,
and VLAN 204 to priority 6.
```

```
huawei(config)#vlan priority 101 4
```

```
huawei(config)#vlan priority 102 5
```

```
huawei(config)#vlan priority 203 4
```

```
huawei(config)#vlan priority 204 6
```

```
huawei(config)#vlan priority 205 5
```

2. Configure VLANs for the AC's port connected to APs.

```
Enable port 1 to support VLAN IDs 101, 102, 203, 204, and 205.
huawei(config)#port vlan 101 0/2 0
huawei(config)#port vlan 102 0/2 0
huawei(config)#port vlan 203 0/2 0
huawei(config)#port vlan 204 0/2 0
huawei(config)#port vlan 205 0/2 0
huawei(config)#port vlan 800 0/2 0
```

## Step 2 Configure profiles for the APs.

1. Create WMM profiles.

# Create WMM profile **huawei** and use the default settings. By default, the voice queue (AC\_VO) has a higher priority than the video queue (AC\_VI).

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wmm-profile name huawei id 1
huawei(config-wlan-wmm-prof-huawei)#quit
```

# Create WMM profile **huawei-vi**.

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wmm-profile name huawei-vi id 2
```

# Change the queue priority in WMM profile **huawei-vi** to ensure that the video queue has a higher priority than the voice queue.

```
huawei(config-wlan-wmm-prof-huawei-vi)#wmm edca ap ac-vi ecw ecwmin 1 ecwmax
 1 aifsn 1 txoplimit 36 ack-policy normal
huawei(config-wlan-wmm-prof-huawei-vi)#wmm edca client ac-vi ecw ecwmin 1
ecwmax 3
 aifsn 1 txoplimit 36
huawei(config-wlan-wmm-prof-huawei-vi)#quit
```

2. Create radio profiles.

# Create a radio profile named **huawei** and bind it to WMM profile **huawei**.

```
huawei(config-wlan-ac-view)#radio-profile name huawei id 1
huawei(config-wlan-radio-prof-huawei)#bind wmm-profile name huawei
huawei(config-wlan-radio-prof-huawei)#quit
```

# Create a radio profile named **huawei-vi** and bind it to WMM profile **huawei-vi**.

```
huawei(config-wlan-ac-view)#radio-profile name huawei-vi id 2
huawei(config-wlan-radio-prof-huawei-vi)#bind wmm-profile name huawei-vi
huawei(config-wlan-radio-prof-huawei-vi)#quit
```

3. Create a security profile.

# Create a security profile named **huawei**.

```
huawei(config-wlan-ac-view)#security-profile name huawei id 6
huawei(config-wlan-security-prof-huawei)#quit
```

4. Create traffic profiles.

# Create a traffic profile named **huawei**. Set the maximum downstream rate to 1024 kbit/s for the VAPs and to 512 kbit/s for the STAs.

```
huawei(config-wlan-ac-view)#traffic-profile name huawei id 1
huawei(config-wlan-traffic-prof-huawei)#rate-limit client down 512
huawei(config-wlan-traffic-prof-huawei)#rate-limit vap down 1024
huawei(config-wlan-traffic-prof-huawei)#quit
```

# Create a traffic profile named **huawei-vip**. Set the maximum downstream rate to 2048 kbit/s for the VAPs and to 1024 kbit/s for the STAs. Set the mapping mode to the designated mode and the priorities of upstream and downstream tunnels to 6.

```
huawei(config-wlan-ac-view)#traffic-profile name huawei-vip id 2
huawei(config-wlan-traffic-prof-huawei-vip)#rate-limit client down 1024
huawei(config-wlan-traffic-prof-huawei-vip)#rate-limit vap down 2048
huawei(config-wlan-traffic-prof-huawei-vip)#8021p designate 6
```

```

 huawei(config-wlan-traffic-prof-huawei-vip)#8021p-map-up 6 6 6 6 6 6 6
 huawei(config-wlan-traffic-prof-huawei-vip)#quit

```

### Step 3 Configure radios for APs.

```

Configure a radio for AP1 and bind it to radio profile huawei.
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name huawei
huawei(config-wlan-radio-1/0)#quit

Configure a radio for AP2 and bind it to radio profile huawei-vi.
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name huawei-vi
huawei(config-wlan-radio-2/0)#quit

```

### Step 4 Configure ESSs and SSIDs.

- # Create an ESS named **huawei-1**, specify SSID **huawei-1** for it, and bind traffic profile **huawei** and security profile **huawei** to it.
 

```

huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-1 traffic-profile huawei
security-profile huawei

Set the VLAN mapping mode to ESS-based mapping and map the ESS to VLAN 101.
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag vlan 101
Success: 1
Failure: 0

```
- # Create an ESS named **huawei-2**, specify SSID **huawei-2** for it, and bind traffic profile **huawei** and security profile **huawei** to it.
 

```

huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-2 traffic-profile huawei
security-profile huawei

Set the VLAN mapping mode to ESS-based mapping and map the ESS to VLAN 102.
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag vlan 102
Success: 1
Failure: 0

```
- # Create an ESS named **huawei-3**, specify SSID **huawei-3** for it, and bind traffic profile **huawei** and security profile **huawei-vi** to it.
 

```

huawei(config-wlan-ac-view)#ess name huawei-3 ssid huawei-3 traffic-profile huawei
security-profile huawei-vi

Set the VLAN mapping mode to ESS-based mapping and map the ESS to VLAN 203.
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-3 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-3 type tag vlan 203
Success: 1
Failure: 0

```
- # Create an ESS named **huawei-4**, specify SSID **huawei-4** for it, and bind traffic profile **huawei** and security profile **huawei** to it.
 

```

huawei(config-wlan-ac-view)#ess name huawei-4 ssid huawei-4 traffic-profile huawei
security-profile huawei

Set the VLAN mapping mode to ESS-based mapping and map the ESS to VLAN 204.
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-4 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-4 type tag vlan 204
Success: 1
Failure: 0

```
- # Create an ESS named **huawei-5**, specify SSID **huawei-5** for it, and bind traffic profile **huawei-vip** and security profile **huawei** to it.
 

```

huawei(config-wlan-ac-view)#ess name huawei-5 ssid huawei-5 traffic-profile huawei-vip
security-profile huawei

Set the VLAN mapping mode to ESS-based mapping and map the ESS to VLAN 205.

```

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-5 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-5 type tag vlan 205
Success: 1
Failure: 0
```

### Step 5 Deliver the WLAN service to the APs.

- Deliver VAP parameters to radio 0 of AP1.  
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1 wlan 2  
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-2 wlan 3  
huawei(config-wlan-ac-view)#commit ap 1
- Deliver VAP parameters to radio 0 of AP2.  
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-3 wlan 4  
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-4 wlan 5  
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-5 wlan 6  
huawei(config-wlan-ac-view)#commit ap 2

----End

## Result

Five WLANs with SSIDs **huawei-1**, **huawei-2**, **huawei-3**, **huawei-4**, and **huawei-5** are available for STAs connected to AP1 and AP2. STAs 1, 2, 3, 4, and 5 respectively select WLANs with SSIDs huawei-1, huawei-2, huawei-3, huawei-4, and huawei-5.

- The maximum rate of STA1, STA2, STA3, and STA4 is 512 kbit/s. The maximum rate of STA5 is 1024 kbit/s.
- Voice data is processed first for STA1 and STA2 connected to AP1. Video data is processed first for STA3 and STA4 connected to AP2.
- When the network bandwidth is insufficient, the following situations occur:
  - Because the priority of STA1 and STA3 is the lowest (4) among the STAs, voice communication will be interrupted first and the download speed will become slow on STA1 and STA3.
  - If the available bandwidth keeps decreasing, video communication will fail and subsequently voice communication will be interrupted on STA2.
  - If the available bandwidth keeps decreasing, the voice communication will be interrupted and subsequently the video communication may fail on STA4 and STA5. As the QoS policy for STA5 is mapped to the priority 6, STA4 and STA5, actually, share the same priority though the priority for STA5 is 5 and for STA4 is 6.

## Configuration Files

Configuration file on the AC

```
#
system-view
vlan 101 to 102
vlan 203 to 205
vlan 800
vlan priority 101 4
vlan priority 102 5
vlan priority 203 4
vlan priority 204 6
vlan priority 205 5
port vlan 101 0/2 0
port vlan 102 0/2 0
port vlan 203 0/2 0
port vlan 204 0/2 0
port vlan 205 0/2 0
port vlan 800 0/2 0
```

```
wlan ac
wmm-profile name huawei id 1
quit
wmm-profile name huawei-vi id 2
wmm edca ap ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
wmm edca client ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
quit
traffic-profile name huawei id 1
rate-limit client down 512
rate-limit vap down 1024
quit
traffic-profile name huawei-vip id 2
rate-limit client down 1024
rate-limit vap down 2048
8021p-map-up 6 6 6 6 6 6 6 6
8021p designate 6
quit
radio-profile name huawei id 1
bind wmm-profile id 1
quit
radio-profile name huawei-vi id 2
bind wmm-profile id 2
quit
security-profile huawei id 6
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 0
quit
ess name huawei-1 id 2 ssid huawei-1 traffic-profile huawei security-profile
huawei
ess name huawei-2 id 3 ssid huawei-2 traffic-profile huawei security-profile
huawei
ess name huawei-3 id 4 ssid huawei-3 traffic-profile huawei security-profile
huawei
ess name huawei-4 id 5 ssid huawei-4 traffic-profile huawei-vip security-profile
huawei
ess name huawei-5 id 6 ssid huawei-5 traffic-profile huawei-vip security-profile
huawei
vlan-mapping ess id 2 type tag vlan 101
vlan-mapping ess id 3 type tag vlan 102
vlan-mapping ess id 4 type tag vlan 203
vlan-mapping ess id 5 type tag vlan 204
vlan-mapping ess id 6 type tag vlan 205
vap ap 1 radio 0 ess id 2 wlan 2
vap ap 1 radio 0 ess id 3 wlan 3
vap ap 2 radio 0 ess id 4 wlan 4
vap ap 2 radio 0 ess id 5 wlan 5
vap ap 2 radio 0 ess id 6 wlan 6
```

### 4.3.8 Configuring Security Policies for APs

If multiple APs are deployed in a region, you can configure different security policies for the APs to provide differentiated access control.

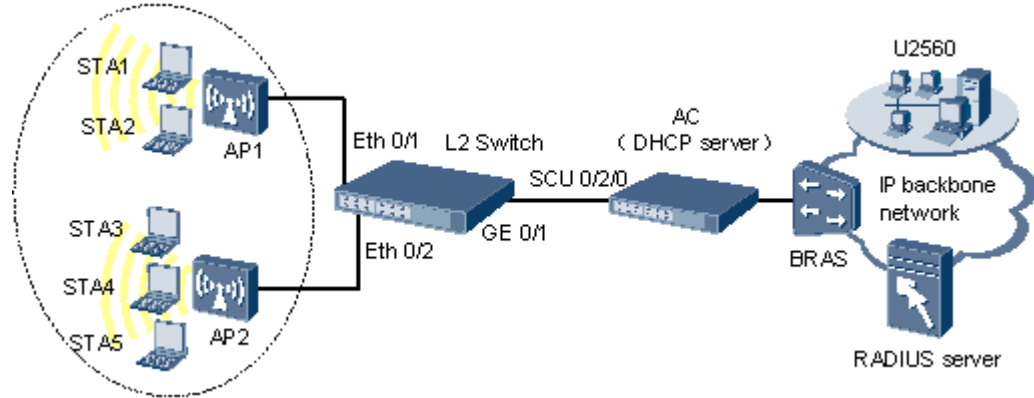
#### Networking Requirements

As shown in [Figure 4-10](#), AP1 and AP2 provide WLAN service for STAs 1 to 5. The WLANs available for the STAs are described as follows:

- WLAN with SSID huawei-1 uses OPEN-SYS authentication.
- WLAN with SSID huawei-2 uses shared key authentication and WEP-104 encryption.
- WLAN with SSID huawei-3 uses WPA1 authentication and TKIP encryption.

- WLAN with SSID huawei-4 uses WPA2 authentication and CCMP encryption.
- WLAN with SSID huawei-5 uses WAPI authentication.

**Figure 4-10** Network topology for configuring security policies



**Table 4-8** Data plan

Configuration Item	Data
Access security policy	<ul style="list-style-type: none"> <li>● Security profile: security-1</li> <li>● SSID: huawei-1</li> <li>● Authentication mode: OPEN-SYS authentication</li> </ul>
	<ul style="list-style-type: none"> <li>● Security profile: security-2</li> <li>● SSID: huawei-2</li> <li>● Authentication mode: shared key authentication</li> <li>● Encryption mode: WEP-104</li> <li>● Key: decimal ABCDEFGHIJKL1, ABCDEFGHIJKL2, ABCDEFGHIJKL3, and ABCDEFGHIJKL4</li> </ul>
	<ul style="list-style-type: none"> <li>● Security profile: security-3</li> <li>● SSID: huawei-3</li> <li>● Authentication mode: WPA1 (802.1x+PEAP)</li> <li>● Encryption mode: TKIP</li> </ul>
	<ul style="list-style-type: none"> <li>● Security profile: security-4</li> <li>● SSID: huawei-4</li> <li>● Authentication mode: WPA2 (802.1x+SIM)</li> <li>● Encryption mode: CCMP</li> </ul>
	<ul style="list-style-type: none"> <li>● Security profile: security-5</li> <li>● SSID: huawei-5</li> <li>● Authentication mode: WAPI (certificate authentication)</li> </ul>

Configuration Item	Data
ASU server's IP address	10.10.10.1/24

## Prerequisite

- The CAPWAP tunnels between the AC and APs have been created.
- The AC and APs can communicate properly. AP1 and AP2 are working properly.
- The AC certificate file **huawei-ap.cer** and ASU certificate file **huawei-asu.cer** have been saved in the flash memory on the AC. The AC's private key file is **ac-key.key**.
- The user name, password, and AAA user information has been configured on the RADIUS server.
- Wireless network configuration has been completed on the STA.

### NOTE

Step 1 to step 3 are the same as those in [4.3.1 Example for Configuring Services for Layer 2 Chain Networking \(Data Forwarded by Tunnel\)](#), so the configuration details are not provided here.

When configuring security profile security-3, use 802.1x authentication and matching encryption mode for WPA.

When configuring security profile security-4, use 802.1x authentication and matching encryption mode for WPA2.

## Procedure

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

**Step 2** Configure basic AC functions.

**Step 3** Configure APs and make APs go online.

**Step 4** Configure radios for APs.

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

```
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #wmm-profile name wmm id 1
huawei (config-wlan-wmm-prof-wmm) #quit
```

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

```
huawei (config-wlan-ac-view) #radio-profile name radio
huawei (config-wlan-radio-prof-radio) #bind wmm-profile name wmm
huawei (config-wlan-radio-prof-radio) #quit
```

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

```
huawei (config-wlan-ac-view) #radio ap-id 0 radio-id 0
huawei (config-wlan-radio-0/0) #bind radio-profile name radio
huawei (config-wlan-radio-0/0) #quit
huawei (config-wlan-ac-view) #radio ap-id 1 radio-id 0
huawei (config-wlan-radio-1/0) #bind radio-profile name radio
huawei (config-wlan-radio-1/0) #quit
```

**Step 5** Configure the RADIUS server and AAA schemes, and set the domain name.

```
huawei (config) #radius-server template peap.radius.com
```



```

huawei (config-radius-peap.radius.com) #radius-server authentication 10.137.146.163
1812
huawei (config-radius-peap.radius.com) #radius-server accounting 10.137.146.163 1813
huawei (config-radius-peap.radius.com) #radius-server shared-key huawei
huawei (config-radius-peap.radius.com) #quit
huawei (config) #aaa
huawei (config-aaa) #authentication-scheme radius
huawei (config-aaa-authen-radius) #authentication-mode radius
huawei (config-aaa-authen-radius) #quit
huawei (config-aaa) #accounting-scheme radius
huawei (config-aaa-accounting-radius) #accounting-mode radius
huawei (config-aaa-accounting-radius) #quit
huawei (config-aaa) #domain peap.radius.com
huawei (config-aaa-domain-peap.radius.com) #authentication-scheme radius
huawei (config-aaa-domain-peap.radius.com) #accounting-scheme radius
huawei (config-aaa-domain-peap.radius.com) #radius-server peap.radius.com
huawei (config-aaa-domain-peap.radius.com) #quit

```

**Step 6** Enable 802.1x and global MAC address-based control for 802.1x when WPA1 or WPA2 authentication is used.

```

huawei (config) #dot1x enable
huawei (config) #dot1x mac-control

```

**Step 7** Create security profiles security-1, security-2, security-3, security-4, and security-5.

```

huawei (config) #wlan ac
huawei (config-wlan-ac-view) #security-profile name security-1 id 1
huawei (config-wlan-security-prof-security-1) #quit
huawei (config-wlan-ac-view) #security-profile name security-2 id 2
huawei (config-wlan-security-prof-security-2) #quit
huawei (config-wlan-ac-view) #security-profile name security-3 id 3
huawei (config-wlan-security-prof-security-3) #quit
huawei (config-wlan-ac-view) #security-profile name security-4 id 4
huawei (config-wlan-security-prof-security-4) #quit
huawei (config-wlan-ac-view) #security-profile name security-5 id 5
huawei (config-wlan-security-prof-security-5) #quit

```

**Step 8** Configure security profiles.

- Configure a security policy for security profile security-1.

# Set the authentication mode to open-system.

```

huawei (config-wlan-ac-view) #security-profile name security-1 id 1
huawei (config-wlan-security-prof-security-1) #policy wep open-system

```

- Configure a security policy for security profile security-2.

# Set the authentication mode to shared-key.

```

huawei (config-wlan-ac-view) #security-profile name security-2 id 2
huawei (config-wlan-security-prof-security-2) #policy wep share-key

```

# Set the encryption mode to WEP-104 and the key to ABCDEFGHIJKL1,

ABCDEFGHIJKL2, ABCDEFGHIJKL3, and ABCDEFGHIJKL4 in decimal notation.

```

huawei (config-wlan-security-prof-security-2) #wep key wep-104 pass-phrase 0
ABCDE
FGHIJKL1
huawei (config-wlan-security-prof-security-2) #wep key wep-104 pass-phrase 1
ABCDE
FGHIJKL2
huawei (config-wlan-security-prof-security-2) #wep key wep-104 pass-phrase 2
ABCDE
FGHIJKL3
huawei (config-wlan-security-prof-security-2) #wep key wep-104 pass-phrase 3
ABCDE
FGHIJKL4

```

 **NOTE**

The WEP data encryption mode requires an encryption key.

# Set the authentication policy to wep.

```
huawei(config-wlan-security-prof-security-2)#authentication policy wep
huawei(config-wlan-security-prof-security-2)#quit
```

- Configure a security policy for security profile security-3.

# Set the authentication mode to WPA1 (802.1x+PEAP) and use the TKIP encryption mode.

```
huawei(config-wlan-ac-view)#security-profile name security-3 id 3
huawei(config-wlan-security-prof-security-3)#policy wpa1 tkip 802dot1x peap
```

# Set the authentication policy to wpa1.

```
huawei(config-wlan-security-prof-security-3)#authentication policy wpa1
huawei(config-wlan-security-prof-security-3)#quit
```

- Configure a security policy for security profile security-4.

# Set the authentication mode to WPA2 (802.1x+SIM) and use the CCMP encryption mode.

```
huawei(config-wlan-ac-view)#security-profile name security-4 id 4
huawei(config-wlan-security-prof-security-4)#policy wpa2 ccmp 802dot1x sim
```

# Set the authentication policy to wpa2.

```
huawei(config-wlan-security-prof-security-4)#authentication policy wpa2
huawei(config-wlan-security-prof-security-4)#quit
```

- Configure a security policy for security profile security-5.

# Set the authentication mode to WPAI (certification authentication).

```
huawei(config-wlan-ac-view)#security-profile name security-5 id 5
huawei(config-wlan-security-prof-security-5)#wapi wai certificate
```

# Set the ASU server's IP address to 10.10.10.1, AC certificate file to huawei-ap.cer, ASU certificate file to huawei-asu.cer, AC private key certificate file to huawei-private.cer, and issuer certificate file to huawei-issuer.cer.

#### NOTE

- A security profile can be bound to only one CA certificate, one AC certificate, and one ASU certificate.
- You must load either the ASU certificate or issuer certificate.

```
huawei(config-wlan-security-prof-security-5)#wapi asu-server ip 10.10.10.1
huawei(config-wlan-security-prof-security-5)#wapi certificate ac import file-
name huawei
-ac.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate issuer import
file-name hua
wei-issuer.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate asu import file-
name huawe
i-asu.cer
huawei(config-wlan-security-prof-security-5)#wapi private-key import file-name
ac-key.key
...
```

# Set the authentication policy to wapi.

```
huawei(config-wlan-security-prof-security-5)#authentication policy wapi
huawei(config-wlan-security-prof-security-5)#quit
```

## Step 9 Configure ESSs and create VAPs.

- # Create an ESS named **ESS-1**, set its SSID to **huawei-1**, and bind it to traffic profile **ctc** and security profile **security-1**. Deliver VAP parameters to radio 0 of AP1 and set the WLAN ID to 1.

```
huawei(config-wlan-ac-view)#traffic-profile name ctc
huawei(config-wlan-traffic-prof-ctc)#quit
huawei(config-wlan-ac-view)#ess name ess-1 ssid huawei-1 traffic-profile ctc
security-profile security-1
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-1 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-1 type tag vlan 101
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name ess-1
huawei(config-wlan-ac-view)#commit ap 1
```

- # Create an ESS named **ESS-2**, set its SSID to **huawei-2**, and bind it to traffic profile **ctc** and security profile **security-2**. Deliver VAP parameters to radio 0 of AP1 and set the WLAN ID to 1.
 

```

huawei(config-wlan-ac-view)#ess name ess-2 ssid huawei-2 traffic-profile ctc
security-profile security-2
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-2 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-2 type tag vlan 101
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name ess-2
huawei(config-wlan-ac-view)#commit ap 1

```
- # Create an ESS named **ESS-3**, set its SSID to **huawei-3**, and bind it to traffic profile **ctc** and security profile **security-3**. Deliver VAP parameters to radio 0 of AP2 and set the WLAN ID to 1.
 

```

huawei(config-wlan-ac-view)#ess name ess-3 ssid huawei-3 traffic-profile ctc
security-profile security-3
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-3 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-3 type tag vlan 102
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name ess-3
huawei(config-wlan-ac-view)#commit ap 2

```
- # Create an ESS named **ESS-4**, set its SSID to **huawei-4**, and bind it to traffic profile **ctc** and security profile **security-4**. Deliver VAP parameters to radio 0 of AP2 and set the WLAN ID to 1.
 

```

huawei(config-wlan-ac-view)#ess name ess-4 ssid huawei-4 traffic-profile ctc
security-profile security-4
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-4 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-4 type tag vlan 102
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name ess-4
huawei(config-wlan-ac-view)#commit ap 2

```
- # Create an ESS named **ESS-5**, set its SSID to **huawei-5**, and bind it to traffic profile **ctc** and security profile **security-5**. Deliver VAP parameters to radio 0 of AP2 and set the WLAN ID to 1.
 

```

huawei(config-wlan-ac-view)#ess name ess-5 ssid huawei-5 traffic-profile ctc
security-profile security-5
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-5 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-5 type tag vlan 102
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name ess-5
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit

```

----End

## Result

Five WLANs whose SSIDs are respectively huawei-1, huawei-2, huawei-3, huawei-4, and huawei-5 are available for AP1 and AP2.

- On the WLAN with SSID huawei-1, STAs can use the WLAN service without authentication.
- On the WLAN with SSID huawei-2, STAs can use the WLAN service only when they have the shared key.
- On the WLAN with SSID huawei-3 or huawei-4, STAs can use the WLAN service only when they pass 802.1x authentication.
- On the WLAN with SSID huawei-5, STAs can use the WLAN service only when they have the required certificate.

## Configuration Files

The configuration file on the AC in this configuration example is as follows:

```

#
[vlan-config]

```

```

 <vlan-config>
vlan 101 to 102
#
[config]
 <config>
dot1x enable
dot1x mac-control
#
[radius]
 <radius>
radius-server template "peap.radius.com"
radius-server authentication 10.137.146.163 1812
radius-server accounting 10.137.146.163 1813
#
[aaa]
 <aaa>
aaa
authentication-scheme "radius"
authentication-mode radius
#
accounting-scheme "radius"
accounting-mode radius
#
domain "peap.radius.com"
authentication-scheme "radius"
accounting-scheme "radius"
radius-server "peap.radius.com"
#
[wlan-ac-view]
wlan ac
wmm-profile name wmm id 1
quit
traffic-profile name ctc id 2
quit
security-profile name security-1 id 1
quit
security-profile name security-2 id 2
policy wep share-key
wep key wep-104 pass-phrase 0 ABCDEFGHIJKL1
wep key wep-104 pass-phrase 1 ABCDEFGHIJKL2
wep key wep-104 pass-phrase 2 ABCDEFGHIJKL3
wep key wep-104 pass-phrase 3 ABCDEFGHIJKL4
quit
security-profile name security-3 id 3
authentication policy wpa1
policy wpa1 tkip 802dot1x peap
quit
security-profile name security-4 id 4
authentication policy wpa2
policy wpa2 ccmp 802dot1x sim
quit
security-profile name security-5 id 5
authentication policy wapi
wapi asu-server ip 10.10.10.1
quit
radio-profile name radio id 2
bind wmm-profile id 1
quit
radio ap-id 0 radio-id 0
bind radio-profile id 2
quit
radio ap-id 1 radio-id 0
bind radio-profile id 2
quit
ess name ess-1 id 1 ssid huawei-1 traffic-profile ctc security-profile
security-1
ess name ess-2 id 2 ssid huawei-2 traffic-profile ctc security-profile
security-2
ess name ess-3 id 3 ssid huawei-3 traffic-profile ctc security-profile

```

```

security-3
 ess name ess-4 id 4 ssid huawei-4 traffic-profile ctc security-profile
security-4
 ess name ess-5 id 5 ssid huawei-5 traffic-profile ctc security-profile
security-5
 vlan-mapping ess id 1 type tag vlan 101
 vlan-mapping ess id 2 type tag vlan 101
 vlan-mapping ess id 3 type tag vlan 102
 vlan-mapping ess id 4 type tag vlan 102
 vlan-mapping ess id 5 type tag vlan 102
#
return

```

### 4.3.9 Example for Configuring an AP Load Balancing Group

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

#### Networking

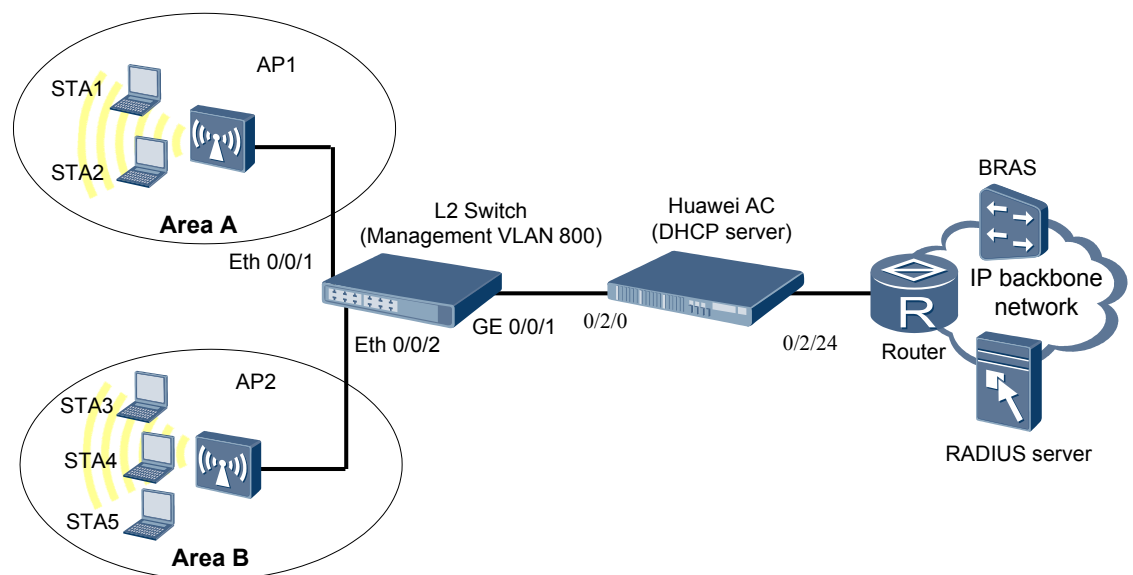
On a WLAN in centralized control mode, the association between a STA and an AP must be permitted by the AC. A STA scans APs and sends association requests to the APs. Regardless of the MAC address that is used, the APs forward the association requests to the AC. Then, according to the AC's policies, the AC will determine which AP is the best for the STA to associate with.

An Internet service provider (ISP) provides the WLAN service for two neighboring areas A and B. AP1 provides the WLAN service for region A, and AP2 provides the WLAN service for region B. After an AP load balancing group on an AC is configured, the AC controls user access according to the policies configured in the load balancing group.

The AC and APs are connected through a Layer 2 network in chain mode, as shown in [Figure 4-11](#).

The AC also functions as a DHCP server to allocate IP addresses to the APs and sends its IP address to the APs using Option 43.

**Figure 4-11** Layer 2 chain networking (tunnel forwarding)



## Prerequisites

- The AP, AC, and Layer 2 switch are working properly.
- The functions of the router, broadband remote access server (BRAS), and AAA/Web server have been verified.
- Authentication and accounting configurations have been performed on the BRAS.

## Data Plan

**Table 4-9** Data plan

Configuration Item	Data
WLAN service	AP authentication: WEP authentication policy and Open-system authentication
	Encryption type of authentication packets: non-encryption
Management VLAN ID for APs	VLAN 800 (with VLAN tags added by the Layer 2 switch)
AP Region	AP1: 101
	AP2: 102
VLANs on the Layer 2 switch	Port connecting to the APs: Its link type is Access and default VLAN ID is 800; port connecting to the AC: Its link type is Trunk and it transmits packets whose VLAN ID is 800. Data flows of management and service VLANs are transmitted over Control And Provisioning of Wireless Access Points (CAPWAP) tunnels.
AC Carrier ID/AC ID	CTC/1
IP address of the management interface (Meth 0) on the AC	10.11.104.2/24
IP address pool of APs	192.168.1.2 to 192.168.1.254/24
Gateway IP address for APs	192.168.1.1/24
DHCP server	AC functioning as the DHCP server to allocate IP addresses to the APs

## Procedure

**Step 1** Configure the Layer 2 switch so that APs can communicate with the AC at Layer 2.

1. Configure the link type of ports ETH 0/0/1 and ETH 0/0/2 on the Layer 2 switch connected to APs as Access and VLAN ID as VLAN 800.

 **NOTE**

In this example, Huawei S3300 is used. If a switch of other series is used, see the relevant command reference.

**CAUTION**

Configure port isolation on all downstream ports of the Layer 2 switching in the management VLANs and service VLANs. If the ports are not isolated, unnecessary broadcast packets may exist on the VLAN or WLAN users of different APs may be unable to communicate with each other at Layer 2.

```
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type access
[huawei-Ethernet0/0/1]port default vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type access
[huawei-Ethernet0/0/2]port default vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. Configure the link type of port GE 0/0/1 on the Layer 2 switch connected to the AC as Trunk and VLAN ID as VLAN 800.

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

**Step 2** Configure basic functions on the AC.

1. Set global AC parameters (carrier ID and global ID).  
# Set the carrier ID of the AC to cmcc (for China Mobile), ctc (for China Telecom), cuc (for China Unicom), or other (for other carriers). Set the global AC ID to 1.  
huawei (config) #wlan ac-global carrier id ctc ac id 1
2. Configure VLANs for ports between the AC and the Layer 2 switch.  
# Create VLAN 101, 102, and 800.  
huawei (config) #vlan 101  
huawei (config) #vlan 102  
huawei (config) #vlan 800  
# Add service port 0/2/0 to VLAN 800.  
huawei (config) #port vlan 800 0/2 0
3. Configure the upstream port of the AC.  
# Add VLAN 101 and VLAN 102 to upstream port 0/2/24.  
huawei (config) #port vlan 101 0/2 24  
huawei (config) #port vlan 102 0/2 24
4. Create a VLANIF interface on the AC.  
# Configure an IP address 192.168.1.1 for VLANIF 800 so that data packets are forwarded at Layer 3 through VLANIF 800.  
huawei (config) #interface vlanif 800  
huawei (config-if-vlanif800) #ip address 192.168.1.1 255.255.255.0  
{ <cr>|description<K>|sub<K> }:  
  
Command:  
ip address 192.168.1.1 255.255.255.0  
# Enable the DHCP function for VLANIF 800 so that the AC can function as the DHCP server to allocate IP addresses to APs.

```
huawei (config-if-vlanif800)#dhcps enable
huawei (config-if-vlanif800)#quit
```

 **NOTE**

- An AP can set up a connection with an AC only after obtaining an IP address from the AC, a BRAS, or a DHCP server.
- In this example, APs obtain IP addresses from the AC.

5. Specify the source IP address for the AC.

# Specify VLANIF 800 as the source interface for the AC.

 **NOTE**

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

```
huawei (config)#wlan ac
huawei (config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei (config-wlan-ac-view)#quit
```

6. Configure an IP address pool for APs on the AC.

# Map the IP address pool **ctc-ap-server** to VLAN 800.

 **NOTE**

The gateway IP address in the IP address pool must be the same as the IP address of the VLANIF interface. After APs go online, they obtain IP addresses from this IP address pool.

```
huawei (config)#ip pool ap-server
 It's successful to create an IP address pool
huawei (config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei (config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
```

# (Optional) Configure DHCP Option 60 and Option 43 so that APs can learn the AC's IP address using Option 43.

```
huawei (config-ip-pool-ap-server)#option 60 string Huawei AP
huawei (config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.1.1
huawei (config-ip-pool-ap-server)#quit
```

 **NOTE**

- The text information must be **Huawei AP** for Option 60.
- The text information must be **HuaweiAC-X.X.X.X** for Option 43. *X.X.X.X* indicates the IP address of the AC.

**Step 3** Connect the AC to APs.

1. Set the authentication mode of the APs to **sn-auth**.

```
huawei (config)#wlan ac
huawei (config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. Add APs offline.

# Query the AP device type.

```
huawei (config-wlan-ac-view)#display ap-type all
 All AP types
information:
```

```

 ID
 Type

```

```
 0
 WA601
 1
 WA631
 2
 WA651
 3
 WA602
```



```

4
WA632
5
WA652
6
WA603SN
7
WA603DN
8
WA633SN
11
WA603DE
12
WA653DE
14
WA653SN

```

```

Total number: 12

Add AP1 and AP2 of the WA601 type offline according to the obtained device type ID
(0). The SN of AP1 is SN000001 and the SN of AP2 is SN000002.
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002

Enable the AP to get online. The AP enters the normal state after it goes online.
huawei(config-wlan-ac-view)#display ap all
All AP information:

```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

```

Total number: 2

```

#### Step 4 Configure an AP load balancing group.

Create a load balancing group and enter the group view.

```

huawei(config-wlan-ac-view)#load-balance-group id 0 name Balanced_Group0
huawei(config-wlan-load-group-Balanced_Group0)

```

1. Add a radio to a specified radio load balancing group.

```

huawei(config-wlan-load-group-Balanced_Group0)#member ap-id 1 radio-id 0
huawei(config-wlan-load-group-Balanced_Group0)#member ap-id 2 radio-id 0

```

2. Set the load balancing mode to traffic mode.

```

huawei(config-wlan-load-group-Balanced_Group0)#traffic gap 40

```

 **NOTE**

To set the load balancing mode to session mode, you only need to change **traffic gap 40** to **session gap gap-threshold**. The value of *gap-threshold* ranges from 1 to 100.

3. Set the maximum number of association requests.

```

huawei(config-wlan-load-group-Balanced_Group0)#associate-threshold 8

```

----End

## Configuration Files

Configuration file of the AC:

```

#
wlan ac-global carrier id ctc ac id 1
vlan 101
vlan 102
vlan 800
port vlan 800 0/2 0

```

```
port vlan 101 0/2 24
port vlan 102 0/2 24
interface vlanif 800
ip address 192.168.1.1 255.255.255.0
dhcp enable
quit
wlan ac
wlan ac source interface vlanif 800
quit
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.1.1
quit
wlan ac
ap-auth-mode sn-auth
quit
ap id 1 type-id 0 sn SN000001
ap id 2 type-id 0 sn SN000002
quit
load-balance-group name Balanced_Group0 id 0
 associate-threshold 8
 session gap 8
 member ap-id 1 radio-id 0
 member ap-id 2 radio-id 0
quit
```

# 5 Protocol Configurations

---

## About This Chapter

Protocol configurations include the configurations of some common protocols. There is no logical relationship between protocol configurations. You can perform protocol configurations according to actual requirements.

### [5.1 Configuring Routing](#)

This section provides examples for configuring a routing policy and routing protocols supported by the AC.

### [5.2 Configuring DHCP](#)

An AC provides the DHCP relay function, enabling users dynamically to obtain IP addresses from a DHCP server on a network.

### [5.3 Configuring AAA](#)

This section describes how to configure authentication, authorization, and accounting (AAA) on the AC, including the configuration of the AC as the local or remote server.

### [5.4 Configuring MSTP](#)

The AC provides Multiple Spanning Tree Protocol (MSTP) functions and is compatible with the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP). The AC supports the MSTP ring network to meet network topology requirements.

### [5.5 Configuring Ethernet CFM OAM](#)

This section describes how to configure Ethernet CFM OAM on the AC.

## 5.1 Configuring Routing

This section provides examples for configuring a routing policy and routing protocols supported by the AC.

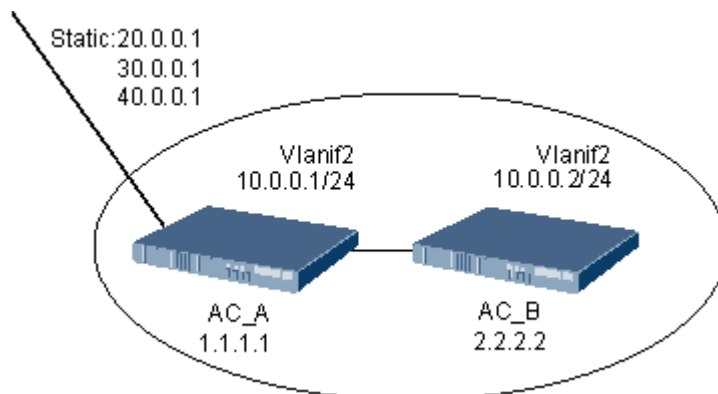
### 5.1.1 Example for Configuring a Routing Policy

This section describes how to configure a routing policy.

#### Service Requirements

- AC\_A and AC\_B run OSPF and are located in Area 0.
- Import external static routes to AC\_A and configure a routing policy on AC\_B.

**Figure 5-1** Network topology of the routing policy configuration



#### Procedure

##### Step 1 Configure AC\_A.

1. Assign an IP address to the VLANIF interface on AC\_A.
 

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.0.0.1 24
huawei(config-if-vlanif2)#quit
```
2. Enable OSPF on AC\_A and specify the area ID for an interface.
 

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.0.0.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```
3. Configure the OSPF router ID of AC\_A.
 

```
huawei(config)#router id 1.1.1.1
```
4. Configure three static routes.

```
huawei(config)#ip route-static 20.0.0.1 32 vlanif 2 10.0.0.2
huawei(config)#ip route-static 30.0.0.1 32 vlanif 2 10.0.0.2
huawei(config)#ip route-static 40.0.0.1 32 vlanif 2 10.0.0.2
```

5. Import static routes into OSPF.

```
huawei(config)#ospf
huawei(config-ospf-1)#import-route static
huawei(config-ospf-1)#quit
```

6. Save the configuration.

```
huawei(config)#save
```

## Step 2 Configure AC\_B.

1. Assign an IP address to the VLANIF interface on AC\_B.

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.0.0.2 24
huawei(config-if-vlanif2)#quit
```

2. Configure an ACL.

```
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule deny source 30.0.0.0 255.255.255.0
huawei(config-acl-basic-2000)#rule permit source any
huawei(config-acl-basic-2000)#quit
```

3. Enable OSPF on AC\_B and specify the area ID for an interface.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.0.0.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Configure the OSPF router ID of AC\_B.

```
huawei(config)#router id 2.2.2.2
```

5. Configure OSPF to filter the received external routes.

```
huawei(config)#ospf
huawei(config-ospf-1)#filter-policy 2000 import
huawei(config-ospf-1)#quit
```

6. Save the configuration.

```
huawei(config)#save
```

----End

## Result

1. AC\_A and AC\_B can run OSPF and can communicate with each other.
2. According to the route filtering rule configured on AC\_B, you can see routes on subnets 20.0.0.0 and 40.0.0.0, but cannot see the routes on 30.0.0.0.

## Configuration Files

### Configuration file of AC\_A

```
vlan 2
port vlan 2 0/2 0
interface vlanif 2
ip address 10.0.0.1 24
quit
ospf
area 0
network 10.0.0.0 0.0.0.255
quit
```

```
quit
router id 1.1.1.1
ip route-static 20.0.0.1 32 vlanif 2 10.0.0.2
ip route-static 30.0.0.1 32 vlanif 2 10.0.0.2
ip route-static 40.0.0.1 32 vlanif 2 10.0.0.2
ospf
import-route static
quit
save
```

#### Configuration file of AC\_B

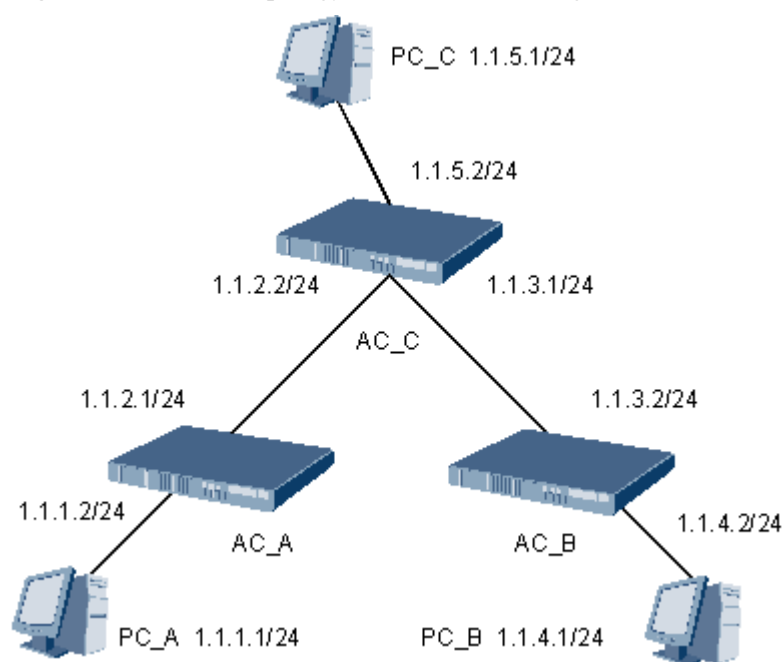
```
vlan 2
port vlan 2 0/2 0
interface vlanif 2
ip address 10.0.0.1 24
acl 2000
rule deny source 30.0.0.0 255.255.255.0
rule permit source any
quit
ospf
area 0
network 10.0.0.0 0.0.0.255
quit
quit
router id 2.2.2.2
ospf
filter-policy 2000 import
quit
save
```

## 5.1.2 Example for Configuring Static Routes

This section describes how to manually add static routes to implement communication between ACs.

### Service Requirements

Configure static routes on AC\_A, AC\_B, and AC\_C that provide router function so that any two PCs can communicate.

**Figure 5-2** Network topology of static route configuration

## Prerequisite

The native VLAN has been configured on the uplink port of each AC so that ACs can communicate.

## Procedure

**Step 1** Assign an IP address to the VLANIF interface.

The configuration methods on the three ACs are the same. The configuration of AC\_A is used as an example.

```
huawei (config) #vlan 2
huawei (config) #port vlan 2 0/2 0
huawei (config) #interface vlanif 2
huawei (config-if-vlanif2) #ip address 1.1.1.2 24
huawei (config-if-vlanif2) #ip address 1.1.2.1 24 sub
huawei (config-if-vlanif2) #quit
```

**Step 2** Configure static routes.

1. Configure a static route on AC\_A.

```
huawei (config) #ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
huawei (config) #ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

2. Configure a static route on AC\_B.

```
huawei (config) #ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
huawei (config) #ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

3. Configure a static route on AC\_C.

```
huawei (config) #ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
huawei (config) #ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

**Step 3** Configure gateway IP addresses of user hosts.

1. Configure the default gateway IP address to 1.1.1.2 on PC\_A.
2. Configure the default gateway IP address to 1.1.4.2 on PC\_B.
3. Configure the default gateway IP address to 1.1.5.2 on PC\_C.

**Step 4** Save the configuration.

```
huawei (config) #save
```

----End

## Result

All user hosts or ACs can communicate with each other.

## Configuration Files

Configuration file of AC\_A

```
vlan 2
port vlan 2 0/2 0
interface vlanif 2
ip address 1.1.1.2 24
ip address 1.1.2.1 24 sub
quit
ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

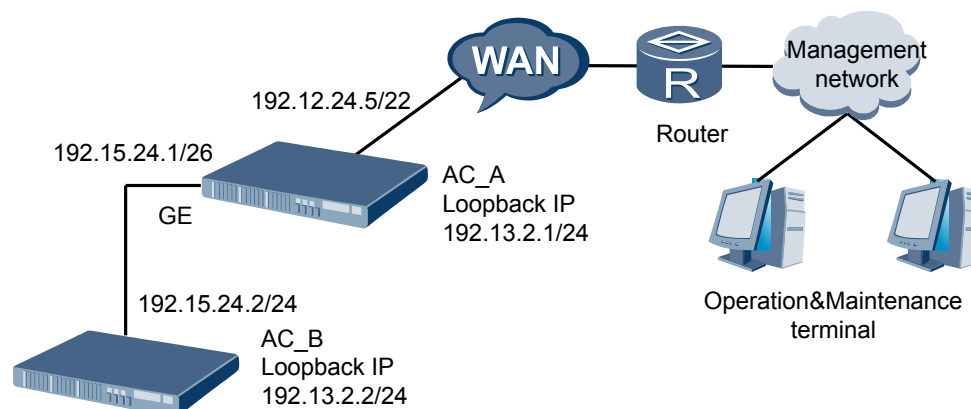
### 5.1.3 Example for Configuring RIP

This section describes how to configure RIP.

#### Service Requirements

- AC\_A is cascaded with AC\_B through port 0/2/16, uses port 0/2/24 to transmit incoming traffic, and connects to the management center network through the WAN.
- RIP is enabled on AC\_A and AC\_B so that administrators can log in to AC\_A and AC\_B through RIP routes to operate and maintain them.

**Figure 5-3** Network topology of RIP configuration





## Data Plan

**Table 5-1** lists the data plan of RIP configuration.

**Table 5-1** Data plan of RIP configuration

Configuration Item	Data
AC_A	Uplink port: 0/2/24 Management VLAN ID: 100 IP address of the VLANIF interface of the management VLAN: 192.13.24.5/22 IP address of the loopback interface: 192.13.2.1/24
	RIP version: V2 RIP route filtering policy: filters routes based on the IP address prefix list <b>abc</b> and allows only the routes with the IP addresses of 192.13.2.1 and 192.13.2.2 to be advertised through VLANIF 100.
	Cascading port: 0/2/16 Cascading management VLAN ID: 10 IP address of the VLANIF interface of the cascading management VLAN: 192.15.24.1/26
AC_B	Cascading port: 0/2/16 Management VLAN ID: 10 IP address of the VLANIF interface of the management VLAN: 192.15.24.2/26 IP address of the loopback interface: 192.13.2.2/24
	RIP version: V2 RIP route filtering policy: filters routes based on the IP address prefix list <b>abc</b> and allows only the routes with the IP address of 192.13.2.2 to be advertised through VLANIF 10.

## Procedure

- Configure AC\_A.
  1. Assign IP addresses to the VLANIF interface and loopback interface.
 

```

 huawei (config) #vlan 100
 huawei (config) #port vlan 100 0/2 24
 huawei (config) #interface vlanif 100
 huawei (config-if-vlanif100) #ip address 192.13.24.5 22
 huawei (config-if-vlanif100) #quit
 huawei (config) #interface loopBack 0
 huawei (config-if-loopback0) #ip address 192.13.2.1 24
 huawei (config-if-loopback0) #quit

```
  2. Enable RIP.
 

```

 huawei (config) #rip 1
 huawei (config-rip-1) #network 192.13.24.0
 huawei (config-rip-1) #network 192.13.2.0

```

- ```

huawei(config-rip-1)#version 2
huawei(config-rip-1)#quit

```
3. Configure a route filtering policy.

```

huawei(config)#ip ip-prefix abc permit 192.13.2.1 32
huawei(config)#ip ip-prefix abc permit 192.13.2.2 32
huawei(config)#rip 1
huawei(config-rip-1)#filter-policy ip-prefix abc export vlanif 100
huawei(config-rip-1)#quit

```
 4. Configure the cascading port.

```

huawei(config)#vlan 10
huawei(config)#port vlan 10 0/2 16
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 192.15.24.1 26
huawei(config-if-vlanif10)#quit

```
 5. Enable RIP on the cascading port.

```

huawei(config)#rip 1
huawei(config-rip-1)#network 192.15.24.0
huawei(config-rip-1)#quit

```
 6. Save the configuration.

```

huawei(config)#save

```
- Configure AC_B.
 1. Assign IP addresses to the VLANIF interface and loopback interface.

```

huawei(config)#vlan 10
huawei(config)#port vlan 10 0/2 16
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 192.15.24.2 26
huawei(config-if-vlanif10)#quit
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 192.13.2.2 24
huawei(config-if-loopback0)#quit

```
 2. Enable RIP.

```

huawei(config)#rip 1
huawei(config-rip-1)#network 192.15.24.0
huawei(config-rip-1)#network 192.13.2.0
huawei(config-rip-1)#version 2
huawei(config-rip-1)#quit

```
 3. Configure a route filtering policy.

```

huawei(config)#ip ip-prefix abc permit 192.13.2.2 32
huawei(config)#rip 1
huawei(config-rip-1)#filter-policy ip-prefix abc export vlanif 10
huawei(config-rip-1)#quit

```
 4. Save the configuration.

```

huawei(config)#save

```

----End

Result

Administrators can log in to AC_A and AC_B from the maintenance terminal of the management center to operate and maintain them.

Configuration Files

Configuration file of AC_A

```

vlan 100
port vlan 100 0/2 24
interface vlanif 100

```

```
ip address 192.13.24.5 22
quit
interface loopBack 0
ip address 192.13.2.1 24
quit
rip 1
network 192.13.24.0
network 192.13.2.0
version 2
quit
ip ip-prefix abc permit 192.13.2.1 32
ip ip-prefix abc permit 192.13.2.2 32
rip 1
filter-policy ip-prefix abc export vlanif 100
quit
vlan 10 smart
interface vlanif 10
ip address 192.15.24.1 26
quit
rip 1
network 192.15.24.0
quit
save
```

Configuration file of AC_B

```
vlan 10
port vlan 10 0/2 16
interface vlanif 10
ip address 192.15.24.2 26
quit
interface loopBack 0
ip address 192.13.2.2 24
quit
rip 1
network 192.15.24.0
network 192.13.2.0
version 2
quit
ip ip-prefix abc permit 192.13.2.2 32
rip 1
filter-policy ip-prefix abc export vlanif 10
quit
save
```

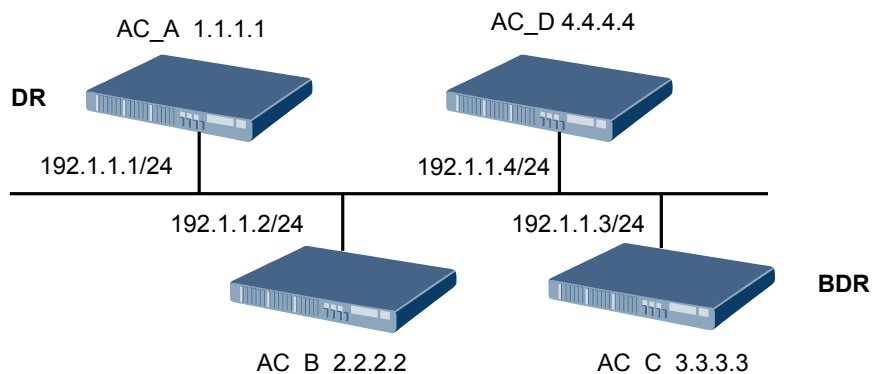
5.1.4 Example for Configuring OSPF

This section describes how to configure OSPF.

Service Requirements

- Four ACs run OSPF.
- AC_A has the highest priority, and AC_C has the second highest priority. AC_A functions as the designated router (DR) to broadcast the network link status.

Figure 5-4 Network topology of OSPF configuration



Data Plan

Table 5-2 lists the data plan of OSPF configuration.

Table 5-2 Data plan of OSPF configuration

| Configuration Item | Data | Remarks |
|--------------------|---|------------------|
| AC_A | IP address of the VLANIF interface:
192.1.1.1/24 | - |
| | Priority: 100 | - |
| | VLAN ID: 2 | - |
| | Router ID: 1.1.1.1 | - |
| AC_B | IP address of the VLANIF interface:
192.1.1.2/24 | - |
| | Priority: 80 | - |
| | VLAN ID: 2 | - |
| | Router ID: 2.2.2.2 | - |
| AC_C | IP address of the VLANIF interface:
192.1.1.3/24 | - |
| | Priority: 90 | - |
| | VLAN ID: 2 | - |
| | Router ID: 3.3.3.3 | - |
| AC_D | IP address of the VLANIF interface:
192.1.1.4/24 | - |
| | Priority: It is not set. | Default value: 1 |
| | VLAN ID: 2 | - |

| Configuration Item | Data | Remarks |
|--------------------|--------------------|---------|
| | Router ID: 4.4.4.4 | - |

Prerequisite

- The native VLAN has been configured on the uplink port of each AC so that ACs can communicate.
- The OSPF area IDs of the ACs are the same.

Procedure

Step 1 Configure AC_A.

1. Assign an IP address to the VLANIF interface on AC_A.

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.1 24
huawei(config-if-vlanif2)#quit
```
2. Configure the OSPF router ID of AC_A.

```
huawei(config)#router id 1.1.1.1
```
3. Enable OSPF on AC_A.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 1.1.1.1 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```
4. Configure the priority of the interface that candidates for the DR on AC_A.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 100
huawei(config-if-vlanif2)#quit
```
5. Save the configuration.

```
huawei(config)#save
```

Step 2 Configure AC_B.

1. Assign an IP address to the VLANIF interface on AC_B.

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.2 24
huawei(config-if-vlanif2)#quit
```
2. Configure the OSPF router ID of AC_B.

```
huawei(config)#router id 2.2.2.2
```
3. Enable OSPF on AC_B.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 2.2.2.2 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```
4. Configure the priority of the interface that candidates for the DR on AC_B.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 80
huawei(config-if-vlanif2)#quit
```

5. Save the configuration.

```
huawei(config)#save
```

Step 3 Configure AC_C.

1. Assign an IP address to the VLANIF interface on AC_C.

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.3 24
huawei(config-if-vlanif2)#quit
```

2. Configure the OSPF router ID of AC_C.

```
huawei(config)#router id 3.3.3.3
```

3. Enable OSPF on AC_C.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Configure the priority of the interface that candidates for the DR on AC_C.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 90
huawei(config-if-vlanif2)#quit
```

5. Save the configuration.

```
huawei(config)#save
```

Step 4 Configure AC_D.

1. Assign an IP address to the VLANIF interface on AC_D.

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.4 24
huawei(config-if-vlanif2)#quit
```

2. Configure the priority of the interface that candidates for the DR on AC_D.

```
huawei(config)#router id 4.4.4.4
```

3. Enable OSPF on AC_D.

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 4.4.4.4 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. Save the configuration.

```
huawei(config)#save
```

----End

Result

Run the **display ip routing-table** command to view the routing table. You can see that ACs can communicate with each other.

Configuration Files

The configurations of ACs are similar. The configuration of AC_A is used as an example.

```

vlan 2
port vlan 2 0/2 24
interface vlanif 2
ip address 192.1.1.1 24
quit
router id 1.1.1.1
ospf
area 0
network 192.1.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
quit
quit
interface vlanif 2
ospf dr-priority 100
quit
save
    
```

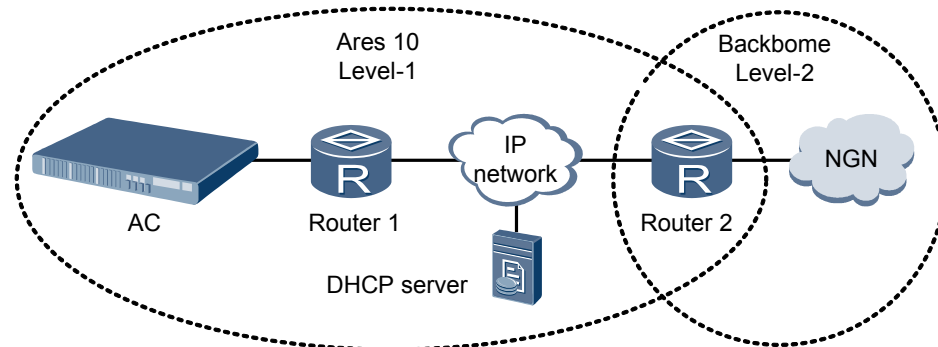
5.1.5 Example for Configuring IS-IS

This section describes how to configure IS-IS.

Service Requirements

- The AC forwards services to the NGN through the VLANIF interface.
- The AC learns NGN routes through the IS-IS protocol. The area ID of the level-2 router connected to the level-1-2 router is different from the area ID of the level-1-2 router.

Figure 5-5 Network topology of IS-IS configuration



Data Plan

Table 5-3 lists the data plan of IS-IS configuration.

Table 5-3 Data plan of IS-IS configuration

| Configuration Item | Data |
|--------------------|---------------------|
| AC | IS-IS process ID: 1 |

| Configuration Item | Data |
|--------------------|--|
| | <p>Network Entity Title (NET): 10.0000.0000.0001.00.</p> <ul style="list-style-type: none"> ● Area ID: 10 ● System ID: 0000.0000.0001 ● Level: level-1 ● Hose name: AC |
| | <p>IS-IS interface:</p> <ul style="list-style-type: none"> ● Port ID: 0/2/24 ● VLAN ID: 20 ● IP address: 192.15.24.5/16 |
| Router1 | <p>IS-IS process ID: 1</p> |
| | <p>NET: 10.0000.0000.0002.00.</p> <ul style="list-style-type: none"> ● Area ID: 10 ● System ID: 0000.0000.0002 ● Level: level-1 ● Host name: Router1 |
| | <p>IS-IS interface: 1/0/0
IP address: 192.15.20.8/16</p> |
| Router2 | <p>IS-IS process ID: 1</p> |
| | <p>NET: 10.0000.0000.0005.00.</p> <ul style="list-style-type: none"> ● Area ID: 10 ● System ID: 0000.0000.0005 ● Level: level-1-2 ● Host name: Router2 |
| | <p>IS-IS interface: 1/0/0
IP address: 192.15.18.5/16</p> |

Procedure

- Configure IS-IS on the AC.
 1. Configure a VLANIF interface.


```

          huawei (config) #vlan 20
          huawei (config) #port vlan 20 0/2 24
          huawei (config) #interface vlanif 20
          huawei (config-if-vlanif20) #ip address 192.15.24.5 16
          huawei (config-if-vlanif20) #quit
          
```
 2. Start the IS-IS process.


```

          huawei (config) #isis 1
          huawei (config-isis-1) #
          
```
 3. Configure the NET.


```
huawei(config-isis-1)#network-entity 10.0000.0000.0001.00
```

4. Configure the level of the router.

```
huawei(config-isis-1)#is-level level-1
```

5. Configure the local host name.

```
huawei(config-isis-1)#is-name AC  
huawei(config-isis-1)#quit
```

6. Enable the IS-IS interface.

```
huawei(config)#interface vlanif 20  
huawei(config-if-vlanif20)#isis enable 1
```

- Configure IS-IS on Router1.

The configuration of Router1 is similar to the configuration on the AC, and is not mentioned here.

- Configure IS-IS on Router2.

The configuration of Router2 is similar to the configuration on the AC, and is not mentioned here.

----End

Result

- You can view the IS-IS LSDB by running the **display isis lsdb** command.
- You can view IS-IS routes by running the **display isis route** command. In the routing table of the level-1 router, a default route exists and the next hop is the level-1-2 router. The routing table of level-2 router has all routes to level-1 and level-2 routers.

Configuration Files

```
vlan 20  
port vlan 20 0/2 24  
interface vlanif 20  
ip address 192.15.24.5 16  
quit  
isis 1  
network-entity 10.0000.0000.0001.00  
is-level level-1  
is-name AC  
quit  
interface vlanif 20  
isis enable 1
```

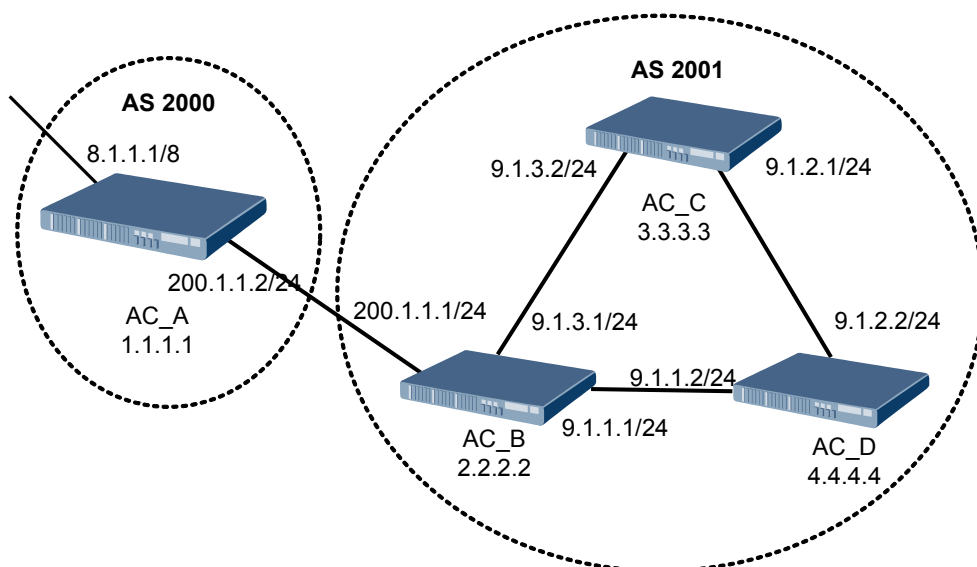
5.1.6 Example for Configuring BGP

This section describes how to configure BGP.

Service Requirements

Configure an EBGP connection between AC_A and AC_B, and configure IBGP connections between AC_B, AC_C, and AC_D.

Figure 5-6 Network topology of BGP configuration



Data Plan

Table 5-4 lists the data plan of BGP configuration.

Table 5-4 Data plan of BGP configuration

| Configuration Item | Data | Remarks |
|--------------------|---|---|
| AC_A | IP address of VLANIF 6:
200.1.1.2/24 | It is used for establishing an EBGP connection with AC_B in AS2001. |
| | IP address of VLANIF 2: 8.1.1.1/8 | - |
| | Router ID: 1.1.1.1 | - |
| | AS ID: 2000 | - |
| AC_B | IP address of VLANIF 6:
200.1.1.1/24 | It is used for establishing an EBGP connection with AC_A in AS2000. |
| | IP address of VLANIF 3: 9.1.3.1/24 | It is used for establishing an IBGP connection with AC_C. |
| | IP address of VLANIF 4: 9.1.1.1/24 | It is used for establishing an IBGP connection with AC_D. |

| Configuration Item | Data | Remarks |
|--------------------|------------------------------------|---|
| | Router ID: 2.2.2.2 | - |
| | AS ID: 2001 | - |
| AC_C | IP address of VLANIF 3: 9.1.3.2/24 | It is used for establishing an IBGP connection with AC_B. |
| | IP address of VLANIF 5: 9.1.2.1/24 | It is used for establishing an IBGP connection with AC_D. |
| | Router ID: 3.3.3.3 | - |
| | AS ID: 2001 | - |
| AC_D | IP address of VLANIF 5: 9.1.2.2/24 | It is used for establishing an IBGP connection with AC_C. |
| | IP address of VLANIF 4: 9.1.1.2/24 | It is used for establishing an IBGP connection with AC_B. |
| | Router ID: 4.4.4.4 | - |
| | AS ID: 2001 | - |

Procedure

Step 1 Configure AC_A.

1. Assign an IP address to the VLANIF interface on AC_A.

```
huawei(config)#vlan 6
huawei(config)#port vlan 6 0/2 16
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ip address 200.1.1.2 24
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 8.1.1.1 8
huawei(config-if-vlanif2)#quit
```

2. Enable BGP on AC_A.

```
huawei(config)#bgp 2000
huawei(config-BGP)#router-id 1.1.1.1
huawei(config-BGP)#peer 200.1.1.1 as-number 2001
huawei(config-BGP)#network 8.0.0.0 8
huawei(config-BGP)#quit
```

3. Save the configuration.

```
huawei(config)#save
```

Step 2 Configure AC_B.

1. Assign an IP address to the VLANIF interface on AC_B.

```
huawei(config)#vlan 6
huawei(config)#port vlan 6 0/2 16
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ip address 200.1.1.1 24
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 3
huawei(config)#port vlan 3 0/2 18
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 9.1.3.1 24
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 4
huawei(config)#port vlan 4 0/2 17
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 9.1.1.1 24
huawei(config-if-vlanif4)#quit
```

2. Enable BGP on AC_B.

```
huawei(config)#bgp 2001
huawei(config-BGP)#router-id 2.2.2.2
huawei(config-BGP)#peer 200.1.1.2 as-number 2000
huawei(config-BGP)#peer 9.1.3.2 as-number 2001
huawei(config-BGP)#peer 9.1.1.2 as-number 2001
huawei(config-BGP)#import-route direct
huawei(config-BGP)#quit
```

3. Save the configuration.

```
huawei(config)#save
```

Step 3 Configure AC_C.

1. Assign an IP address to the VLANIF interface on AC_C.

```
huawei(config)#vlan 3
huawei(config)#port vlan 3 0/2 18
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 9.1.3.2 24
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 5
huawei(config)#port vlan 5 0/2 19
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ip address 9.1.2.1 24
huawei(config-if-vlanif5)#quit
```

2. Enable BGP on AC_C.

```
huawei(config)#bgp 2001
huawei(config-BGP)#router-id 3.3.3.3
huawei(config-BGP)#peer 9.1.3.1 as-number 2001
huawei(config-BGP)#peer 9.1.2.2 as-number 2001
huawei(config-BGP)#quit
```

3. Save the configuration.

```
huawei(config)#save
```

Step 4 Configure AC_D.

1. Assign an IP address to the VLANIF interface on AC_D.

```
huawei(config)#vlan 4
huawei(config)#port vlan 4 0/2 17
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 9.1.1.2 24
huawei(config-if-vlanif4)#quit
huawei(config)#vlan 5 smart
huawei(config)#port vlan 5 0/2 19
huawei(config)#interface vlanif 5
```

```
huawei(config-if-vlanif5)#ip address 9.1.2.2 24
huawei(config-if-vlanif5)#quit

2. Enable BGP on AC_D.
huawei(config)#bgp 2001
huawei(config-BGP)#router-id 4.4.4.4
huawei(config-BGP)#peer 9.1.2.1 as-number 2001
huawei(config-BGP)#peer 9.1.1.1 as-number 2001
huawei(config-BGP)#quit

3. Save the configuration.
huawei(config)#save
```

----End

Result

- After running the **display bgp routing-table** command, you can see that:
 - An EBGP connection between AC_A and AC_B is established.
 - IBGP connections between AC_B, AC_C, and AC_D are established.
 - AC_C and AC_D have all routes with the destination subnet of 8.0.0.0/8 and the next hop is the interface's IP address of AC_A.
- After running the **ping** command on AC_C and AC_D, you can see that AC_C and AC_D are connected to the VLANIF interface with the IP address of 8.1.1.1/24 on AC_A.

Configuration Files

The configurations of ACs are similar. The configuration of AC_A is used as an example.

```
vlan 6
port vlan 6 0/2 16
interface vlanif 6
ip address 200.1.1.2 24
quit
vlan 2
port vlan 2 0/2 24
interface vlanif 2
ip address 8.1.1.1 8
quit
bgp 2000
router-id 1.1.1.1
peer 200.1.1.1 as-number 2001
network 8.0.0.0 8
quit
```

5.2 Configuring DHCP

An AC provides the DHCP relay function, enabling users dynamically to obtain IP addresses from a DHCP server on a network.

Context

The AC works in Layer 2 or Layer 3 DHCP relay mode to forward DHCP packets exchanged between the DHCP server and a client. By default, the AC works in Layer 2 DHCP relay mode. In this mode, the AC transparently transmits DHCP packets initiated by the client and relevant configurations are not required. If the AC works in Layer 3 DHCP relay mode, the DHCP server must support the DHCP relay function and relevant configurations must be performed. The AC supports the following Layer 3 DHCP relay modes:

- **DHCP standard mode**
In this mode, the AC identifies the VLANs that users belong to and binds VLANs to DHCP server groups.
To configure the DHCP standard mode, configure the operating mode of the DHCP relay, configure a DHCP server group, and bind a VLAN to the DHCP server group.
- **DHCP Option 60 mode**
The AC differentiates DHCP packets transmitted from clients according to domain names in Option 60 fields in DHCP packets, and binds domains to DHCP server groups.
To configure the DHCP Option 60 mode, configure the operating mode of the DHCP relay, configure a DHCP server group, create a DHCP Option 60 domain, and bind the DHCP Option 60 domain to the DHCP server group.
- **MAC address segment mode**
The AC differentiates users according to MAC address segments of user terminals, and binds different MAC address segments to DHCP server groups.
To configure the MAC address segment mode, configure the operating mode of the DHCP relay, configure a DHCP server group, create a MAC address segment, and bind the MAC address segment to the DHCP server group.

5.2.1 Configuring the Standard DHCP Mode

The standard DHCP mode applies to the scenario where different DHCP server groups are specified for different users of a VLAN that is used when service ports are created.

Prerequisites

A VLAN has been configured.

Procedure

Step 1 Configure the DHCP forwarding mode.

You can use either of the following methods to configure the DHCP forwarding mode:

- In global config mode, run the **dhcp mode layer-3 standard** command to configure the standard Layer 3 DHCP relay mode. If you select a VLAN and specifies its ID, this configuration takes effect only for this VLAN.

 **NOTE**

The selected VLAN must be configured with the VLANIF interface and cannot be bound to any service profiles.

- Use a VLAN service profile.
 1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
 2. Run the **dhcp mode layer-3 standard** command to configure the DHCP mode.
 3. Run the **commit** command to make the service profile take effect.
 4. Run the **quit** command to exit from the VLAN service profile mode.
 5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in [1.1](#).

Step 2 Configure a DHCP server group.

1. In global config mode, run the **dhcp-server** command to create a DHCP server group.
 - *igroup-number* specifies the number of the DHCP server group and identifies the DHCP server group. You can run the **display dhcp-server all-group** command to check configured DHCP server groups and specify a unique number for the DHCP server group.
 - *ip-addr* specifies the IP address of a DHCP server in the DHCP server group. You can specify up to four IP addresses.



CAUTION

The IP address of the DHCP server configured here must be the same as the IP address of the DHCP server on the network side.

2. (Optional) Run the **dhcp server mode** command to configure the operating mode of the DHCP server.

DHCP servers in the DHCP server group work in load balancing mode or active/standby mode. By default, they work in load balancing mode.

Step 3 Bind the VLAN to the DHCP server.

1. In global config mode, run the **interface vlanif** command to create a VLANIF interface. The VLAN ID specified in this command must be the same as the ID of the configured VLAN.
2. Run the **ip address** command to assign an IP address to the VLANIF interface. After the configuration is complete, this IP address is used as the source IP address for forwarding IP packets in the VLAN at Layer 3.



CAUTION

- If the upper-layer device of the AC is a Layer 2 device, the IP address of the VLANIF interface must be on the same network segment as the IP address of the DHCP server.
- If the upper-layer device of the AC is a Layer 3 device, the IP address of the VLANIF interface and the IP address of the DHCP server can be on different network segments; however, a route must exist between the VLANIF interface and the DHCP server.

3. Run the **dhcp-server** command on the VLANIF interface to bind a DHCP server to the VLAN.

You need to specify *igroup-number*, the value of which is the number of a created DHCP server group.

----End

Example

DHCP server group 1 contains two DHCP servers working in active/standby mode; the IP address of the active DHCP server is 10.1.1.9 and the IP address of the standby server is 10.1.1.10. The maximum response time of the DHCP server is 20s and the number of times no response is received is 10. Bind DHCP server group 1 to VLAN 2.

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp server mode backup 20 10
huawei(config)#dhcp-server 1 ip 10.1.1.9 10.1.1.10
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.1.101 24
huawei(config-if-vlanif2)#dhcp-server 1
huawei(config-if-vlanif2)#quit
```

5.2.2 Configuring the DHCP Server Mode

The DHCP server mode applies to the scenario where the AC functions as the DHCP server to provide the DHCP service for APs.

Prerequisites

A VLAN has been configured.

Procedure

Step 1 Configure a VLANIF interface and enable DHCP on the VLANIF interface.

1. In global config mode, run the **interface vlanif** command to create a VLANIF interface. The VLAN ID specified in this command must be the same as the ID of the configured VLAN.
2. Run the **ip address** command to assign an IP address to the VLANIF interface. After the configuration is complete, this IP address is used as the source IP address for forwarding IP packets in the VLAN at Layer 3.



CAUTION

- If the upper-layer device of the AC is a Layer 2 device, the IP address of the VLANIF interface must be on the same network segment as the IP address of the DHCP server.
- If the upper-layer device of the AC is a Layer 3 device, the IP address of the VLANIF interface and the IP address of the DHCP server can be on different network segments; however, a route must exist between the VLANIF interface and the DHCP server.

-
3. Run the **dhcp enable** command on the VLANIF interface to enable DHCP.

Step 2 Create an IP address pool on the VLANIF interface.

1. In global config mode, run the **ip pool** command to create an IP address pool.
2. In IP address pool mode, run the **gateway** command to configure the gateway IP address of the IP address pool.

----End

Example

Enable DHCP on VLANIF 2 with the IP address of 10.1.1.101 and create an IP address pool named **ap-server** on the VLANIF interface.

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.1.101 255.255.255.0
huawei(config-if-vlanif2)#dhcps enable
huawei(config-if-vlanif2)#quit
```



```
huawei(config)#ip pool ap-server
huawei(config-ip-pool-ap-server)#gateway 10.1.1.101 255.255.255.0
huawei(config-ip-pool-ap-server)#quit
```

5.2.3 Configuring the DHCP Option 43 Function

If the DHCP Option 43 function is enabled on an AC, an AP can obtain the AC's IP address from the DHCP server.

Prerequisites

- A VLAN has been configured.
- The Option 43 attributes have been defined.

Context

If an AP needs to obtain the IP address of an AC from the DHCP server, the DHCP Option 43 function needs to be enabled on the AC so that the AC can deliver its IP address by means of Option 43 to the DHCP server. Then the DHCP server can notify the AP of the AC' IP address by using a packet, and the AP can use the obtained IP address to communicate with the AC.

Procedure

Step 1 Create a VLANIF interface on the AC.

```
# Set the IP address of VLANIF 800 to 172.1.1.1.
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:
ip address 172.1.1.1 255.255.255.0

Step 2 Specify the source IP address for the AC.

```
# Configure VLANIF 800 as the source interface of the AC.
```

NOTE

You must specify the source IP address of an AC so that all APs connected to the AC can learn this IP address.

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

Step 3 Configure an IP address pool for APs on the AC.

```
# Configure IP address pool ctc-ap-server on VLANIF 800.
```

NOTE

The gateway IP address in the IP address pool must be the same as the IP address of the VLANIF interface. After APs go online, they obtain IP addresses from this IP address pool.

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
```

Step 4 # Configure DHCP Option 43 that carries the AC's IP address.

```
# Enable the AC to broadcast its IP address 172.1.1.1 over the network.
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-172.1.1.1
huawei(config-ip-pool-ap-server)#quit
```

**CAUTION**

- If the AP needs to obtain the IP address of the AC, the Option field is optional for Layer 2 networking and mandatory for Layer 3 networking.
- When configuring Option 43, ensure that the Option field is in the **HuaweiAC-x.x.x.x** format, where *x.x.x.x* indicates an IP address.
- If multiple IP addresses are involved, separate the IP address in the text information for Option 43 by a comma, for example, **HuaweiAC-x.x.x.x,x.x.x.x**.

---End

Example

Create the VLANIF 800 interface on the AC, set the interface's IP address to **172.1.1.1**, and use it as the source IP address of the AC. Create IP address pool **ap-server** and enable the AC to broadcast its source IP address over the network.

```
huawei (config) #interface vlanif 800
huawei (config-if-vlanif800) #ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 172.1.1.1 255.255.255.0
huawei (config-if-vlanif800) #quit
huawei (config) #wlan ac
huawei (config-wlan-ac-view) #wlan ac source interface vlanif 800
huawei (config-wlan-ac-view) #quit
huawei (config) #ip pool ap-server
It's successful to create an IP address pool
huawei (config-ip-pool-ap-server) #gateway 172.1.1.1 255.255.255.0
huawei (config-ip-pool-ap-server) #section 0 172.1.1.2 172.1.1.254
huawei (config-ip-pool-ap-server) #option 43 string HuaweiAC-172.1.1.1
huawei (config-ip-pool-ap-server) #quit
```

5.2.4 Configuring the DHCP Option 60 Mode

The DHCP Option 60 mode applies to the scenario where different DHCP servers are specified for users in different Option 60 domains.

Prerequisites

- A VLAN has been configured.
- The Option 60 domain name of a user terminal has been obtained.

Context

Different service providers (SPs) may provide multiple services, such as video multicast and IP telephone services on an AC. The SPs may use different relay IP addresses of the same DHCP server or different DHCP servers to allocate IP addresses to users. Therefore, a user uses the DHCP Option 60 mode to apply for an IP address.

The binding relationship between the string (domain name) in the Option 60 field of a DHCP packet and a DHCP server group is configured. Then the AC selects the DHCP server group according to the domain name in the Option 60 field when working in the DHCP Option 60 mode. The DHCP Option 60 mode differentiates users according to domain names in DHCP packets. This mode can also differentiate service types in the same VLAN.

Procedure

Step 1 Configure the DHCP forwarding mode.

You can use either of the following methods to configure the DHCP forwarding mode:

- In global config mode, run the **dhcp mode layer-3 option60** command to configure the Layer 3 Option 60 mode. If you select a VLAN and specifies its ID, this configuration takes effect only for this VLAN.

 **NOTE**

The selected VLAN must be configured with the VLANIF interface and cannot be bound to any service profiles.

- Use a VLAN service profile.
 1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
 2. Run the **dhcp mode layer-3 option60** command to configure the DHCP mode.
 3. Run the **commit** command to make the service profile take effect.
 4. Run the **quit** command to exit from the VLAN service profile mode.
 5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in 1.1.

Step 2 Configure a DHCP server group.

1. In global config mode, run the **dhcp-server** command to create a DHCP server group.
 - *igroup-number* specifies the number of the DHCP server group and identifies the DHCP server group. You can run the **display dhcp-server all-group** command to check configured DHCP server groups and specify a unique number for the DHCP server group.
 - *ip-addr* specifies the IP address of a DHCP server in the DHCP server group. You can specify up to four IP addresses.



CAUTION

The IP address of the DHCP server configured here must be the same as the IP address of the DHCP server on the network side.

2. (Optional) Run the **dhcp server mode** command to configure the operating mode of the DHCP server.

DHCP servers in the DHCP server group work in load balancing mode or active/standby mode. By default, they work in load balancing mode.

Step 3 Create a DHCP Option 60 domain.

In global config mode, run the **dhcp domain** command to create a DHCP domain and enter the DHCP domain mode. The domain name of the Option 60 field must be configured based on the type of the terminal connected to the AC.

Step 4 Bind the DHCP Option 60 domain to the DHCP server group.

In Option 60 domain mode, run the **dhcp-server** command to bind the DHCP domain to the DHCP server group. After the configuration is complete, the DHCP clients in the DHCP domain connect to DHCP servers in the DHCP server group.

Step 5 Configure the IP address of the gateway corresponding to the DHCP domain.

1. In global config mode, run the **interface vlanif** command to create a VLANIF interface. The VLAN ID specified in this command must be the same as the ID of the configured VLAN.
2. Run the **ip address** command to assign an IP address to the VLANIF interface. After the configuration is complete, this IP address is used as the source IP address for forwarding IP packets in the VLAN at Layer 3.

**CAUTION**

- If the upper-layer device of the AC is a Layer 2 device, the IP address of the VLANIF interface must be on the same network segment as the IP address of the DHCP server.
 - If the upper-layer device of the AC is a Layer 3 device, the IP address of the VLANIF interface and the IP address of the DHCP server can be on different network segments; however, a route must exist between the VLANIF interface and the DHCP server.
-
3. Run the **dhcp domain gateway** command on the VLANIF interface to configure the IP address of the gateway for the DHCP domain.
The IP address of the gateway must be the IP address of the VLANIF interface. On the same VLANIF interface, different Option 60 domains can be configured with different gateways' IP addresses. Therefore, the AC selects different DHCP servers according to domain names in DHCP packets.

----End

Example

DHCP server group 2 contains two DHCP servers working in load balancing mode; the IP address of the active server is 10.10.10.10 and the IP address of the standby server is 10.10.10.11. Bind DHCP server group 2 to users whose Option 60 domain name is **msft** in VLAN 2.

```
huawei (config) #dhcp mode layer-3 Option60
huawei (config) #dhcp-server 2 ip 10.10.10.10 10.10.10.11
huawei (config) #dhcp domain msft
huawei (config-dhcp-domain-msft) #dhcp-server 2
huawei (config-dhcp-domain-msft) #quit
huawei (config) #interface vlanif 2
huawei (config-if-vlanif2) #ip address 10.1.2.1 24
huawei (config-if-vlanif2) #dhcp domain msft gateway 10.1.2.1
```

5.2.5 Configuring the DHCP Option 15 Function

If the DHCP Option 15 function is enabled on an AC, an AP can obtain the AC's IP address from the DNS server.

Prerequisites

- A VLAN has been configured.
- The domain names have been mapped to the IP addresses on the DNS server according to the plan.
- The Option 15 attributes have been defined.

Context

If an AP obtains its IP address from the DHCP server, you can enable the DHCP Option 15 function on the AC so that the AC can deliver the AC's domain name and the IP address of the corresponding DNS server to the DHCP server. After obtaining its IP address, the AC's domain name, and the DNS server's IP address from the DHCP server, the AP can send the AC's domain name to the DNS server to obtain the AC's IP address.

Procedure

Step 1 Create a VLANIF interface on the AC.

```
# Set the IP address of VLANIF 800 to 172.1.1.1.
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 172.1.1.1 255.255.255.0
```

Step 2 Specify the source IP address for the AC.

```
# Configure VLANIF 800 as the source interface of the AC.
```

NOTE

You must specify the source IP address of an AC so that all APs connected to the AC can learn this IP address.

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

Step 3 Configure an IP address pool for APs on the AC.

```
# Configure IP address pool ctc-ap-server on VLANIF 800.
```

NOTE

The gateway IP address in the IP address pool must be the same as the IP address of the VLANIF interface. After APs go online, they obtain IP addresses from this IP address pool.

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
```

Step 4 Enable the DHCP Option 15 function on the AC to allow the AC to advertise its domain name and the IP address of the corresponding DNS server.

```
# Set the DNS suffix to huawei.com for the IP address pool.
huawei(config-ip-pool-ap-server)#dns-suffix huawei.com
```

```
# Create the primary DNS server whose IP address is 172.10.1.1 for the IP address pool.
```

```
huawei(config-ip-pool-ap-server)#dns-server 172.10.1.1
huawei(config-ip-pool-ap-server)#quit
```

----End

Example

```
# Create the VLANIF 800 interface on the AC, set the interface's IP address to 172.1.1.1, and use it as the source IP address of the AC. Create IP address pool ap-server, set the AC' domain name to huawei.com, and the IP address of the corresponding DNS server to 172.10.1.1.
```

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 172.1.1.1 255.255.255.0
```

```
huawei(config-if-vlanif800)#quit
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
huawei(config)#ip pool ap-server
    It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
huawei(config-ip-pool-ap-server)#dns-suffix huawei.com
huawei(config-ip-pool-ap-server)#dns-server 172.10.1.1
{ <cr>|secondary<K>|third<K> }:
```

Command:

```
dns-server 172.10.1.1
huawei(config-ip-pool-ap-server)#quit
```

5.2.6 Configuring the DHCP MAC Address Segment Mode

The MAC address segment mode applies to the scenario where different DHCP servers are specified for users on different MAC address segments.

Prerequisites

A VLAN has been configured.

Context

Devices of various manufacturers may exist on a network. The devices of each manufacturer have a fixed MAC address segment. You can use the MAC address segment mode to obtain IP addresses from the DHCP server.

The AC can select the DHCP server based on the MAC address segment. After the configuration is complete, clients on this MAC address segment obtain IP addresses from the DHCP server.

Procedure

Step 1 Configure the DHCP forwarding mode.

You can use either of the following methods to configure the DHCP forwarding mode:

- In global config mode, run the **dhcp mode layer-3 mac-range** command to configure the Layer 3 MAC address segment mode. If you select a VLAN and specifies its ID, this configuration takes effect only for this VLAN.

NOTE

The selected VLAN must be configured with the VLANIF interface and cannot be bound to any service profiles.

- Use a VLAN service profile.
 1. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
 2. Run the **dhcp mode layer-3 mac-range** command to configure the DHCP mode.
 3. Run the **commit** command to make the service profile take effect.
 4. Run the **quit** command to exit from the VLAN service profile mode.
 5. Run the **vlan bind service-profile** command to bind the VLAN to the VLAN service profile created in [1.1](#).

Step 2 Configure a DHCP server group.

1. In global config mode, run the **dhcp-server** command to create a DHCP server group.
 - *igroup-number* specifies the number of the DHCP server group and identifies the DHCP server group. You can run the **display dhcp-server all-group** command to check configured DHCP server groups and specify a unique number for the DHCP server group.
 - *ip-addr* specifies the IP address of a DHCP server in the DHCP server group. You can specify up to four IP addresses.



CAUTION

The IP address of the DHCP server configured here must be the same as the IP address of the DHCP server on the network side.

2. (Optional) Run the **dhcp server mode** command to configure the operating mode of the DHCP server.

DHCP servers in the DHCP server group work in load balancing mode or active/standby mode. By default, they work in load balancing mode.

Step 3 Create a MAC address segment.

1. In global config mode, run the **dhcp mac-range** command to create a MAC address segment and enter the MAC address segment mode.
range-name specifies the name of the MAC address segment.
2. In MAC address segment mode, run the **mac-range** command to configure the MAC address range.

Step 4 Bind the DHCP server group to the MAC address segment.

In MAC address segment mode, run the **dhcp-server** command to bind a DHCP server group to the MAC address segment.

Step 5 Configure the IP address of the gateway corresponding to the MAC address segment.

1. In global config mode, run the **interface vlanif** command to create a VLANIF interface. The VLAN ID specified in this command must be the same as the ID of the configured VLAN.
2. Run the **ip address** command to assign an IP address to the VLANIF interface. After the configuration is complete, this IP address is used as the source IP address for forwarding IP packets in the VLAN at Layer 3.



CAUTION

- If the upper-layer device of the AC is a Layer 2 device, the IP address of the VLANIF interface must be on the same network segment as the IP address of the DHCP server.
 - If the upper-layer device of the AC is a Layer 3 device, the IP address of the VLANIF interface and the IP address of the DHCP server can be on different network segments; however, a route must exist between the VLANIF interface and the DHCP server.
-
3. Run the **dhcp mac-range gateway** command on the VLANIF interface to configure the IP address of the gateway corresponding to the DHCP domain.

The IP address of the gateway must be the IP address of the VLANIF interface. On the same VLANIF interface, different MAC address segments can be configured with different gateways. Therefore, the AC selects different DHCP servers according to MAC address segments in DHCP packets.

----End

Example

DHCP server group 2 contains two DHCP servers working in load balancing mode; the IP address of the active server is 10.10.10.10 and the IP address of the standby server is 10.10.10.11. Bind DHCP server group 2 to users with MAC addresses in the range of 0000-0000-0001 to 0000-0000-0100 in VLAN 2.

```
huawei(config)#dhcp mode layer-3 mac-range
huawei(config)#dhcp-server 2 ip 10.10.10.10 10.10.10.11
huawei(config)#dhcp mac-range huawei
huawei(config-mac-range-huawei)#mac-range 0000-0000-0001 to 0000-0000-0100
huawei(config-mac-range-huawei)#dhcp-server 2
huawei(config-mac-range-huawei)#quit
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.2.1 24
huawei(config-if-vlanif2)#dhcp mac-range huawei gateway 10.1.2.1
```

5.3 Configuring AAA

This section describes how to configure authentication, authorization, and accounting (AAA) on the AC, including the configuration of the AC as the local or remote server.

Context

When users access network resources, the system grants certain rights to authenticated users and records the network resources used by users. AAA is a security technology in which:

- Authentication: checks whether a user can access a network.
- Authorization: authorizes a user to use specific services.
- Accounting: records the network resources used by a user.

Applicable Environment

AAA is applicable to access users in PPPoA, PPPoE, 802.1x, VLAN, WLAN, ISDN, and Admin Telnet (association between the user name, password, and domain name) modes.

Figure 5-7 shows the AAA networking.

Figure 5-7 AAA networking



AAA can be implemented on the AC in the following ways:

- The AC functions as a local AAA server. You need to configure local AAA. Local AAA does not support accounting.
- The AC functions as the client of a remote AAA server, and is connected to the Remote Authentication Dial-In User Service (RADIUS) server through the RADIUS protocol. The RADIUS protocol does not support authorization.

5.3.1 Configuring Remote AAA (RADIUS)

The AC connects to a Remote Authentication Dial-In User Service (RADIUS) server to implement authentication and accounting using the RADIUS protocol.

Context

- RADIUS is described as follows:
 - RADIUS uses the client/server model and manages a large number of distributed dialup users.
 - RADIUS implements authentication and accounting for users by managing a simple user database.
 - Users send authentication and accounting requests to the RADIUS server through a network access server (NAS).
- The RADIUS working process is as follows:
 - When a user attempts to connect to the NAS through a network to access other networks or use network resources, the NAS sends authentication and accounting information about the user to the RADIUS server. The RADIUS protocol defines how user information and accounting information are exchanged between the NAS and the RADIUS server.
 - The RADIUS server receives the connection request of the user sent from the NAS, authenticates the user by checking the user name and password, and sends required configuration information about the user to the NAS.
- The RADIUS configuration specifications are as follows:
 - A RADIUS server group can be either of the following:
 - An independent RADIUS server
 - Two (primary and secondary) RADIUS servers with the same configuration but different IP addresses
 - Each RADIUS server template contains the following attributes:
 - IP address of the primary server
 - IP address of the secondary server
 - Shared key and RADIUS server type
- RADIUS defines only the mandatory parameters for information exchange between the AC and the RADIUS server. To make the parameters take effect, apply the RADIUS server group to a domain.

Procedure

- Configure an authentication scheme.

 **NOTE**

- An authentication scheme specifies the authentication mode for all the users in an ISP domain.
 - The system supports a maximum of 16 authentication schemes. The system provides a default authentication scheme, which cannot be deleted. The authentication mode in the default authentication scheme can be modified.
1. Run the **aaa** command to enter the AAA mode.
 2. Run the **authentication-scheme** command to create an authentication scheme.
 3. Run the **authentication-mode radius** command to configure the authentication mode in the authentication scheme.
 4. Run the **quit** command to exit from the AAA mode.
- Configure an accounting scheme.

 **NOTE**

- An accounting scheme specifies the accounting mode for all the users in an ISP domain.
 - The system supports a maximum of 128 accounting schemes. The system provides a default accounting scheme, which cannot be deleted. The accounting mode in the default accounting scheme can be modified.
1. In AAA mode, run the **accounting-scheme** command to create an AAA accounting scheme.
 2. Run the **accounting-mode radius** command to configure the accounting mode.
 3. Run the **accounting interim interval** command to set the interval for real-time accounting. The default interval is 0 minutes, that is, real-time accounting is not performed.
 4. Run the **quit** command to exit from the AAA mode.
- Configure a RADIUS server template.
 1. Run the **radius-server template** command to create a RADIUS server template and enter the RADIUS server template mode.
 2. Run the **radius-server authentication** command to configure the IP address and the UDP port number of the RADIUS authentication server.

 **NOTE**

- Before configuring the IP address and the UDP port number of the RADIUS authentication server, ensure that there is a reachable route between the RADIUS authentication server and the AC.
 - Ensure that the RADIUS service port on the AC is the same as the port on the RADIUS authentication server.
3. Run the **radius-server accounting** command to configure the IP address and UDP port number of the RADIUS accounting server.
 4. (Optional) Run the **hwtacacs-server shared-key** command to configure the shared key of the RADIUS accounting server.

 **NOTE**

- The RADIUS client (AC) and the RADIUS server use the MD5 algorithm to encrypt RADIUS packets. They check validity of the RADIUS packets based on the shared key. They can receive packets from each other and respond to each other only when their shared keys are the same.
 - By default, the shared key of the RADIUS accounting server is **huawei**.
5. (Optional) Run the **radius-server timeout** command to set the response timeout interval of the RADIUS server. By default, the response timeout interval is 5s.

The AC sends a request packet to the RADIUS server. If the RADIUS server does not respond within the response timeout interval, the AC retransmits the request packet to the RADIUS to ensure that users can obtain services from the RADIUS server.

6. (Optional) Run the **radius-server retransmit** command to set the maximum number of times RADIUS request packets are retransmitted. The default value is 3.

When the number of times RADIUS request packets are retransmitted exceeds the maximum value, the AC considers that communication with the RADIUS server is interrupted, and transmits a RADIUS request packet to another RADIUS server.

7. Run the **radius-server user-name domain-included** command to configure the AC to encapsulate the domain name in the user name in RADIUS packets. By default, the AC encapsulates the domain name in the user name when sending RADIUS packets to a RADIUS server.
 - The user name format is `userid@domain-name`, and the character string following `@` is the domain name. The AC adds a user to a domain according to the domain name.
 - If a RADIUS server group rejects the user name carrying the domain name, the RADIUS server group can be only used in one domain. Otherwise, when some access users in different domains have the same user name, the RADIUS server considers these users as the same user because the names transmitted to the server are the same.
8. Run the **quit** command to return to the global config mode.

- Create a domain.

A domain is a group of users of the same type.

When the user name is in the format of `userid@domain-name` (for example, `huawei20041028@isp1.net`), the character string following `@` is the domain name, and the character string before `@` is the user name.

The domain name for user login cannot exceed 15 characters, and the other domain names cannot exceed 20 characters.

1. Run the **aaa** command to enter the AAA mode.
2. In AAA mode, run the **domain** command to create a domain.

- Apply the RADIUS server template to the domain.

 **NOTE**

Before applying a RADIUS server template to a domain, ensure that the RADIUS server template has been created.

1. In domain mode, run the **radius-server template** command to apply the RADIUS server template.
2. Run the **quit** command to return to the AAA mode.

----End

Example

In domain **isp**, user1 uses RADIUS to communicate with the RADIUS server for authentication and accounting. The accounting interval is 10 minutes and the authentication password is a123456. The RADIUS server at IP address 129.7.66.66 functions as the primary server. The RADIUS server at 129.7.66.67 functions as the secondary server. The authentication port

number is 1812 and the accounting port number is 1813. Other parameters use the default settings.

```
huawei (config) #aaa
huawei (config-aaa) #authentication-scheme newscheme
huawei (config-aaa-authen-newscheme) #authentication-mode radius
huawei (config-aaa-authen-newscheme) #quit
huawei (config-aaa) #accounting-scheme newscheme
huawei (config-aaa-accounting-newscheme) #accounting-mode radius
huawei (config-aaa-accounting-newscheme) #accounting interim interval 10
huawei (config-aaa-accounting-newscheme) #quit
huawei (config-aaa) #quit
huawei (config) #radius-server template hwtest
huawei (config-radius-hwtest) #radius-server authentication 129.7.66.66 1812
huawei (config-radius-hwtest) #radius-server authentication 129.7.66.67 1812
secondary
huawei (config-radius-hwtest) #radius-server accounting 129.7.66.66 1813
huawei (config-radius-hwtest) #radius-server accounting 129.7.66.67 1813 secondary
huawei (config-radius-hwtest) #quit
huawei (config) #aaa
huawei (config-aaa) #domain isp
huawei (config-aaa-domain-isp) #authentication-scheme newscheme
huawei (config-aaa-domain-isp) #accounting-scheme newscheme
huawei (config-aaa-domain-isp) #radius-server hwtest
huawei (config-aaa-domain-isp) #quit
huawei (config-aaa) #quit
```

5.3.2 Example for Configuring RADIUS Authentication and Accounting

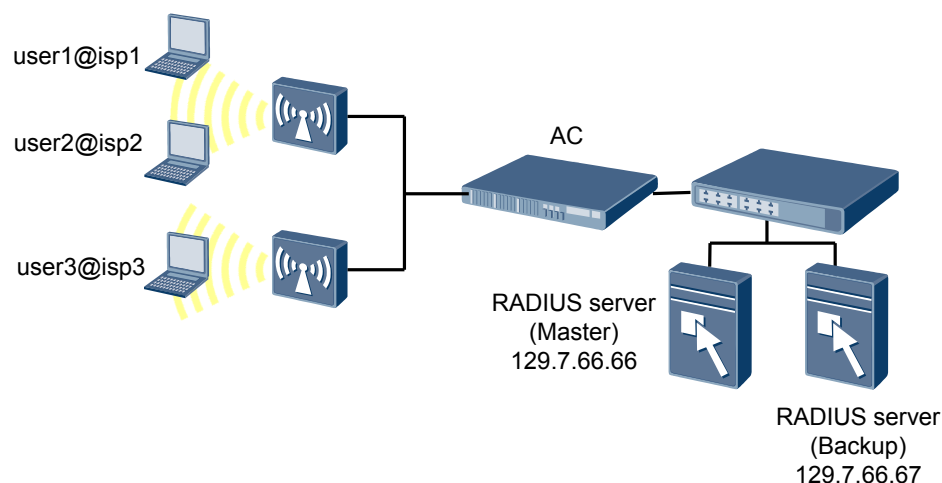
The AC connects to a Remote Authentication Dial-In User Service (RADIUS) server to implement authentication and accounting using the RADIUS protocol.

Service Requirements

- The RADIUS server performs authentication and accounting for user1 in domain **isp1**.
- The RADIUS server at IP address 129.7.66.66 functions as the primary server.
- The RADIUS server at 129.7.66.67 functions as the secondary server.
- The authentication port number is 1812, and the accounting port number is 1813.
- Other parameters use the default settings.

Network Diagram

[Figure 5-8](#) shows networking of RADIUS authentication and accounting.

Figure 5-8 Networking of RADIUS authentication and accounting

Procedure

Step 1 Configure an authentication scheme.

Configure an authentication scheme named **newscheme** and use RADIUS to authenticate users.

```
huawei (config) #aaa
huawei (config-aaa) #authentication-scheme newscheme
huawei (config-aaa-authen-newscheme) #authentication-mode radius
huawei (config-aaa-authen-newscheme) #quit
```

Step 2 Configure an accounting scheme.

Configure an accounting scheme named **newscheme**, use RADIUS to perform accounting for users, and set the accounting interval to 10 minutes.

```
huawei (config-aaa) #accounting-scheme newscheme
huawei (config-aaa-accounting-newscheme) #accounting-mode radius
huawei (config-aaa-accounting-newscheme) #accounting interim interval 10
huawei (config-aaa-accounting-newscheme) #quit
huawei (config-aaa) #quit
```

Step 3 Configure the RADIUS protocol.

Create a RADIUS server template named **radtest**; configure the RADIUS server at 129.7.66.66 as the primary server and the RADIUS server at 129.7.66.67 as the secondary server.

```
huawei (config) #radius-server template radtest
Note: Create a new server template
huawei (config-radius-radtest) #radius-server authentication 129.7.66.66 1812
huawei (config-radius-radtest) #radius-server authentication 129.7.66.67 1812
secondary
huawei (config-radius-radtest) #radius-server accounting 129.7.66.66 1813
huawei (config-radius-radtest) #radius-server accounting 129.7.66.67 1813 secondary
huawei (config-radius-radtest) #quit
```

Step 4 Create a domain.

Create domain **isp1**.

```
huawei (config)
#aaa
```

```
huawei(config-aaa)#domain isp1
Info: Create a new domain
```

Step 5 Apply the authentication scheme to the domain.

Before applying an authentication scheme to a domain, ensure that the authentication scheme has been created.

```
huawei(config-aaa-domain-isp1)#authentication-scheme newscheme
```

Step 6 Apply the accounting scheme to the domain.

Before applying an accounting scheme to a domain, ensure that the accounting scheme has been created.

```
huawei(config-aaa-domain-isp1)#accounting-scheme newscheme
```

Step 7 Apply the RADIUS server template to the domain.

Before applying a RADIUS server template to a domain, ensure that the RADIUS server template has been created.

```
huawei(config-aaa-domain-isp1)#radius-server radtest
huawei(config-aaa-domain-isp1)#quit
```

Step 8 Configure a local AAA user.

Create AAA user **user1** and set the password to **a123456**.

```
huawei(config-aaa)#local-user shenzhen@isp1 password a123456
```

----End

Result

In domain **isp1**, **user1** can be authenticated only when the user name and password are correct. Then **user1** is allowed to log in to the AC and accounting is performed for **user1**.

Configuration Files

```
aaa
authentication-scheme newscheme
authentication-mode radius
quit
accounting-scheme
newscheme
accounting-mode
radius
accounting interim interval 10
quit
quit
radius-server template radtest
radius-server authentication 129.7.66.66
1812
radius-server authentication 129.7.66.67 1812 secondary
radius-server accounting 129.7.66.66
1813
radius-server accounting 129.7.66.67 1813 secondary
quit
aaa
domain
isp1
authentication-scheme newscheme
radius-server
```

```
radtest
quit
quit
aaa
local-user shenzhen@isp1 password a123456
```

5.4 Configuring MSTP

The AC provides Multiple Spanning Tree Protocol (MSTP) functions and is compatible with the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP). The AC supports the MSTP ring network to meet network topology requirements.

Applicable Environment

- MSTP can compensate for the defects of STP and RSTP. MSTP implements fast convergence and allows traffic from different VLANs to be forwarded along different paths. It provides a better load balancing mechanism for redundant links.
- MSTP reconstructs the network with loops to a loop-free network, avoiding packet proliferation and infinite looping. It load balances data traffic among VLANs during data forwarding.

Procedure

Step 1 Enable MSTP.

- By default, MSTP is disabled on the AC.
 - After MSTP is enabled, the AC determines whether to work in STP or MSTP mode based on the configured protocol.
 - After MSTP is enabled, MSTP dynamically maintains the spanning tree of the VLAN based on the received BPDUs. After MSTP is disabled, the AC becomes a transparent bridge and does not maintain the spanning tree.
1. Run the **stp enable** command to enable MSTP on a bridge.
 2. Run the **stp mode mstp** command to enable MSTP on a port.
 3. Run the **display stp** command to check whether MSTP is enabled on a bridge or a port.

Step 2 Configure the MST region name.

1. Run the **stp region-configuration** command to enter the MST region mode.
2. (Optional) Run the **region-name** command to configure the MST region name.
The default MST region name is the bridge MAC address of the AC.

Step 3 Configure an MSTP instance (MSTI).

Configure VLAN mapping tables (relationships between VLANs and spanning trees) to associate VLANs with spanning trees.

1. Run the **stp region-configuration** command to enter the MST region mode.
2. Run the **instance vlan** command to map a VLAN to an MSTI.
 - By default, all VLANs are mapped to the common and internal spanning tree (CIST), that is, MSTI 0.
 - A VLAN can be mapped to only one MSTI, that is, if a mapped VLAN is remapped to a different MSTI, the previous mapping is deleted automatically.

- A maximum of 10 VLAN segments can be mapped to an MSTI.

 **NOTE**

A VLAN segment consists of consecutive VLAN IDs in the range of a start VLAN ID to an end VLAN ID.

3. Run the **check region-configuration** command to view the configuration of the MST region.

Step 4 Manually activate the MST region configuration.

1. Run the **stp region-configuration** command to enter the MST region mode.
2. Run the **active region-configuration** command to manually activate the MST region configuration.
3. Run the **display stp region-configuration** command to view the activated configuration of the MST region.

Step 5 Set the priority of the AC in the MSTI.

1. Run the **stp priority** command to set the priority of the AC in a specified MSTI.
2. Run the **display stp** command to view the MSTP configuration of the AC.

Step 6 Perform the following operations.

- Set parameters of the MST region.
 - Run the **stp md5-key** command to configure the MD5-Key for the MD5 encryption algorithm in an MST region.
 - In MST region mode, run the **vlan-mapping module** command to map all VLANs to the specified MSTI by module.
 - In MST region mode, run the **revision-level** command to configure the MSTP revision level of the AC.
 - Run the **reset stp region-configuration** command to restore all MST region parameters to the default values.
- Configure the AC as a root bridge or a backup root bridge.
 - Run the **stp root** command to configure the AC as a root bridge or a backup root bridge.
- Set time parameters of a specified bridge.
 - Run the **stp timer forward-delay** command to set the forward delay of a specified bridge.
 - Run the **stp timer hello** command to set the hello time of a specified bridge.
 - Run the **stp timer max-age** command to set the max age of a specified bridge.
 - Run the **stp time-factor** command to set the timeout time factor of a specified bridge.
- Set parameters of a specified port.
 - Run the **stp port transmit-limit** command to set the number of BPDUs transmitted by the port within a hello time period.
 - Run the **stp port edged-port enable** command to set the port as an edge port.
 - Run the **stp port cost** command to set the path cost of a port in a specified MSTI.
 - Run the **stp port port-priority** command to set the priority of a specified port.
 - Run the **stp port point-to-point** command to set the link connected to the port as a point-to-point (P2P) link or a non-P2P link.
- Configure protection functions.
 - Run the **stp bpd protection enable** command to enable BPDU protection on the AC.

- Run the **stp port loop-protection enable** command to enable loop protection on the port.
- Run the **stp port root-protection enable** command to enable root protection on the port.
- Set the maximum number of hops in an MST region.
 - Run the **stp max-hops** command to set the maximum number of hops in an MST region.
- Set the network diameter.
 - Run the **stp bridge-diameter** command to set the network diameter.
- Configure the calculation standard for the path cost.
 - Run the **stp pathcost-standard** command to set the calculation standard for the path cost.
- Clear the MSTP statistics.
 - Run the **reset stp statistics** command to clear the MSTP statistics on the AC.

----End

Example

Set MSTP parameters as follows:

- Enable MSTP.
- Enable MSTP on port 0/2/16.
- Sets the MSTP running mode to MSTP compatible mode.
- Set parameters of the MST region.
 - Set the MD5-Key of the MD5 algorithm to 0x11ed224466.
 - Set the MST region name to huawei-mstp-bridge.
 - Map VLANs 2-10 and VLANs 12-16 to MSTI 3.
 - Map all VLANs to the specified MSTI by module 16.
 - Set the MSTP revision level of the AC to 100.
- Set the maximum number of hops of the MST region to 10.
- Manually activate the MST region configuration.
- Set the priority of the AC in MSTI 2 to 4096.
- Configure the AC as the root bridge of MSTI 2.
- Set the network diameter to 6.
- Configure the calculation standard for the path cost as IEEE 802.1t.
- Set time parameters of a specified bridge.
 - Set the forward delay of the specified bridge to 2000 centiseconds.
 - Set the hello time of the specified bridge to 1000 centiseconds.
 - Set the max age of the specified bridge to 3000 centiseconds.
 - Set the timeout time factor of the specified bridge to 6.
- Set parameters of the specified port:
 - Set the maximum number of BPDUs transmitted by the port within a hello time period to 16.
 - Configure port 0/2/16 as an edge port.
 - Set the path cost of the port in a specified MSTI to 1024.
 - Set the port priority to 64.

- Set the link connected to port 0/2/16 as a P2P link.

- Enable BPDU protection.

```
huawei(config)#stp enable
Change global stp state may active region configuration,it may take several
minutes,are you sure to change global stp state? [Y/N][N]y
huawei(config)#stp port 0/2/16 enable
huawei(config)#stp mode mstp
huawei(config)#stp md5-key 11ed224466
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name huawei-mstp-bridge
huawei(stp-region-configuration)#instance 3 vlan 2 to 10 12 to 16
huawei(stp-region-configuration)#vlan-mapping module 16
huawei(stp-region-configuration)#revision-level 100
huawei(stp-region-configuration)#active region-configuration
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 2 priority 4096
huawei(config)#stp instance 2 root primary
huawei(config)#stp max-hops 10
huawei(config)#stp bridge-diameter 6
huawei(config)#stp pathcost-standard dot1t
huawei(config)#stp timer forward-delay 2000
huawei(config)#stp timer hello 1000
huawei(config)#stp timer max-age 3000
huawei(config)#stp time-factor 6
huawei(config)#stp port 0/2/16 transmit-limit 16
huawei(config)#stp port 0/2/16 edged-port enable
huawei(config)#stp port 0/2/16 instance 0 cost 1024
huawei(config)#stp port 0/2/16 instance 0 port-priority 64
huawei(config)#stp port 0/2/16 point-to-point force-true
huawei(config)#stp bpdu-protection enable
```

5.5 Configuring Ethernet CFM OAM

This section describes how to configure Ethernet CFM OAM on the AC.

Prerequisites

The router supports Ethernet CFM OAM.

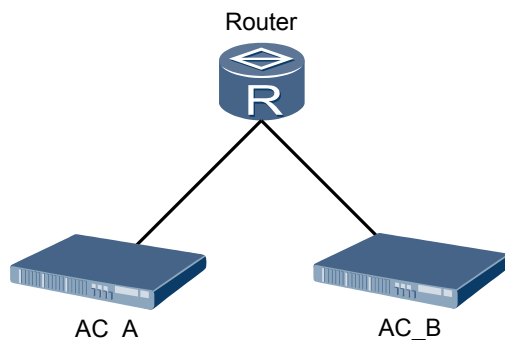
Service Requirements

The two remote devices send detection packets periodically to check connectivity.

Network Diagram

Figure 5-9 shows the network topology of Ethernet CFM OAM configuration.

On the Ethernet, Ethernet CFM OAM detects faults on the link between AC_A and AC_B. The local MEP ID of AC_B must be the same as the RMEP ID of AC_A and the RMEP ID of AC_B must be the same as the local MEP ID of AC_A.

Figure 5-9 Network topology of Ethernet CFM OAM configuration

Data Plan

Table 5-5 provides the data plan for Ethernet CFM OAM configuration.

Table 5-5 Data plan for Ethernet CFM OAM configuration

| Configuration Item | Data |
|--------------------|---|
| AC_A | Port number: 0/2/24
Smart VLAN: 100
MEP: 2/6/5
CC-interval: 10 minutes |
| AC_B | Port number: 0/2/24
Smart VLAN: 200
MEP: 2/6/5
CC-interval: 10 minutes |

Procedure

Step 1 Create a VLAN.

The S-VLAN ID is 100, and the VLAN is a smart VLAN.

```
huawei(config)#vlan 100
```

Step 2 Add an uplink port to the VLAN.

Add port 0/2/24 to VLAN 100.

```
huawei(config)#port vlan 100 0/2 24
```

Step 3 (Optional) Configure a native VLAN on the port.

This step is performed to configure packets on the uplink Ethernet port to or not to carry VLAN tags. Whether the native VLAN needs to be configured on the uplink port depends on whether

the upper-layer device connected to the uplink port supports packets with VLAN tags. The setting on the AC must be the same as that on the upper-layer device. Packets are untagged.

```
huawei (config) #interface scu 0/2
huawei (config-if-scu-0/2) #native-vlan 24 vlan 100
huawei (config-if-scu-0/2) #quit
```

Step 4 Configure the MD.

- MDs with the same index or level cannot be created.
- The name format and the name of an MD must be unique.
- The total length of the names of an MD and its MAs must be shorter than or equal to 44 characters.

```
huawei (config) #cfm md 2 name-format string huawei level 3
```

Step 5 Configure the MA.

- The system supports up to 4096 MAs. If an MD is configured with 4096 MAs, the other MDs in the system cannot be configured with any MA. An MA cannot be configured for a non-existing MD. An existing MA cannot be created again.
- The total length of the names of an MD and its MAs must be shorter than or equal to 44 characters.
- The interval for an MA to send CC packets is 10 minutes. The default value is 1 minute.

```
huawei (config) #cfm ma 2/6 name-format string cfmhuawei cc-interval 10m
```

Step 6 Configure the MEP.

- Ethernet CFM OAM detects link connectivity by using MEPs at the two ends of the link.
- By default, the MEP management function is enabled, the priority of sending CFM packets is 7, and the AC is configured to send CC packets.

```
huawei (config) #cfm ma 2/6 vlan 100 mhf-creation default-mhf
huawei (config) #cfm ma 2/6 meplist 5
huawei (config) #cfm mep 2/6/5 direction down port 0/2/24 priority 7
```

Step 7 Enable the RMEP detection function.

By default, the RMEP detection function is disabled.

```
huawei (config) #cfm remote-mep-detect enable
```

Step 8 Enable the local CFM function globally. By default, the local CFM function is disabled globally.

```
huawei (config) #cfm enable
```

Step 9 Enable the RMEP detection function globally. By default, the RMEP detection function is disabled globally.

```
huawei (config) #cfm remote-mep-detect enable
```

Step 10 Save the configuration.

```
huawei (config) #save
```

 **NOTE**

The RMEP of AC_A must be configured on AC_B. The configuration is similar to that on AC_A, and is not mentioned here.

----End

Result

After the configuration is complete, run the **display cfm statistics mep** command to view the packet statistics on AC_A or AC_B. You can see that the statistics on CCM Sent Pkt Num and CCM Received Pkt Num are not 0.

Configuration Files

```
vlan 100 smart
port vlan 100 0/2 24
interface scu 0/2
native-vlan 24 100
quit
cfm md 2 name-format string huawei level 3
cfm ma 2/6 name-format string cfmhuawei cc-interval 10m
cfm mep 2/6/5 direction down port 0/2/24 priority 7
cfm remote-mep-detect enablecfm enable
cfm remote-mep-detect enable
save
```

6 Configuring the Multicast Service

About This Chapter

This section describes how to configure the multicast service on a single AC, multiple cascading ACs, or on ACs on an MSTP network.

The multicast feature of the AC is applied to the live TV and near-video on demand (NVOD) services.

The AC supports IGMP proxy and IGMP snooping, which both support multicast video data forwarding but use different processing mechanisms:

- IGMP snooping maintains multicast forwarding entries by listening to IGMP packets exchanged between users and the multicast router.
- IGMP proxy intercepts IGMP packets exchanged between the user and the multicast router, processes them, and then forwards them to the upper-layer multicast router. Multicast users consider the AC as a multicast router, and the multicast router considers the AC as a multicast user.

The AC can use a static multicast program library or dynamically generate a multicast program library.

- Static multicast program library: A program list is configured before users watch video programs. In this mode, the AC uses an authority profile to control the multicast service. You must maintain the program list and the authority profile according to video service changes. The AC supports program host, program pre-join, and multicast bandwidth management functions.
- Dynamic multicast program library: The AC dynamically generates a program list according to the programs requested by users. In this mode, you do not need to configure or maintain the program list. The AC, however, does not support program management, user multicast bandwidth management, program preview, or program pre-join.

A sudden increase in the traffic with a high priority in the triple play service will not result in loss of IGMP packets because the AC first processes and sends IGMP packets.

[6.1 Default Settings of the Multicast Service](#)

This section describes the default settings of the multicast service.

6.1 Default Settings of the Multicast Service

This section describes the default settings of the multicast service.

Table 6-1 lists the default settings of the multicast service of the AC.

Table 6-1 Default settings of the multicast service

| Feature | Default Setting |
|---|----------------------|
| Multicast protocol | Disabled |
| IGMP version | V3 |
| Configuration mode of the multicast program | Static configuration |
| Multicast bandwidth management | Enabled |
| Program preview | Enabled |
| Multicast log | Enabled |

6.1.1 Setting Global Multicast Parameters

Parameters of Layer 2 multicast protocols (IGMP proxy and IGMP snooping) are valid for all the multicast VLANs.

Context

Global multicast parameters include the parameters for IGMP General Query messages, parameters for IGMP Group-Specific Query messages, and policy of processing multicast packets.

General Query:

- Purpose: The AC sends an IGMP General Query message periodically to check whether there is any multicast user who has left the multicast group without sending a Leave message. Based on the query result, the AC updates the multicast forwarding table and releases the bandwidth of the multicast user who has left the multicast group.
- Principle: The AC sends an IGMP General Query message periodically to all online IGMP users. If the AC does not receive the response message from an IGMP user within a specified duration (Robustness variable x Interval at which IGMP General Query messages are sent + Maximum response time of IGMP General Query messages), it considers that the user has left the multicast group. Then the AC deletes the user from the multicast group.

Group-Specific Query:

- Purpose: After an outbound interface for a multicast user that is not configured with the prompt leave function sends a Leave message, the AC sends an IGMP Group-Specific Query message to check whether the multicast user has left the multicast group.
- Principle: When a multicast user leaves a multicast group, for example, switches to another channel, the user sends a Leave message to the AC. If the outbound interface for the user

is not configured with the prompt leave function, the AC sends an IGMP Group-Specific Query message to the multicast group. If the AC does not receive the response message from the multicast user within a specified duration (Robustness variable x Interval at which IGMP Group-Specific Query messages are sent + Maximum response time of IGMP Group-Specific Query messages), it deletes the multicast user from the multicast group.

Table 6-2 lists the default settings of global multicast parameters.

Table 6-2 Default settings of global multicast parameters

| Item | Default Setting |
|---|--|
| Parameters for IGMP General Query messages | Interval at which IGMP General Query messages are sent: 125s
Maximum response time of IGMP General Query messages: 10s
IGMP robustness variable: 2 |
| Parameters for IGMP Group-Specific Query messages | Interval at which IGMP Group-Specific Query messages are sent: 1s
Maximum response time of IGMP Group-Specific Query messages: 0.8s.
IGMP robustness variable: 2 |

Procedure

Step 1 In global config mode, run the **btv** command to enter the BTV mode.

Step 2 Set parameters for IGMP General Query messages.

1. Run the **igmp proxy router gen-query-interval** command to set the interval at which IGMP General Query messages are sent. The default value is 125s.
2. Run the **igmp proxy router gen-response-time** command to set the maximum response time of IGMP General Query messages. The default value is 10s.
3. Run the **igmp proxy router robustness** command to set the IGMP robustness variable. The default value is 2.

Step 3 Set parameters for IGMP Group-Specific Query messages.

1. Run the **igmp proxy router sp-query-interval** command to set the interval at which IGMP Group-Specific Query messages are sent. The default value is 1s.
2. Run the **igmp proxy router sp-response-time** command to set the maximum response time of IGMP Group-Specific Query messages. The default value is 0.8s.
3. Run the **igmp proxy router sp-query-number** command to set the number of times a querier sends IGMP Group-Specific Query messages. The default value is 2.

Step 4 Run the **display igmp config global** command to check whether the values of multicast parameters are correct.

----End

Example

Set the interval at which IGMP General Query messages are sent to 150s, the maximum response time of IGMP General Query messages to 20s, and the IGMP robustness variable to 3.

```
huawei (config) #btv
huawei (config-btv) #igmp proxy router gen-query-interval 150
huawei (config-btv) #igmp proxy router gen-response-time v3 20
huawei (config-btv) #igmp proxy router robustness 3
```

Set the interval at which IGMP Group-Specific Query messages are sent to 150s, the maximum response time of IGMP Group-Specific Query messages to 20s, and the number of times a querier sends IGMP Group-Specific Query messages to 3.

```
huawei (config) #btv
huawei (config-btv) #igmp proxy router sp-query-interval 200
huawei (config-btv) #igmp proxy router sp-response-time v3 100
huawei (config-btv) #igmp proxy router sp-query-number 3
```

6.1.2 Configuring a Multicast VLAN and a Multicast Program

Multicast VLANs (MVLANS) distinguish multicast ISPs. An MVLAN is allocated to each multicast ISP to manage multicast programs, multicast protocols, and multicast versions, and control multicast domains and user rights based on VLANs.

Context

Before configuring an MVLAN, create a common VLAN. When multicast and unicast VLANs are different VLANs, multicast and unicast flows use different service channels.

A user port can be added to multiple MVLANS, but there are restrictions on these MVLANS:

- Only one MVLAN is allowed to have dynamically generated programs.
- The IGMP versions supported by all the MVLANS must be the same.
- Only one MVLAN can run IGMPv3 snooping.

When the AC processes multicast packets:

- If the VLANIF interface of the program has an IP address, this IP address is the source IP address. Ensure that the IP address is on the same segment as IP addresses of the BRAS and the upper-layer router.
- If the VLANIF interface does not have an IP address, the source IP address is the host IP address of the multicast program source.
- If the host IP address is not configured, the default IP address (0.0.0.0) is used.

Table 6-3 lists the default settings of the multicast VLAN attributes, including the Layer 2 multicast protocol, IGMP version, multicast program, and multicast uplink port priority.

Table 6-3 Default settings of the multicast VLAN attributes

| Item | Default Setting |
|----------------------------|------------------------|
| Program matching mode | Configured dynamically |
| Multicast uplink port mode | Default |
| Layer 2 multicast protocol | off |

| Item | Default Setting |
|--|-----------------|
| IGMP version | V3 |
| Priority of forwarding IGMP packets by the uplink port | 6 |

Procedure

Step 1 Create an MVLAN.

1. Run the **vlan** command to create a VLAN.
2. Run the **multicast-vlan** command to configure the created VLAN as a multicast VLAN.

Step 2 Configure multicast programs.

Programs of the MVLAN are generated dynamically. A program list is not required and the programs are dynamically generated according to the user's request. In this mode, the AC does not support program management, user multicast bandwidth management, program preview, or program pre-join.

1. Run the **igmp match group** command to configure the IP address range of the program group that can be dynamically generated. Users can request only the programs whose IP addresses are within the specified range.

Step 3 Configure the multicast uplink port.

1. Run the **igmp uplink-port** command to configure the multicast uplink port. The packets of the MVLAN are forwarded and received by this uplink port.
2. In BTV mode, run the **igmp uplink-port-mode** command to change the working mode of the multicast uplink port. On an MSTP network, the port works in MSTP mode. In other cases, the port works in default mode.
 - Default mode: If the MVLAN contains only one uplink port, incoming multicast packets can be sent only by this port. If the MVLAN contains multiple uplink ports, incoming multicast packets are sent by all the uplink ports.
 - MSTP mode: This mode is used on an MSTP network.

Step 4 Configure a multicast protocol.

Run the **igmp mode { proxy | snooping }** command to configure a Layer 2 multicast protocol. By default, the multicast function is disabled.

When IGMP snooping is used, the proxy function can be enabled for Report and Leave messages. When a multicast user joins or leaves a multicast program, the AC can implement IGMP proxy. IGMP snooping and IGMP proxy are independent of each other.

- Run the **igmp report-proxy enable** command to enable IGMP proxy for Report messages. When the first user requests a program and is authenticated, after authentication, the AC sends the user's Report message to the upper-layer multicast router and obtains a corresponding multicast stream from the multicast router. The AC does not send the Report message from subsequent users for joining the same program to the upper-layer multicast router.
- Run the **igmp leave-proxy enable** command to enable IGMP proxy for Leave messages. When the last user requests to leave a program, the AC sends the Leave message to upper-

layer router of so that the router stops sending multicast streams. If a user is not the last user to leave a program, the AC does not send the Leave message of the user to the network side.

Step 5 Configure the IGMP version.

Run the **igmp version { v2 | v3 }** command to configure the IGMP version. By default, IGMPv3 is enabled in the system. If upper-layer and lower-layer devices on the network run IGMPv2 and cannot identify IGMPv3 messages, run this command to change the IGMP version.

IGMPv3 is compatible with IGMPv2. If IGMPv3 is enabled on the AC and the upper-layer multicast router uses IGMPv2, the AC switches to IGMPv2 when receiving IGMPv2 messages. If the AC does not receive any IGMPv2 messages within the preset IGMPv2 timeout time, it switches back to IGMPv3. In BTV mode, run the **igmp proxy router timeout** command to set the IGMPv2 timeout time. The default value is 400s.

Step 6 Change the priority for forwarding IGMP messages.

Run the **igmp priority** command to change the priority for forwarding IGMP messages by the uplink port. By default, the priority is 6 and does not need to be changed.

- IGMP proxy forwards IGMP messages using the configured priority.
- IGMP snooping forwards IGMP messages to the network side based on the priority of the user-side service stream. The priority of the service stream is set using the traffic profile.

Step 7 Check whether the configuration is correct.

- Run the **display igmp config vlan** command to view the attributes of the MVLAN.
- Run the **display igmp program vlan** command to view information about programs of the MVLAN.

---End

Example

Create VLAN 101, configure multicast programs dynamically, configure port 0/2/24 as the uplink port of the MVLAN, enable IGMP proxy, and set the IGMP version to IGMPv3.

```
huawei(config)#vlan 101
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp uplink-port 0/2/24
huawei(config-mvlan101)#igmp mode proxy
Are you sure to change IGMP mode?(y/n)[n]:y
huawei(config-mvlan101)#igmp version v3
```

7 Operation and Maintenance Management

About This Chapter

This chapter describes how to perform basic operation and maintenance management for an AC by setting alarms and saving data.

[7.1 Configuring Alarms](#)

Alarm management enables the system to record alarms, set alarm severity, and collect statistics on alarms for efficient device maintenance.

[7.2 Configuring a New AP Replacement Quickly](#)

When an AP needs to be replaced, you can change the MAC address or SN of the AP to the MAC address or SN of the new AP. Then the new AP can use the ID of the replaced AP to go online, and all the configurations of the replaced AP will take effect on the new AP when the new AP is online.

7.1 Configuring Alarms

Alarm management enables the system to record alarms, set alarm severity, and collect statistics on alarms for efficient device maintenance.

Context

An alarm refers to the notification generated when the system detects a fault. After an alarm is generated, the system broadcasts the alarm to terminals, including the Network Management System (NMS) and the Command Line Interface (CLI).

Alarms are classified into fault alarm and clear alarm. After a fault alarm is generated at a certain time, it lasts until the fault is rectified to clear the alarm.

You can modify the alarm settings according to actual requirements, including alarm severity, alarm output mode, and alarm statistics.

Procedure

- Run the **alarm active clear** command to clear alarms in the system.
 - When an active alarm lasts a long period of time, you can run this command to clear the alarm.
 - Before clearing an alarm, run the **display alarm active** command to view the active alarms.
- Run the **alarm alarmlevel** command to configure the alarm severity.
 - The severity of an alarm is critical, major, minor, or warning.
 - The **default** parameter indicates the alarm is restored to the default severity.
 - You can run the **display alarm list** command to query the alarm severity.
 - The system specifies the default (also recommended) alarm severity for each alarm. Use the default alarm severity unless otherwise required.
- Run the **alarm jitter-proof** command to configure the alarm anti-jitter function and the anti-jitter period.
 - To prevent a fault alarm and its clear alarm from being displayed frequently, you can enable the alarm anti-jitter function to filter alarms in the system.
 - After the alarm anti-jitter function is enabled, an alarm is reported to the NMS only after an alarm anti-jitter period expires.
 - If an alarm is cleared within an alarm anti-jitter period, the alarm is not reported to the NMS.
 - You can run the **display alarm jitter-proof** command to check whether the alarm anti-jitter function is enabled and whether the alarm anti-jitter period is set.
 - By default, the alarm anti-jitter function is disabled. You can determine whether to enable the function according to the running of the device.
- Run the **alarm output/undo alarm output** command to enable the AC to send alarms to the CLI terminal or disable the AC from sending alarms to the CLI terminal.
 - Setting the output mode of alarms does not affect alarm generation. The alarms generated by the system are still recorded. You can run the **display alarm history** command to check the alarms that are shielded.

- When the new output mode of an alarm conflicts with the previous mode, the new output mode takes effect.
- The output mode of the clear alarm is the same as the output mode of the fault alarm. When the output mode of the fault alarm is set, the system synchronizes the output mode of its clear alarm with the output mode of the fault alarm.
- Run the **alarm-event statistics period** command to set the alarm statistics collection period.
 - The system collects the occurrence times of alarms and events according to the configured period. To save the statistics result to the flash memory, run the **alarm-event statistics save** command.
 - You can use the statistics result of alarms and events to locate a problem in the system.
 - You can run the **display alarm statistics** command to query the alarm statistics record.
- Run the **display alarm configuration** command to check the alarm configuration according to the alarm ID. The alarm configuration that you can query includes the alarm ID, alarm name, alarm class, alarm type, alarm severity, default alarm severity, number of parameters, CLI output flag, conversion flag, and detailed alarm description.
- Run the **display alarm statistics** command to check the alarm statistics record.
 - To view the frequency in which one alarm occurs within a time range and the device running status and analyze the fault that may exist, run this command.
 - Currently, you can query the alarm statistics in the current 15 minutes, current 24 hours, last 15 minutes, and last 24 hours in the system.

---End

Example

Shield all alarms at the **warning** level from the CLI terminal, enable the alarm anti-jitter function, set the alarm anti-jitter period to 15s, change the severity of alarm with ID 0x0a310021 to **major**, and save the statistics record of alarms at the **major** level to the flash memory.

```
huawei (config) #undo alarm output alarmlevel warning
huawei (config) #alarm jitter-proof on
huawei (config) #alarm jitter-proof 15
huawei (config) #alarm alarmlevel 0x0a310021 critical
huawei (config) #alarm-event statistics save
```

7.2 Configuring a New AP Replacement Quickly

When an AP needs to be replaced, you can change the MAC address or SN of the AP to the MAC address or SN of the new AP. Then the new AP can use the ID of the replaced AP to go online, and all the configurations of the replaced AP will take effect on the new AP when the new AP is online.

Context

AP configurations are bound to the MAC address or SN. If a failed AP needs to be replaced online, you need to configure data for the new AP. To minimize the impact on services, the AP quick configuration function is provided. To use this function, ensure:

- The new AP is of the same type of the replaced AP.
- The MAC address and SN of the new AP must be unique on the network.

Procedure

- Step 1** Replace the failed AP with an AP that is of the same type as the failed AP. Run the **ap modify** command to change the MAC address and SN of the failed AP to the MAC address and SN of the new AP.

---End

Result

The new AP properly provides services of the failed AP.

Example

Replace AP 0 with the AP whose MAC address is 0002-3333-3333 and whose SN is SN000008.

```
huawei(config-wlan-ac-view)#ap modify 0 mac 0002-3333-3333 sn SN000008
```