Building a Basic WLAN

Instructor Version

Huawei Technologies Co., Ltd.

Trademarks and Permissions

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 a 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: https://e.huawei.com/

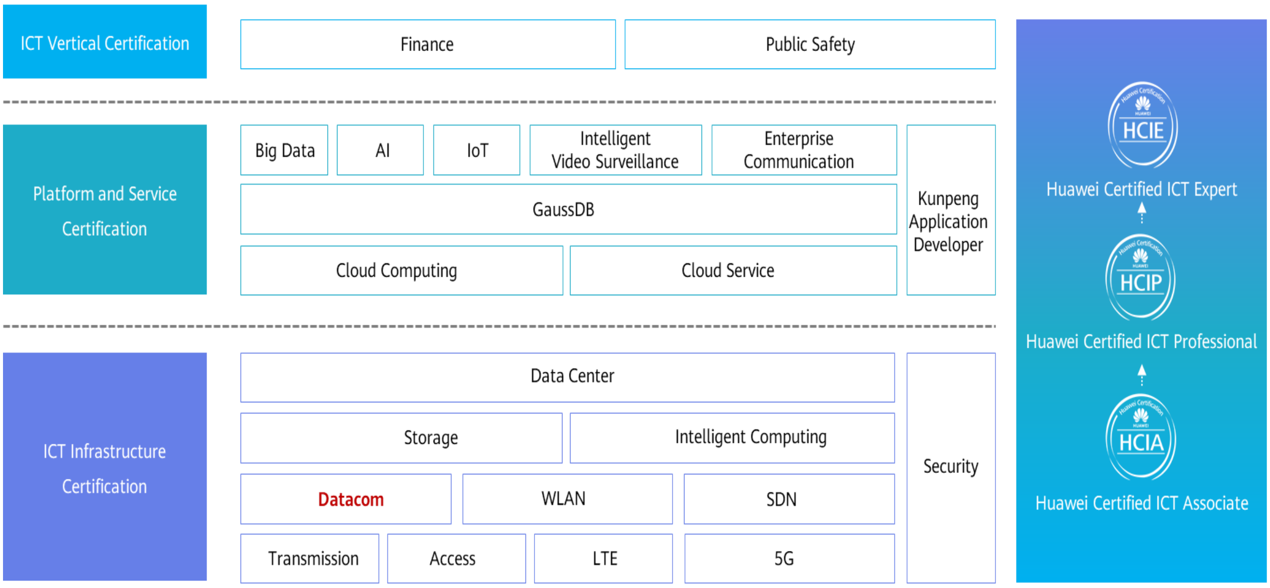
Huawei Certification System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.

Huawei Certification


ICT Vertical Certification
Finance
Public Safety
Platform and Service Certification
Big Data
AI
IoT
Intelligent Video Surveillance
Enterprise Communication
Kunpeng Application Developer
GaussDB
Cloud Computing
Cloud Service
ICT Infrastructure Certification
Data Center
Security
Storage
Intelligent Computing
Datacom
WLAN
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

1 Building a Basic WLAN

1.1 Background

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

In this lab activity, you will configure a WLAN using an AC and fit APs.

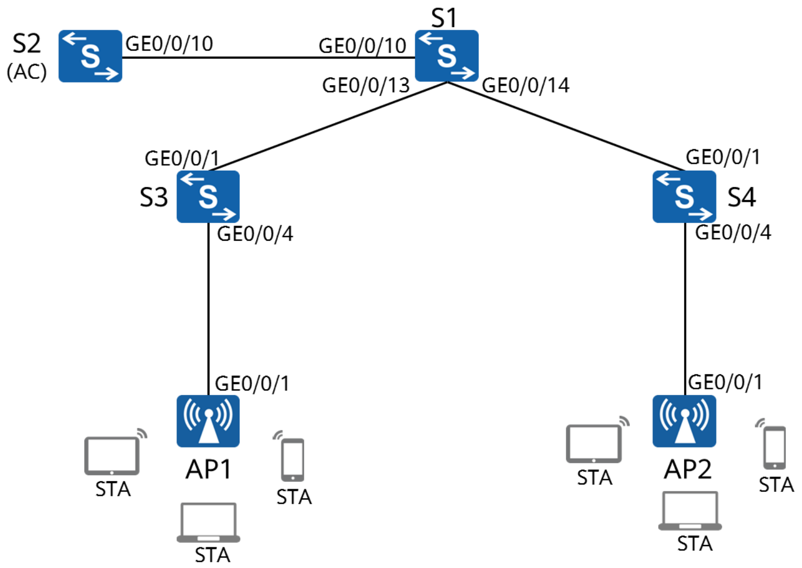
1.2 Objectives

Upon completion of this task, you will be able to:

- Learn how to authenticate APs
- Learn how to configure WLAN profiles
- Understand the basic WLAN configuration process

1.3 Topology

Figure 1-1 Lab Topology



1. The S2 switch supports the WLAN-AC function. If the switch does not support the WLAN-AC function, use a common AC to replace the switch. The AC in the following content is an S2 switch.
2. The AC is deployed in an out-of-path mode and is on the same Layer 2 network as the APs.
3. The AC functions as a DHCP server to assign IP addresses to APs, S1 functions as a DHCP server to assign IP addresses to stations (STAs).
4. Service data is directly forwarded.

1.4 Data Planning

An enterprise needs to create a WLAN to provide mobility in workplace.

Table 1-1 AC data planning

Item	Configuration
AP management VLAN	VLAN100
Service VLAN	VLAN101
DHCP server	The AC functions as a DHCP server to allocate IP addresses to APs.

Item	Configuration
	S1 functions as a DHCP server to allocate IP addresses to STAs. The default gateway address of STAs is 192.168.101.254.
IP address pool for APs	192.168.100.1-192.168.100.253/24
IP address pool for STAs	192.168.101.1-192.168.101.253/24
IP address of the AC's source interface	VLANIF100: 192.168.100.254/24
AP group	Name: ap-group1
	Referenced profiles: VAP profile **HCIA-wlan** and regulatory domain profile **default**
Regulatory domain profile	Name: default
	Country code: CN
SSID profile	Name: HCIA-WLAN
	SSID name: HCIA-WLAN
Security profile	Name: HCIA-WLAN
	Security policy: WPA-WPA2+PSK+AES
	Password: HCIA-Datacom
VAP profile	Name: HCIA-WLAN
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 101
	Referenced profiles: SSID profile **HCIA- WLAN** and security profile **HCIA- WLAN**

1.5 Implementation

1.5.1 Roadmap

1. Configure the connectivity of the wired network.
2. Configure the APs and bring them online.
   (1) Create AP groups and add APs of the same configuration to the same group for unified configuration.
   (2) Configure AC system parameters, including the country code and source interface used by the AC to communicate with the APs.

(3) Configure the AP authentication mode and import the APs to bring them online.

3. Configure WLAN service parameters and deliver them to APs for STAs to access the WLAN.

1.5.2 Procedure

Step 1 Complete basic device configurations.

# Name the devices (name S2 in the topology **AC**)

The details are not provided here.

```
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]poe enable
```

The **poe enable** command enables the PoE function on a port. When a port detects a powered device (PD) connected to it, the port supplies power to the PD. By default, the PoE function is enabled. Therefore, this command is unnecessary and is provided for demonstration purpose only.

```
[S4]interface GigabitEthernet 0/0/4
[S4-GigabitEthernet0/0/4]poe enable
```

Step 2 Configure the wired network.

# Configure VLANs.

```
[S1]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]port link-type trunk
[S1-GigabitEthernet0/0/13]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14]port link-type trunk
[S1-GigabitEthernet0/0/14]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/14]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/10]quit
```

```
[AC]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC]interface GigabitEthernet 0/0/10
[AC-GigabitEthernet0/0/10]port link-type trunk
[AC-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[AC-GigabitEthernet0/0/10]quit
```

```
[S3]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S3]interface GigabitEthernet 0/0/1
```

```
[S3-GigabitEthernet0/0/1]port link-type trunk
[S3-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/1]quit
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]port link-type trunk
[S3-GigabitEthernet0/0/4]port trunk pvid vlan 100
[S3-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/4]quit
```

```
[S4]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S4]interface GigabitEthernet0/0/1
[S4-GigabitEthernet0/0/1] port link-type trunk
[S4-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/1]quit
[S4]interface GigabitEthernet0/0/4
[S4-GigabitEthernet0/0/4] port link-type trunk
[S4-GigabitEthernet0/0/4] port trunk pvid vlan 100
[S4-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/4]quit
```

# Configure interface IP addresses.

```
[S1]interface Vlanif 101
[S1-Vlanif101]ip address 192.168.101.254 24
Gateway for STAs
[S1-Vlanif101]quit
[S1]interface LoopBack 0
[S1-LoopBack0] ip address 10.0.1.1 32
```

This operation is for subsequent test only.

```
[S1-LoopBack0]quit
```

```
[AC]interface Vlanif 100
[AC-Vlanif100]ip address 192.168.100.254 24
```

# Configure DHCP.

```
[S1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[S1]ip pool sta
Info:It's successful to create an IP address pool.
IP address pool for STAs
[S1-ip-pool-sta]network 192.168.101.0 mask 24
[S1-ip-pool-sta]gateway-list 192.168.101.254
[S1-ip-pool-sta]quit
[S1]interface Vlanif 101
[S1-Vlanif101]dhcp select global
[S1-Vlanif101]quit
```

```
[AC]dhcp enable
```

```
Info: The operation may take a few seconds. Please wait for a moment.done.
[AC]ip pool ap
Info: It is successful to create an IP address pool.
IP address pool for APs
[AC-ip-pool-ap]network 192.168.100.254 mask 24
[AC-ip-pool-ap]gateway-list 192.168.100.254
[AC-ip-pool-ap]quit
[AC]interface Vlanif 100
[AC-Vlanif100]dhcp select global
[AC-Vlanif100]quit
```

S1 is the DHCP server for STAs and the AC is the DHCP server for APs.

Step 3 Configure the APs to bring them online.

# Create an AP group and name it ap-group1.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[AC-wlan-ap-group-ap-group1]quit
```

# Create a regulatory domain profile, and set the AC country code in the profile.

```
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name default
```

A regulatory domain profile provides configurations of country code, calibration channel, and calibration bandwidth for an AP.

The default regulatory domain profile is named **default**. Therefore, the default profile is displayed.

```
[AC-wlan-regulate-domain-default]country-code cn
Info: The current country code is same with the input country code.
```

A country code identifies the country in which the APs are deployed. Different countries require different AP radio attributes, including the transmit power and supported channels. Correct country code configuration ensures that radio attributes of APs comply with local laws and regulations. By default, the country code CN is configured.

```
[AC-wlan-regulate-domain-default]quit
```

# Bind the regulatory domain profile to an AP group.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio
and reset the AP. Continue?[Y/N]:y
```

The **regulatory-domain-profile** command in the AP group view binds a regulatory domain profile to an AP or AP group. By default, regulatory domain profile **default** is bound to an AP group, but no regulatory domain profile is bound to an AP. In the default regulatory domain profile, the country code is CN. Therefore, the 2.4 GHz calibration channels include channels 1, 6, and 11, and the 5 GHz calibration channels include channels 149, 153, 157, 161, and 165. Therefore, this step and the previous step can be skipped.

```
[AC-wlan-ap-group-ap-group1]quit
```

# Specify a source interface on the AC for establishing CAPWAP tunnels.

```
[AC]capwap source interface Vlanif 100
```

The **capwap source interface** command configures the interface used by the AC to set up CAPWAP tunnels with APs.

# Import APs to the AC and add the APs to AP group **ap-group1**.

APs can be added to an AC in the following ways:

- Manual configuration: Specify the MAC addresses and serial numbers (SNs) of APs on the AC in advance. When APs are connected the AC, the AC finds that their MAC addresses and SNs match the preconfigured ones and establish connections with them.
- Automatic discovery: When the AP authentication mode is set to no authentication, or the AP authentication mode is set to MAC or SN authentication and the MAC addresses or SNs are whitelisted, the AC automatically discovers connected APs and establish connections with them.
- Manual confirmation: If the AP authentication mode is set to MAC or SN authentication and MAC address or SN of a connected AP is not included in the whitelist on the AC, the AC adds the AP to the list of unauthorized APs. You can manually confirm the identify of such an AP to bring it online.

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

The **ap auth-mode** command configures the AP authentication mode. Only authenticated APs can go online. The authentication modes include MAC address authentication, SN authentication, and no authentication. The default AP authentication mode is MAC address authentication.

Note: For MAC address and SN information of an AP, check the MAC address label and SN label in the package.

```
[AC-wlan-view]ap-id 0 ap-mac 60F1-8A9C-2B40
```

The **ap-id** command adds an AP or displays the AP view.

The **ap-mac** argument specifies MAC address authentication, and the **ap-sn** argument specifies SN authentication.

In the AP view, you can enter ap-id to enter the corresponding AP view.

```
[AC-wlan-ap-0]ap-name ap1
```

The **ap-name** command configures the name of an AP. AP names must be unique. If the AP name is not configured, the default name is the MAC address of the AP.

```
[AC-wlan-ap-0]ap-group ap-group1
```

The **ap-group** command configures the group for an AP. The AC delivers the configuration to the APs. For example, if AP1 is added to ap-group1, the regulatory domain profile, radio profile, and VAP profile associated with ap-group1 are delivered to AP1. By default, an AP is not added to any group. When an AP is added to a group or the group of an AP changes, the group configuration will be delivered automatically by the AC, and the AP will automatically restart to join the group.

```
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and
antenna gain configurations of the radio, Whether to continue? [Y/N]:y            //Enter y to confirm.
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-0]quit
[AC-wlan-view]ap-id 1 ap-mac B4FB-F9B7-DE40
[AC-wlan-ap-1]ap-name ap2
[AC-wlan-ap-1]ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and
antenna gain configurations of the radio, Whether to continue? [Y/N]:y       //Enter y to confirm.
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-1]quit
```

# Display the information about the current AP.

```
[AC]wlan
[AC-wlan-view]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor    : normal                  [2]
------------------------------------------------------------------------------------------------------------------------------
ID       MAC              Name   Group          IP                       Type             State     STA    Uptime
------------------------------------------------------------------------------------------------------------------------------
0        00e0-fc25-0ed0    ap1    ap-group1  192.168.100.206   AirEngine5760    nor       0       30M:4S
1        00e0-fc0f-07a0    ap2    ap-group1  192.168.100.170   AirEngine5760    nor       0       31M:31S
------------------------------------------------------------------------------------------------------------------------------
Total: 2
```

The **display ap** command displays AP information, including the IP address, model (AirEngine5760), status (normal), and online duration of the AP.

In addition, you can add **by-state** *state* or **by-ssid** *ssid* to filter APs in a specified state or using a specified SSID.

The command output shows that the two APs are working properly. (For more status description, see the appendix of this lab.)

Step 4 Configure WLAN service parameters.

# Create security profile **HCIA-WLAN** and configure a security policy.

```
[AC-wlan-view]security-profile name HCIA-WLAN
[AC-wlan-sec-prof-HCIA-WLAN]security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
```

The **security psk** command configures WPA/WPA2 pre-shared key (PSK) authentication and encryption.

Currently, both WPA and WPA2 are used. User terminals can be authenticated using either WPA or WPA2. The PSK is set to **HCIA-Datacom**. User data is encrypted using the AES encryption algorithm.

```
[AC-wlan-sec-prof-HCIA-WLAN]quit
```

# Create SSID profile **HCIA-WLAN** and set the SSID name to **HCIA-WLAN**.

```
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
SSID profile HCIA-WLAN is created.
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
The SSID name is set to HCIA-WLAN.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-HCIA-WLAN]quit
```

# Create VAP profile **HCIA-WLAN**, configure the data forwarding mode and service VLAN, and apply the security profile and SSID profile to the VAP profile.

```
[AC]wlan
[AC-wlan-view]vap-profile name HCIA-WLAN
```

The **vap-profile** command creates a VAP profile.

You can configure the data forwarding mode in a VAP profile and bind the SSID profile, security profile, and traffic profile to the VAP profile.

```
[AC-wlan-vap-prof-HCIA-WLAN]forward-mode direct-forward
```

The **forward-mode** command configures the data forwarding mode in a VAP profile. By default, the data forwarding mode is direct forwarding.

```
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
```

The **service-vlan** command configures the service VLAN of a VAP. After a STA accesses a WLAN, the user data forwarded by the AP carries the **service-VLAN** tag.

```
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
Security profile HCIA-WLAN is bound.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
SSID profile HCIA-WLAN is bound.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]quit
```

# Bind the VAP profile to the AP group and apply configurations in VAP profile **HCIA-WLAN** to radio 0 and radio 1 of the APs in the AP group.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

The **vap-profile** command binds a VAP profile to a radio. After this command is executed, all configurations in the VAP, including the configurations in the profiles bound to the VAP, are delivered to the radios of APs.

```
Info: This operation may take a few seconds, please wait...done.
[AC-wlan-ap-group-ap-group1]quit
```

----End

1.6 Verification

1. Use an STA to access the WLAN with the SSID of **HCIA-WLAN**. Check the IP address obtained by the STA and ping the IP address (10.0.1.1) of LoopBack0 on S1.
2. When the STA is connected to the AC, run the **display station all** command on the AC to check the STA information.

1.7 Configuration Reference

Configuration on S1

```
#
sysname S1
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool sta
  gateway-list 192.168.101.254
  network 192.168.101.0 mask 255.255.255.0
#
interface Vlanif101
  ip address 192.168.101.254 255.255.255.0
  dhcp select global
#
interface GigabitEthernet0/0/10
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/14
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface LoopBack0
  ip address 10.0.1.1 255.255.255.255
#
return
```

Configuration on the AC

```
#
sysname AC
```

```
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool ap
  gateway-list 192.168.100.254
  network 192.168.100.0 mask 255.255.255.0
#
interface Vlanif100
  ip address 192.168.100.254 255.255.255.0
  dhcp select global
#
interface GigabitEthernet0/0/10
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
wlan
security-profile name HCIA-WLAN
    security wpa-wpa2 psk pass-phrase %^%#V-rr;CTW$X%,nJ/0jcmO!tRQ(pt;^8IN,z1||UU)%^%# aes
ssid-profile name HCIA-WLAN
    ssid HCIA-WLAN
vap-profile name HCIA-WLAN
    service-vlan vlan-id 101
    ssid-profile HCIA-WLAN
    security-profile HCIA-WLAN
ap-group name ap-group1
    radio 0
      vap-profile HCIA-WLAN wlan 1
    radio 1
      vap-profile HCIA-WLAN wlan 1
    radio 2
      vap-profile HCIA-WLAN wlan 1
  ap-id 0 type-id 75 ap-mac 60f1-8a9c-2b40 ap-sn 21500831023GJ9022622
    ap-name ap1
    ap-group ap-group1
  ap-id 1 type-id 75 ap-mac b4fb-f9b7-de40 ap-sn 21500831023GJ2001889
    ap-name ap2
    ap-group ap-group1
  provision-ap
#
return
```

Configuration on S3

```
#
sysname S3
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
```

```
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
return
```

Configuration on S4

```
#
sysname S4
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
return
```

1.8 Appendix

Table 1-2 AP State

AP State	Description
commit-failed	WLAN service configurations fail to be delivered to the AP after the AP goes online on an AC.
committing	WLAN service configurations are being delivered to the AP after the AP goes online on an AC.
config	WLAN service configurations are being delivered to the AP when the AP is going online on an AC.
config-failed	WLAN service configurations fail to be delivered to the AP when the AP is going online on an AC.
download	The AP is in upgrade state.
fault	The AP fails to go online.
idle	It is the initialization state of the AP before it establishes a link with the AC for the first time.

AP State	Description
name-conflicted	The name of the AP conflicts with that of an existing AP.
normal	The AP is working properly.
standby	The AP is in normal state on the standby AC.
unauth	The AP is not authenticated.