Lab6

1 Lab6 Creating a WLAN

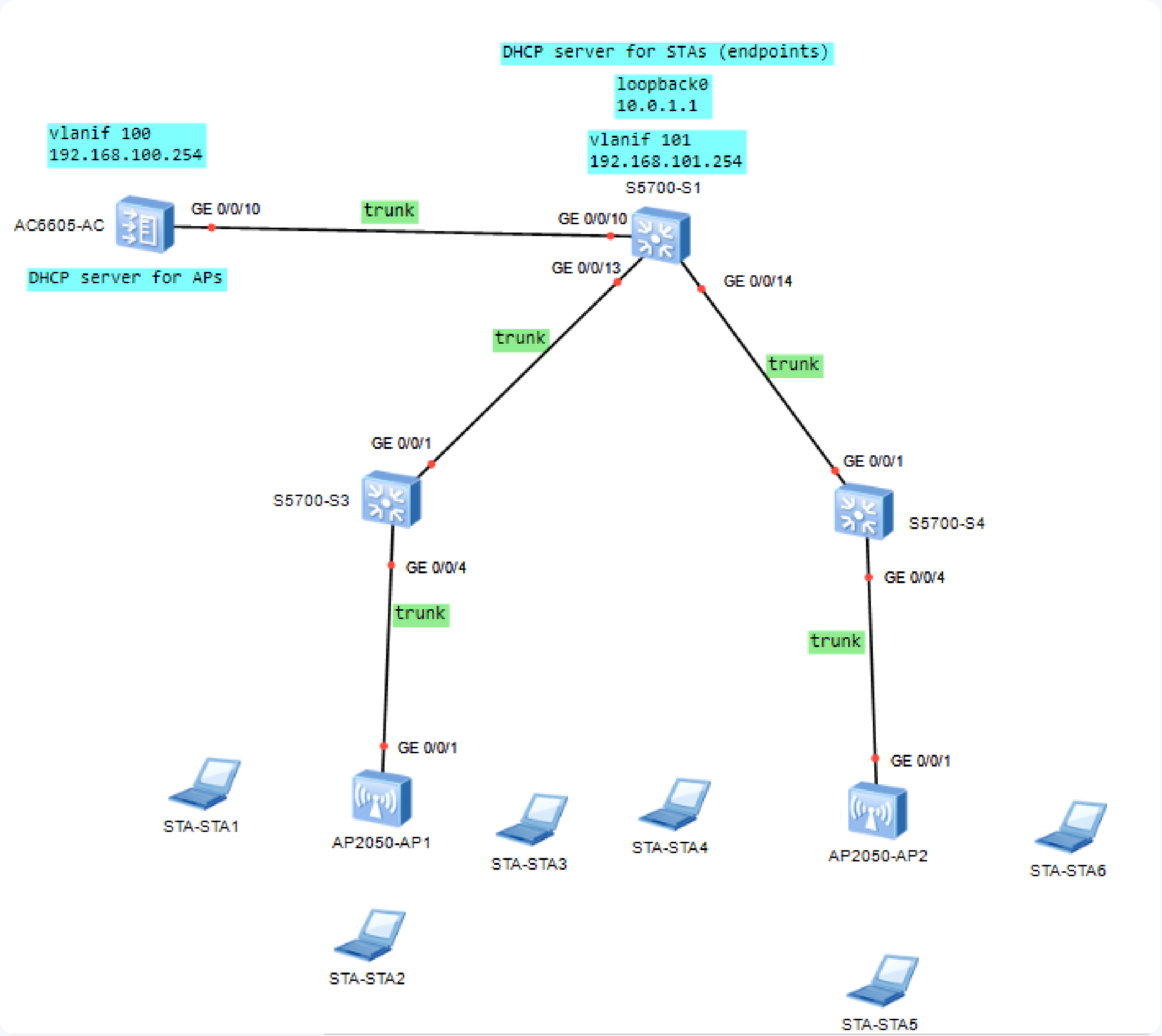
1.1 Overview

These notes summarize the process of configuring a WLAN with Huawei equipment, including setting up VLANs, DHCP services, AP groups, regulatory domain settings, and WLAN service parameters.

1.1.1 Network Components

- Access Controller (AC)
- Access Points (AP)
- Switches (S1, S3, S4)
- Service Terminal (STA)

1.1.2 General Steps



1. Create VLANs and assign IP addresses.
2. Configure IP pools for DHCP.
3. Set up AP groups and regulatory domains.
4. Configure CAPWAP source interface.
5. Bind regulatory domain profile to AP group.
6. Import APs to the AC.
7. Configure WLAN service parameters.

> 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.

> 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)

> (end devices)

Topology Service data

- Service data is directly forwarde
    - An Access Control system in out-of-path mode is on the same network as the Access Point but doesn't intercept all traffic; it's part of the local network but not a direct gateway for client data.
    - While the AP communicates directly with clients, the AC can monitor or apply policies to traffic without routing packets through itself, allowing data to travel unimpeded to its destination.

Item	Configuration
AP Management VLAN	VLAN100
Service VLAN	VLAN101
DHCP Server (for APs)	AC as DHCP server
DHCP Server (for STAs)	S1 as DHCP server
STA Default Gateway	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
AC's Source Interface IP	VLANIF100: 192.168.100.254/24
AP Group Name	ap-group1
Referenced Profiles	VAP profile HCIA-wlan, Regulatory domain profile default

Item	Configuration
Regulatory Domain Profile	Name: default
Country Code	CN

Item	Configuration
SSID Profile	Name: HCIA-WLAN
SSID Name	HCIA-WLAN

Item	Configuration
Security Profile	Name: HCIA-WLAN
Security Policy	WPA-WPA2+PSK+AES
Password	HCIA-Datacom

VAP Profile Attribute	Value
Name	HCIA-WLAN
Forwarding Mode	Direct Forwarding
Service VLAN	VLAN 101
Referenced SSID Profile	HCIA-WLAN
Referenced Security Profile	HCIA-WLAN

Explanation

- **AP Management VLAN (VLAN 100):** A dedicated VLAN for network management traffic between Access Points and the wireless controller.
- **Service VLAN (VLAN 101):** A VLAN for user data traffic to segregate it from other network traffic.
- **IP Address of AC's Source Interface (VLANIF100):** 192.168.100.254/24 is the IP address used by the Access Controller to communicate with APs on VLAN 100.
- **AP Group (ap-group1):** A collection of APs sharing common settings like SSID and regulatory domain profiles.
- **Regulatory Domain Profile (default):** Sets power levels and channels per local regulations, here preset for China ("CN").
- **SSID Profile (HCIA-WLAN):** Configures the Wi-Fi network name that users see when connecting to the WLAN.
- **Security Profile (HCIA-WLAN):** Defines WPA-WPA2 PSK authentication with AES encryption for WLAN access using the passphrase "HCIA-Datacom".
- **VAP Profile (HCIA-WLAN):** Details virtual AP settings including direct forwarding mode and associations with Service VLAN, SSID, and

Security profiles.

1.2 Configurations

1.2.1 Configure poe link

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

> These configuration for S3 & S4

> The `poe enable` command turns on Power over Ethernet to power devices connected to a port, but it's usually on by default.

1.2.2 VLAN Configuration with IP's

Requirement :

AP Management VLAN	**VLAN100**
Service VLAN	VLAN101
STA Default Gateway	192.168.101.254

AC:

```
[AC]vlan batch 100 101
[AC]interface GigabitEthernet0/0/10
[AC-GigabitEthernet0/0/10]port link-type trunk
```

```
[AC-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[AC-GigabitEthernet0/0/10]quit
[AC]int vlanif100
[AC-Vlanif100]ip add 192.168.100.254 24
```

> Creating vlans and configure trunk port to carry vlan tag frame and set ip as source ip for AC and gateway for AP's to communicate with AC

S1:

```markdown
[S1]vlan batch 100 101
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/10]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type trunk
[S1-GigabitEthernet0/0/13]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/13]interface GigabitEthernet0/0/14
[S1-GigabitEthernet0/0/14]port link-type trunk
[S1-GigabitEthernet0/0/14]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/14]q
[S1]int vlanif101
[S1-vlanif101]ip address 192.168.101.254 24
[S1-vlanif101]int loopback0
[S1-loopback0]ip address 10.0.1.1 32
```

> Creating vlans and configure trunk port to carry vlan tag frame and set ip as gateway for AP's to communicate with S1 to get ip address and

> communicate with external network

> Loopback address act as external network for testing purpose

S3:

```markdown
[S3]vlan batch 100 101
[S3]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/4
[S1-GigabitEthernet0/0/4]port link-type trunk
[S1-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/4]port trunk pvid vlan 100
```

> Creating vlans and configure trunk port to carry vlan tag frame

> The `port trunk pvid vlan 100` command assigns VLAN 100 as the default VLAN for untagged traffic on a trunk port.

S4:

```markdown
[S4]vlan batch 100 101
[S3]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/4
[S1-GigabitEthernet0/0/4]port link-type trunk
[S1-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
```

```
[S1-GigabitEthernet0/0/4]port trunk pvid vlan 100
```

> Creating vlans and configure trunk port to carry vlan tag frame

> The `port trunk pvid vlan 100` command assigns VLAN 100 as the default VLAN for untagged traffic on a trunk port.

1.2.3 DHCP Settings for STAs and APs on AC

Requirement:

AP Management VLAN	VLAN100
Service VLAN	VLAN101

DHCP Server (for APs)	AC as DHCP server
DHCP Server (for STAs)	S1 as DHCP server
STA Default Gateway	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

AC:

```
[AC]dhcp enable
[AC]ip pool ap
[AC-ip-pool-ap]network 192.168.100.0 mask 24
[AC-ip-pool-ap]gateway-list 192.168.101.254
[AC-ip-pool-ap]quit
[AC]int vlanif100
[AC-Vlanif100]dhcp select global
```

> Configure dhcp for AC to assign IP's AP's

S1:

```
[S1]dhcp enable
[S1]ip pool sta
[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]int vlanif101
[S1-Vlanif101]dhcp select global
```

> Configure dhcp for S1 to assign IP's STA's

1.2.4 AP Group Configuration on AC

Requirement:

AP Group Name	ap-group1

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
```

AP group

> An AP group aggregates multiple access points as a single entity for easy configuration and management.

1.2.5 Regulatory Domain Profile Binding on AC

Requirement:

Item	Configuration
Regulatory Domain Profile	Name: default
Country Code	CN

```Markdown
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name default
[AC-wlan-regulate-domain-default]country-code cn
```

⚠ **Regulatory Domain**

> Changing the country code will reset the AP after clearing channel and power configurations.

```Markdown
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
```

> Bind the regulatory domain profile to an AP group.

1.2.6 CAPWAP Tunnel Source Interface on AC

Requirement:

AP Management VLAN	VLAN100
Service VLAN	VLAN101
STA Default Gateway	192.168.101.254

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

> CAPWAP tunnels are used by access points to communicate with the controller.

1.3 Importing APs to AC

```
[AC]wlan
[AC-wlan-view]ap auth-mode mac-auth
[AC-wlan-view]ap-id 0 ap-mac 00e0-fc9a-6cc0
[AC-wlan-ap-0]ap-name ap1
[AC-wlan-ap-0]ap-group ap-group1
[AC-wlan-ap-0]ap-id 1 ap-mac 00e0-fcf2-4430
[AC-wlan-ap-1]ap-name ap2
[AC-wlan-ap-1]ap-group ap-group1
```

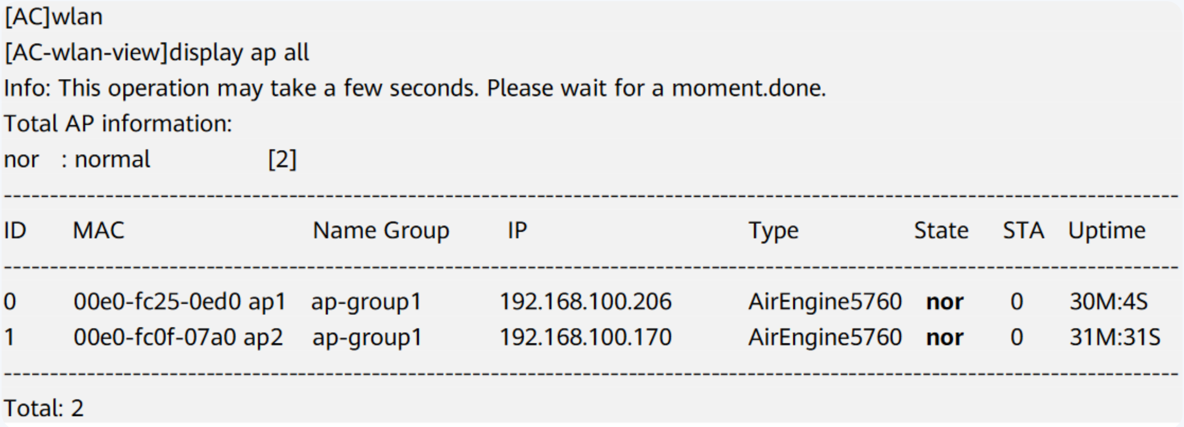
> Sets authentication mode based on MAC address for AP's

> Adds an AP using its MAC address

> Sets a custom name for an AP

> Binds an AP to a specific group

Display the information about the current:



```
[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
```

1.4 WLAN Service Parameters

1.4.1 Security Profile Creation on AC

Requirement:

Item	Configuration
Security Profile	Name: HCIA-WLAN
Security Policy	WPA-WPA2+PSK+AES
Password	HCIA-Datacom

```
[AC]wlan
[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

> The PSK is set to HCIA-Datacom. User data is encrypted using the AES encryption algorit

1.4.2 SSID Profile Creation on AC

Requirement:

Item	Configuration
SSID Profile	Name: HCIA-WLAN
SSID Name	HCIA-WLAN

```markdown
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
```

> Create SSID profile HCIA-WLAN and set the SSID name to HCIA-WLAN

1.4.3 VAP Profile Binding to AP Group on AC

Requirement:

VAP Profile Attribute	Value
Name	HCIA-WLAN
Forwarding Mode	Direct Forwarding
Service VLAN	VLAN 101
Referenced SSID Profile	HCIA-WLAN
Referenced Security Profile	HCIA-WLAN

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

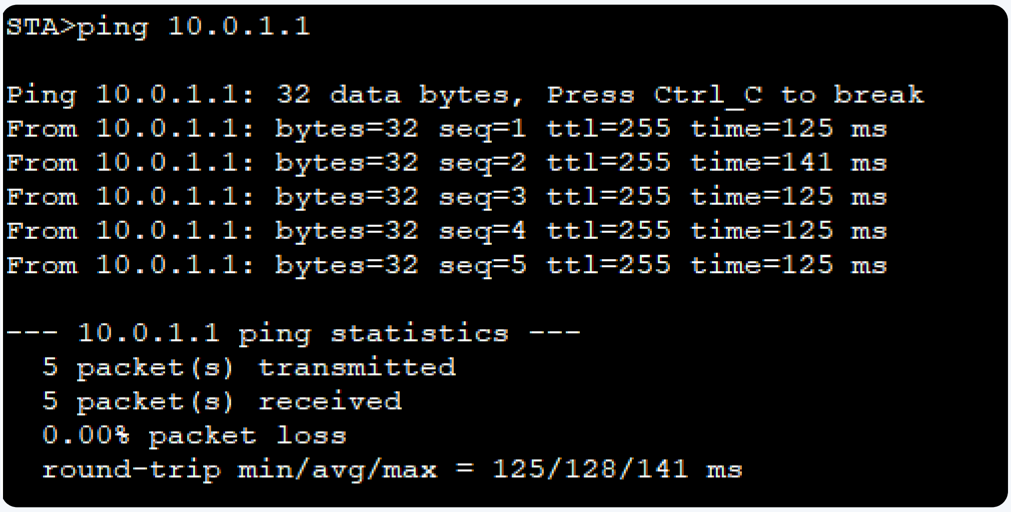
```
[AC-wlan-view]vap-profile name HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]forward-mode direct-forward
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]quit
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

Explanation

1. Create a VAP profile named HCIA-WLAN and configure data forwarding mode using `vap-profile` and `forward-mode` commands, respectively.
2. Set the service VLAN for the VAP with the `service-vlan` command, and bind the SSID and security profiles to the VAP.
3. Apply the VAP profile to both radio 0 and radio 1 in the AP group to ensure configurations are consistent across radios.
4. Use the `vap-profile` command to bind VAP profile HCIA-WLAN to the AP group, delivering all related configurations.

1.5 Verification Commands

1.5.1 Check connectivity from STA to S1 loopback

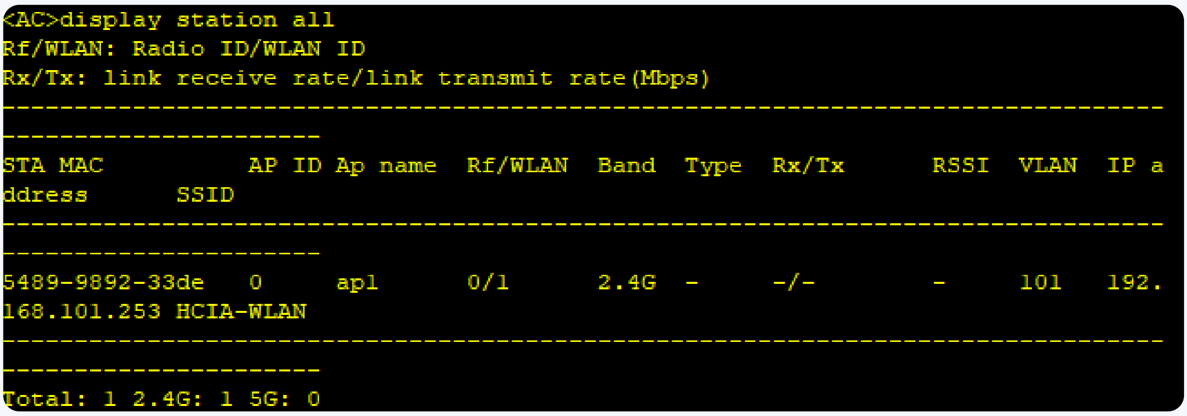


```
STA>ping 10.0.1.1

Ping 10.0.1.1: 32 data bytes, Press Ctrl_C to break
From 10.0.1.1: bytes=32 seq=1 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=2 ttl=255 time=141 ms
From 10.0.1.1: bytes=32 seq=3 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=4 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=5 ttl=255 time=125 ms

--- 10.0.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 125/128/141 ms
```

1.5.2 display station all



```
<AC>display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------
----------------------
STA MAC          AP ID Ap name  Rf/WLAN  Band  Type  Rx/Tx      RSSI  VLAN  IP a
ddress      SSID
--------------------------------------------------------------------------------
----------------------
5489-9892-33de   0     ap1      0/1      2.4G  -     -/-        -     101   192.
168.101.253 HCIA-WLAN
--------------------------------------------------------------------------------
----------------------
Total: 1 2.4G: 1 5G: 0
```

1.6 Quiz

Question1

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.

Answer1

1. If VLAN 101 is blocked on the network controller's port, devices won't be able to reach services on that VLAN, like S1.
2. If all traffic is sent through a tunnel to the network controller and VLAN 101 isn't blocked there, devices can access S1 even if local network ports block VLAN 101.

- Here's what happens with your data traffic:
  - If direct forwarding is used, your data is sent directly through the network without going through a specific port (GigabitEthernet0/0/10) on the Access Controller (AC).
  - If tunnel forwarding is used and you need to go through GigabitEthernet0/0/10 on the AC, make sure that this port is configured to allow traffic from VLAN 101; otherwise, your device will not be able to communicate with S1.

- > Direct Forwarding: Sending data packets directly to the destination within the same network without intermediaries.

- > Tunnel Forwarding: Encapsulating data packets within another packet to securely traverse different networks or boundaries via a tunnel.

Question2

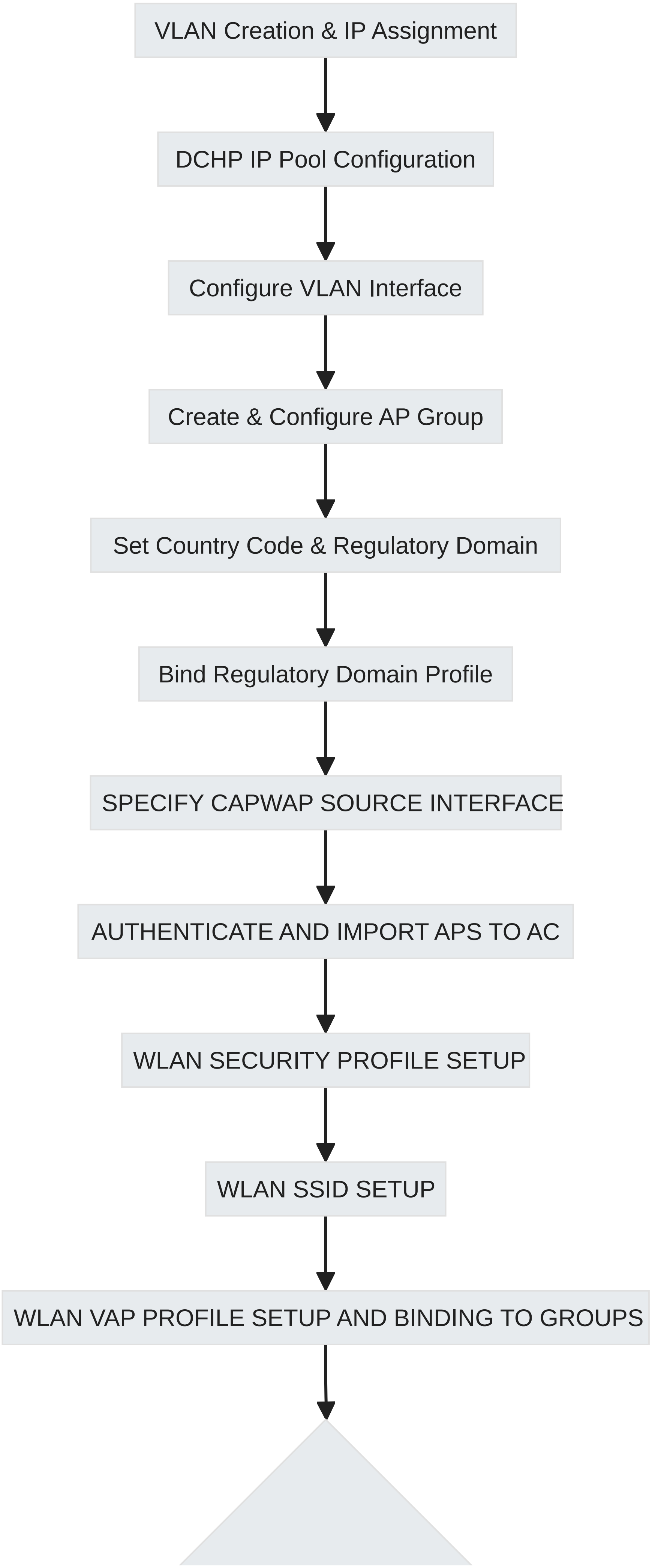
When the STA is connected to the AC, run the display station all command on the AC to check the STA information

✓ **Answer2**

AP1 and AP2 use different VAP profiles, and different service-VLAN parameters are configured in the VAP profile

1.7 Simplified Process Flow

Below is a simplified process flow chart illustrating the steps from VLAN creation through verification using the Mermaid syntax suitable for Markdown rendering:


VLAN Creation & IP Assignment
DCHP IP Pool Configuration
Configure VLAN Interface
Create & Configure AP Group
Set Country Code & Regulatory Domain
Bind Regulatory Domain Profile
SPECIFY CAPWAP SOURCE INTERFACE
AUTHENTICATE AND IMPORT APS TO AC
WLAN SECURITY PROFILE SETUP
WLAN SSID SETUP
WLAN VAP PROFILE SETUP AND BINDING TO GROUPS

VERIFICATION STEPS