TE 156: Introduction to Communication Networks

Dr. Justice Owusu Agyemang

Presentation Outline

- WLAN

Foreword

- Wired LANs are expensive and lack mobility. The increasing demand for portability and mobility requires wireless local area network (WLAN) technologies.
- WLAN is now the most cost-efficient and convenient network access mode.
- This course introduces the development of WLAN in different phases, concepts related to WLAN technologies, implementation and basic configurations of common WLAN networking architectures, and WLAN development trends.

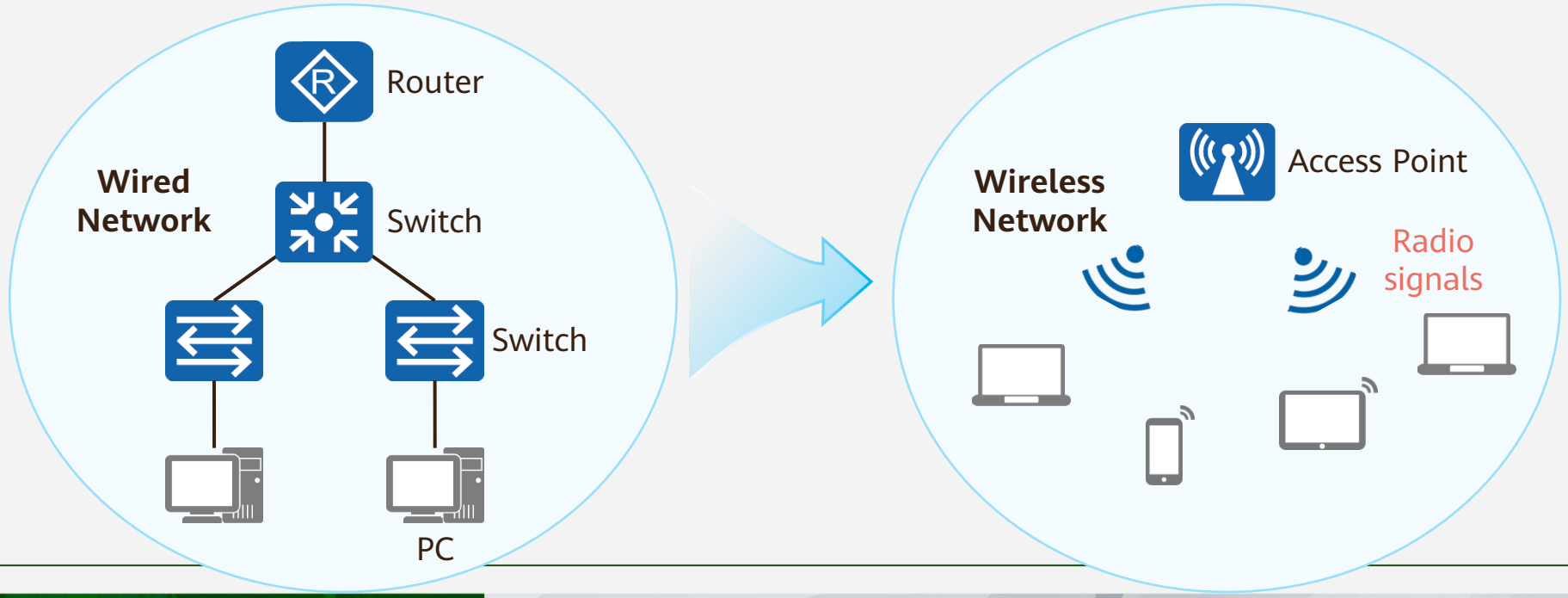
Objectives

- On completion of this course, you will be able to:
  - Understand basic concepts of WLAN and the history of the 802.11 protocol family.
  - Learn about different WLAN devices.
  - Distinguish between different WLAN networking architectures.
  - Understand the WLAN working process.
  - Complete basic WLAN configurations.

Contents

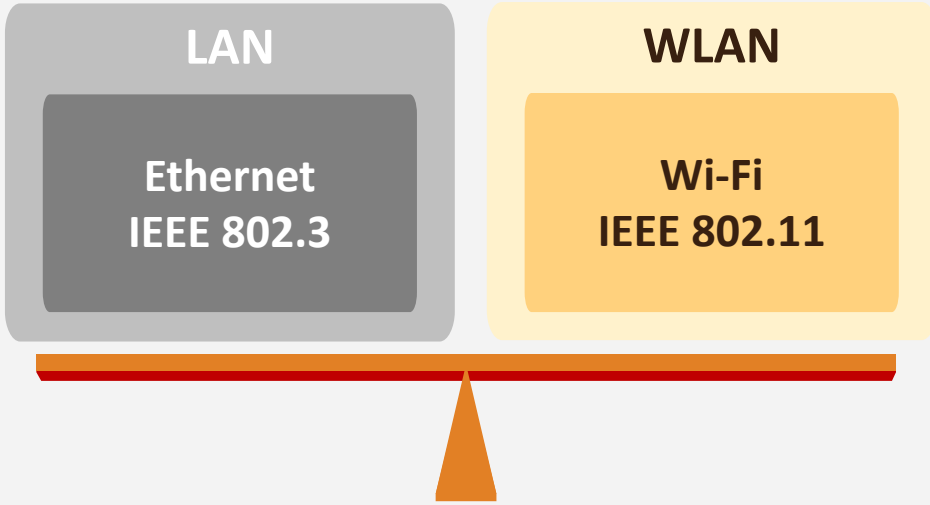
Introduction to WLAN

- A wireless local area network (WLAN) is constructed using wireless technologies. It uses high-frequency (2.4 GHz or 5 GHz) signals such as radio waves, lasers, and infrared rays to replace the traditional media used for transmission on a wired LAN.
- WLAN technology allows users to easily access a wireless network and move around within the coverage of the wireless network.



IEEE 802.11、WLAN and Wi-Fi

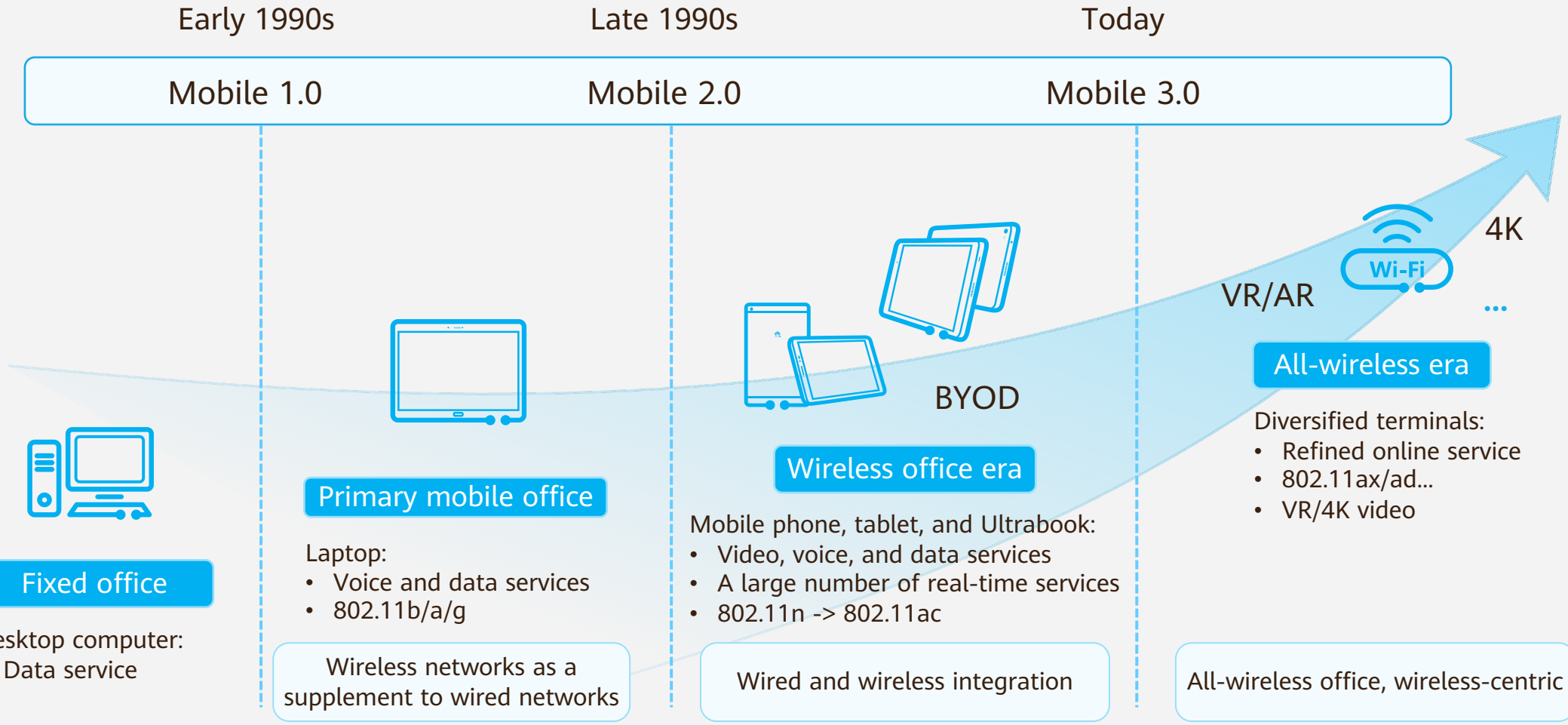
- IEEE 802.11 suites are standards for WLANs which are definded by the Institute of Electrical and Electronics Engineering (IEEE).
- Wi-Fi Alliance was formed by a group of major manufacturers and the logo "Wi-Fi" was created. The Wi-Fi standards are WLAN technologies based on IEEE 802.11 standards.



- **IEEE 802.11 Standards and Wi-Fi Generations**

Frequency Band	2.4GHz	2.4GHz	2.4GHz、5GHz	2.4GHz & 5GHz	5GHz	5GHz	2.4GHz & 5GHz
Throughput	2Mbit/s	11Mbit/s	54Mbit/s	300Mbit/s	1300Mbit/s	6.9Gbit/s	9.6Gbit/s
Standard	802.11	802.11b	802.11a、802.11g	802.11n	802.11ac wave1	802.11ac wave2	802.11ax
Wi-Fi	Wi-Fi 1	Wi-Fi 2	Wi-Fi 3	Wi-Fi 4	Wi-Fi 5		Wi-Fi 6
Released In	1997	1999	2003	2009	2013	2015	2018

Wi-Fi Development Trends in Office Scenarios



Contents

WLAN Devices

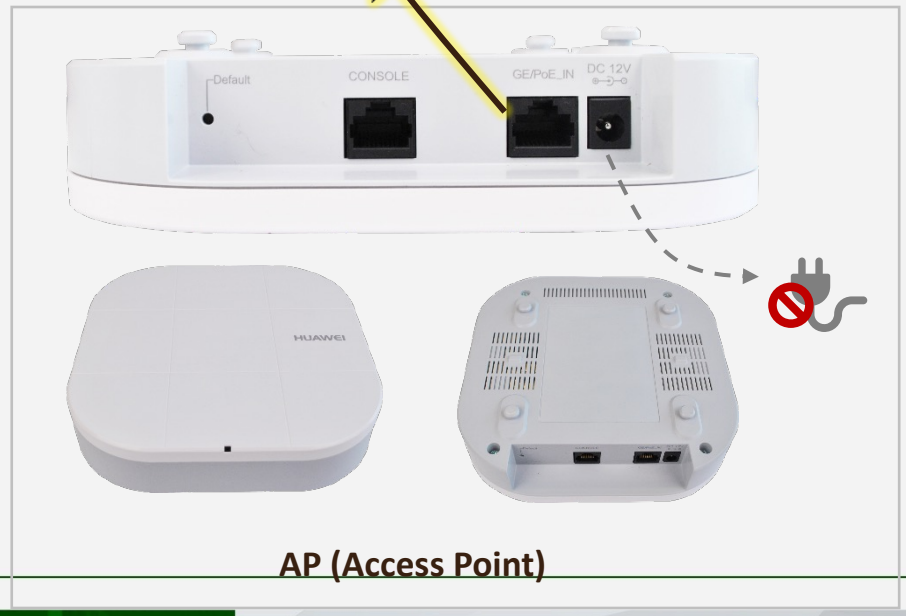
Home

Enterprise

PoE Switch

Network

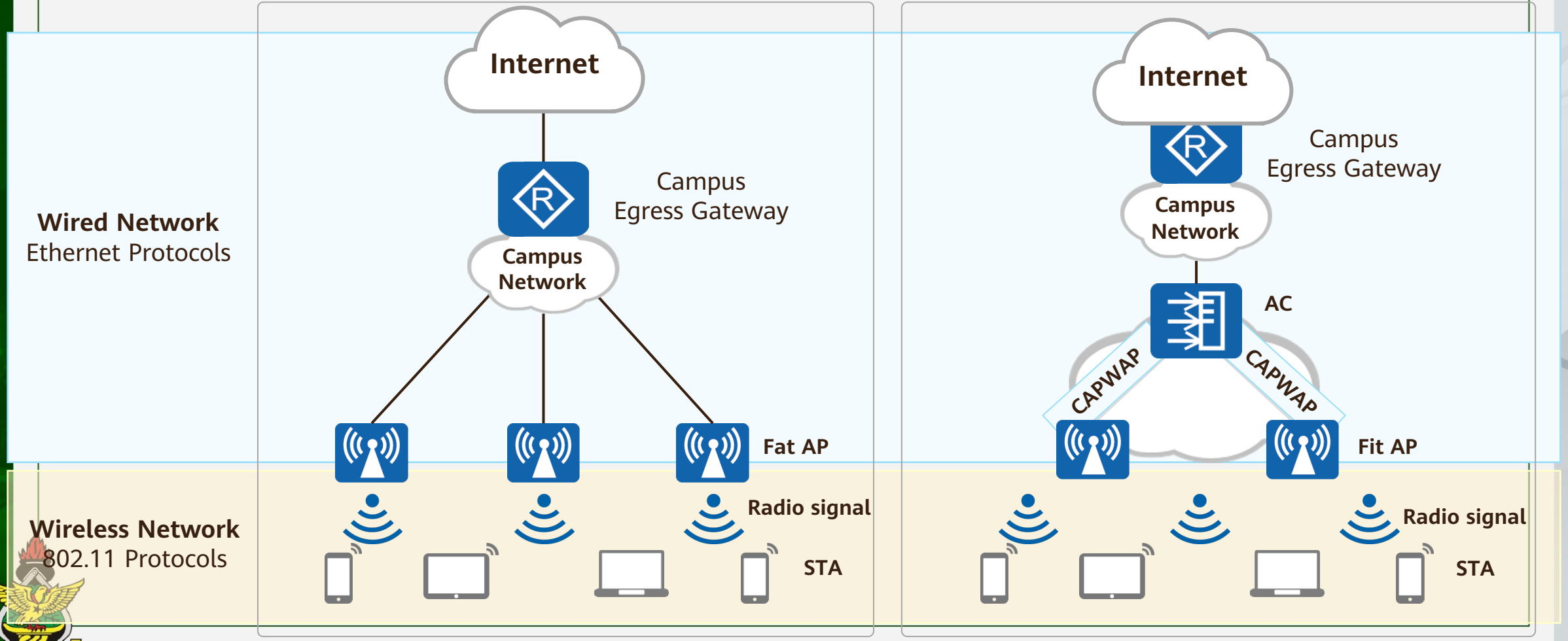
Wireless Router



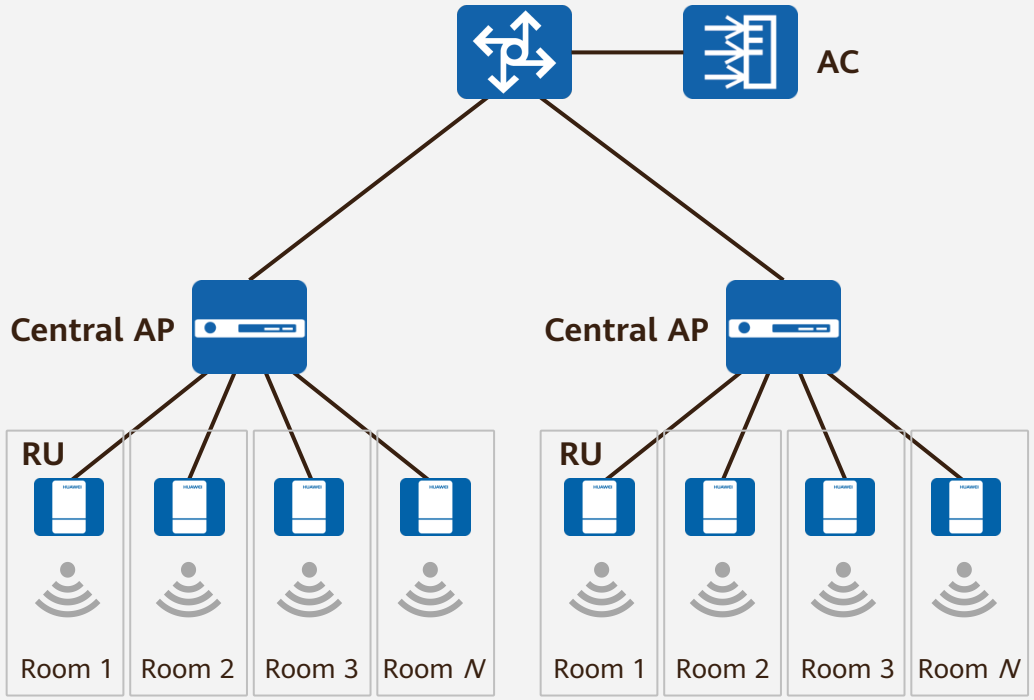
AP (Access Point)

AC (Access Controller)

Basic WLAN Networking Architecture



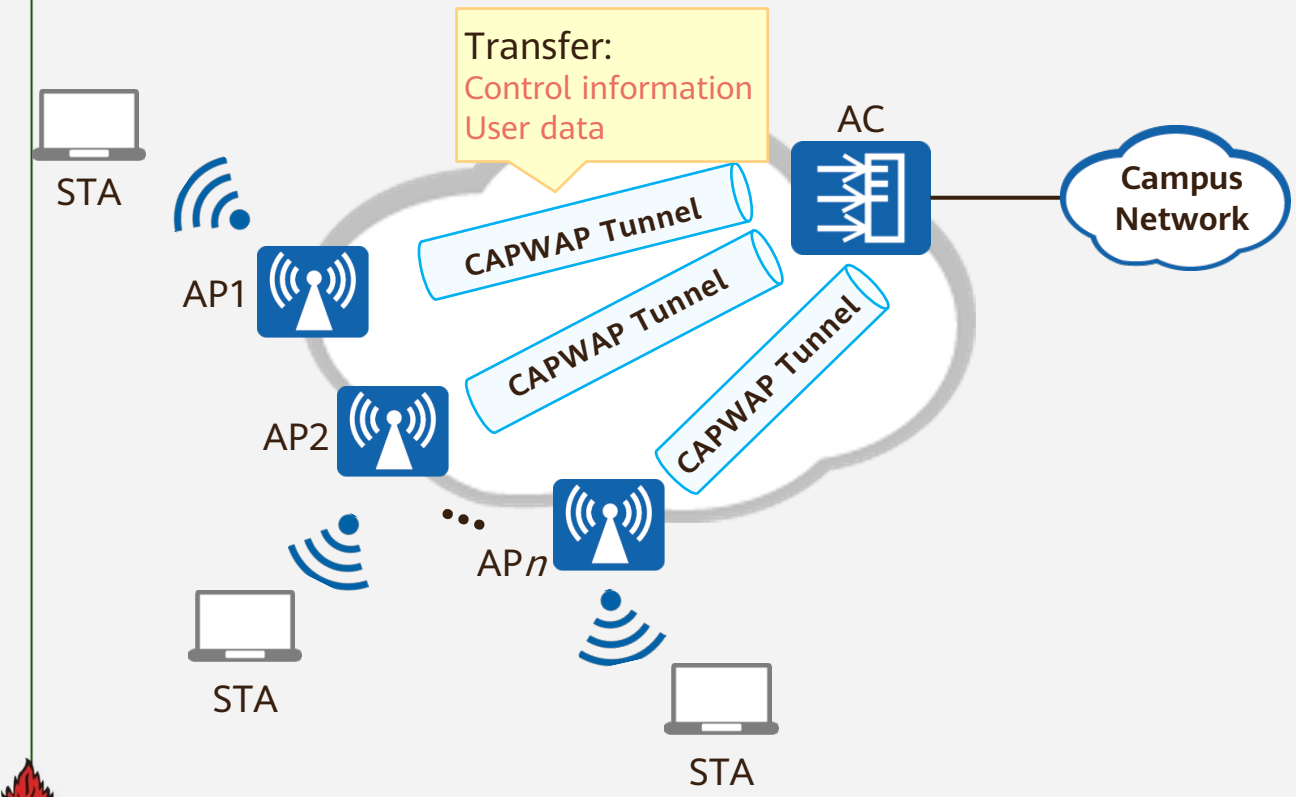
Agile Distributed Architecture



Architecture Characteristics

- The agile distributed architecture divides an AP into a central AP and remote units (RUs). The central AP can manage multiple RUs, which provides good coverage and reduces costs. RUs can be used in the Fat AP, AC + Fit AP, and cloud management architectures.
- Application scope: densely distributed rooms

CAPWAP



What Is a CAPWAP Tunnel?

- **Control And Provisioning of Wireless Access Points (CAPWAP)**: defines how to manage and configure APs. That is, an AC manages and controls APs in a centralized manner through CAPWAP tunnels.

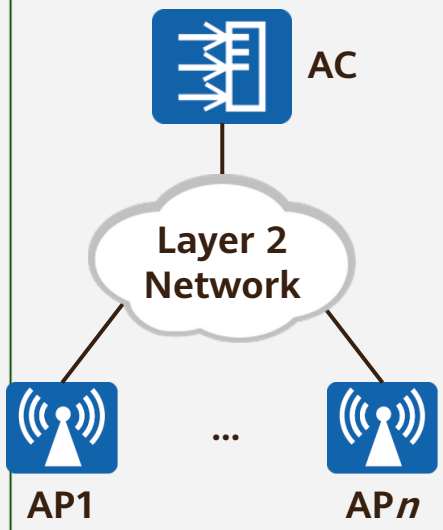
CAPWAP Tunnel Functions

- Maintains the running status of the AC and APs.
- Allows the AC to manage APs and deliver service configurations to the APs.
- Allows APs to exchange data sent by STAs with the AC through CAPWAP tunnels when the tunnel forwarding mode is used.

AP-AC Networking

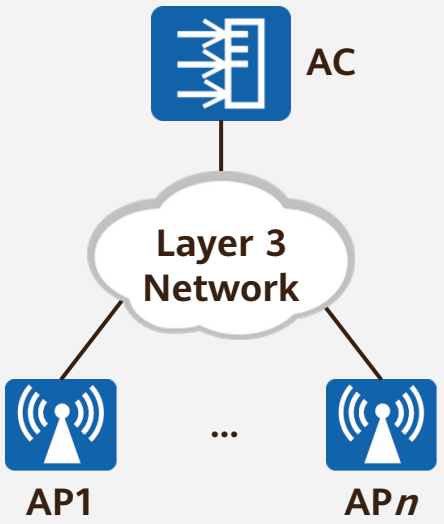
- The AP-AC networking modes are classified into Layer 2 networking and Layer 3 networking.

Layer 2 Networking



- Layer 2 networking: APs are connected to an AC directly or across a Layer 2 network.
- The Layer 2 networking features quick deployment. It is applicable to simple or temporary networking but not to large networking.

Layer 3 Networking

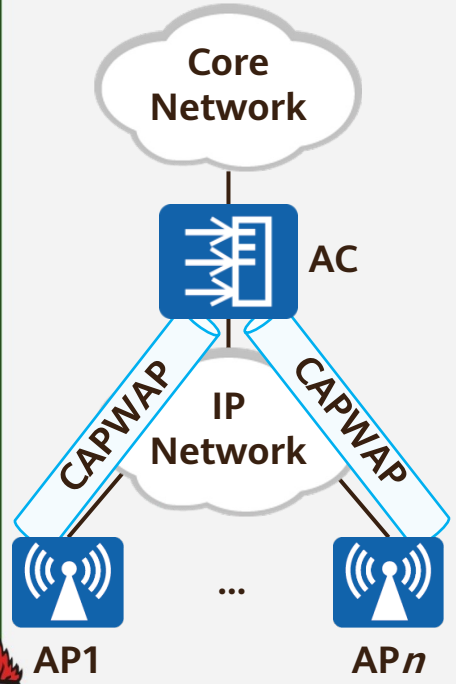


- Layer 3 networking: APs are connected to an AC across a Layer 3 network.
- In the actual networking, an AC can connect to dozens or even hundreds of APs, which is usually complex. In most cases, the Layer 3 networking is used on a large network.

AC Connection Mode

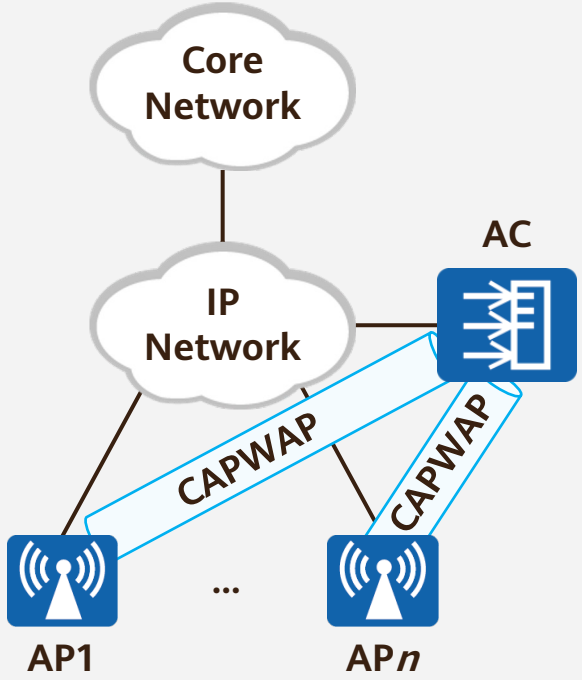
- ACs can be connected in in-path or off-path mode.

In-Path Networking



- In the in-path networking, the APs, AC, and core network are connected in a chain. All data destined for the core layer passes through the AC.
- In this networking, the AC also functions as an aggregation switch to forward and process data traffic and management traffic of APs.

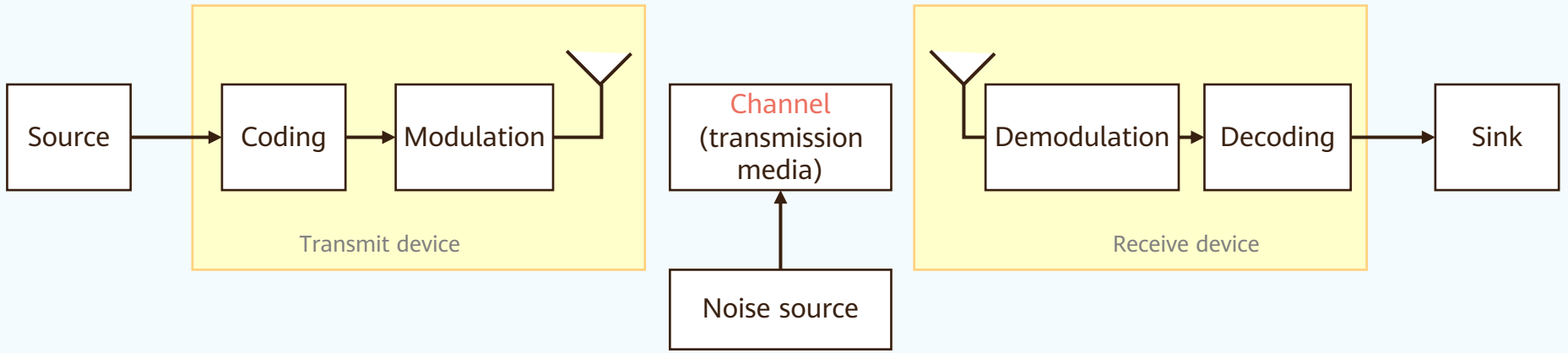
Off-Path Networking



- In the off-path networking, the AC connects to the network between APs and the core network, but does not directly connect to APs.
- In this networking, the AC is connected to APs in off-path mode, the service data of APs reaches the uplink network without passing through the AC.

Wireless Communications System

- In a wireless communications system, information may be an image, a text, a sound, or the like. The transmit device first applies source coding to convert information into digital signals that allow for circuit calculation and processing, and then into radio waves by means of channel coding and modulation.

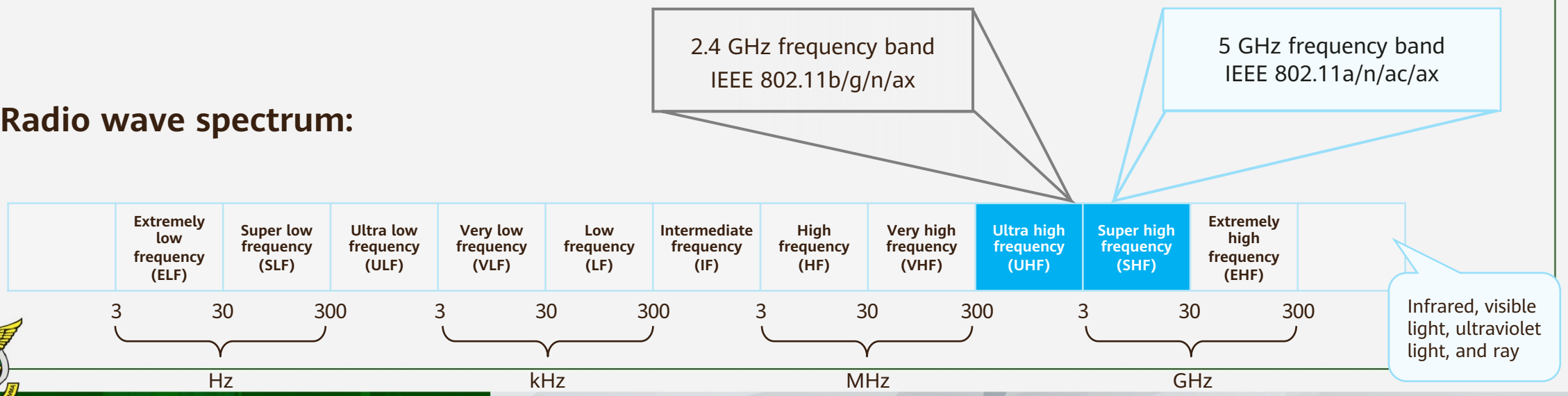


Wireless Communications System

Radio Wave

- A radio wave is an electromagnetic wave whose frequency is between 3 Hz and about 300 GHz. Radio technology converts sound signals or other signals and transmits them by using radio waves.
- WLAN technology enables transmission of information by radio waves over the air. Currently, the WLAN uses the following frequency bands:
  - 2.4 GHz frequency band (2.4–2.4835 GHz)
  - 5 GHz frequency band (5.15–5.35 GHz, 5.725–5.85 GHz)

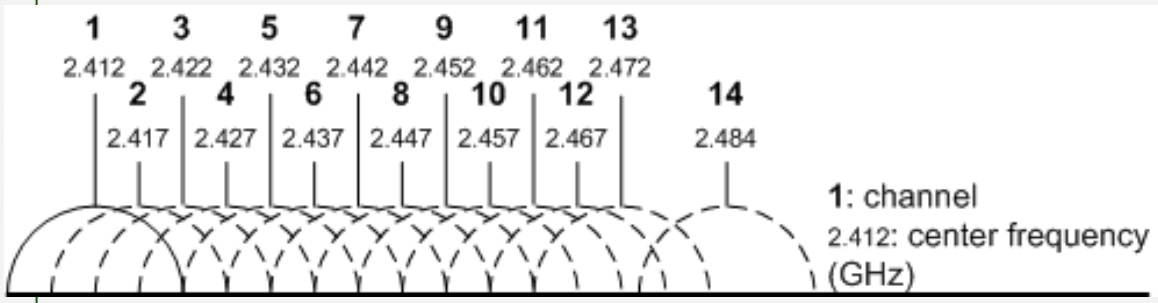
- **Radio wave spectrum:**



Radio Channel

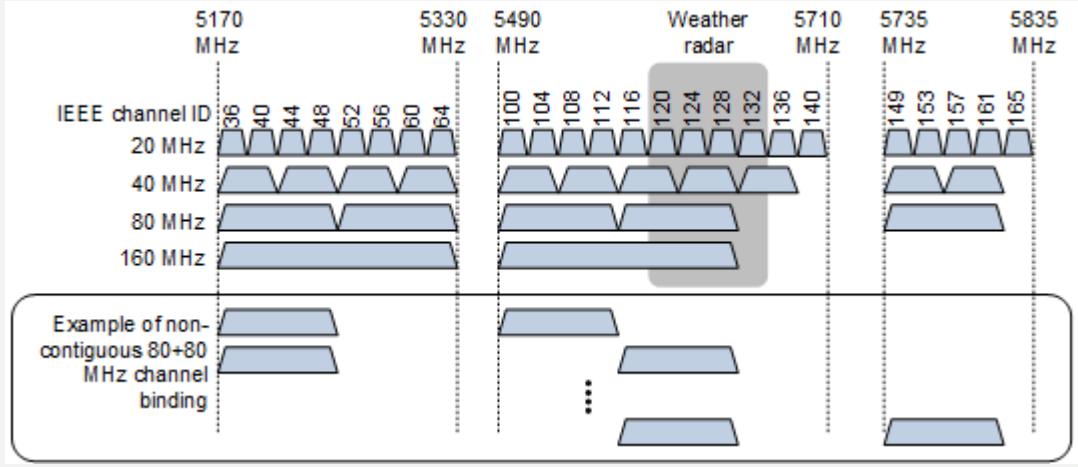
- A channel transmits information, and a radio channel is a radio wave in space. Given that radio waves are ubiquitous, the random use of spectrum resources will cause endless interference issues. Therefore, in addition to defining the usable frequency bands, wireless communication protocols must also accurately divide the frequency ranges. Each frequency range is a channel.

2.4 GHz Frequency Band



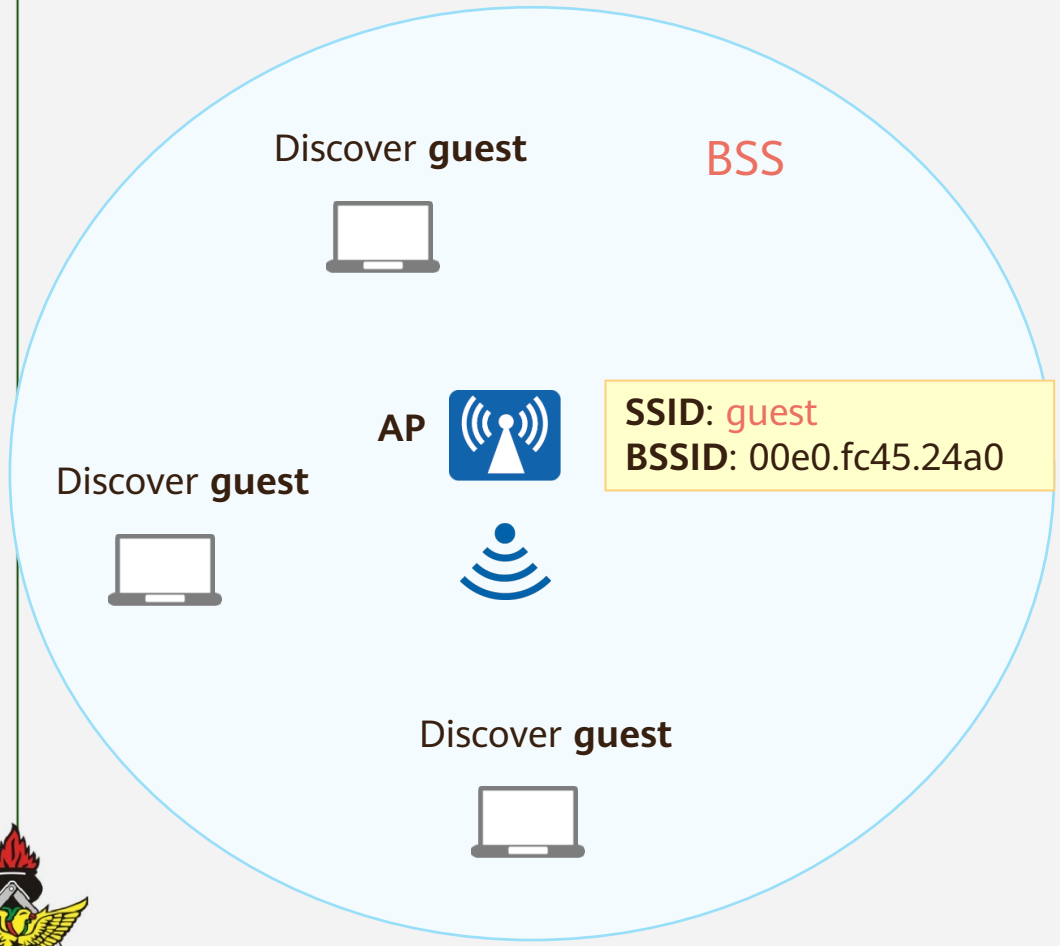
- The 2.4 GHz frequency band is divided into 14 channels with overlapping or non-overlapping relationships, each with a bandwidth of 20 MHz.
  - Overlapping channels, such as channels 1 and 2, interfere with each other.
  - Non-overlapping channels, such as channels 1 and 6, do not interfere with each other.

5 GHz Frequency Band



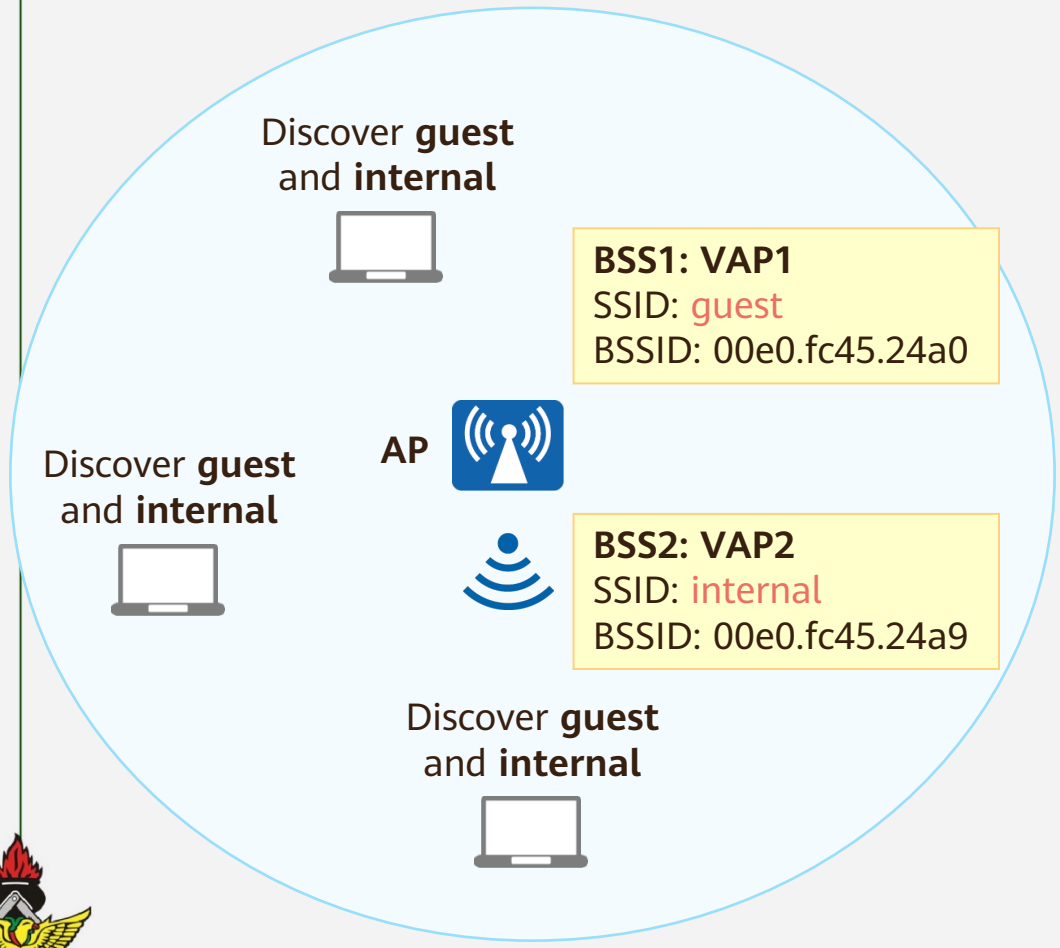
- The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz, 80 MHz, and higher-bandwidth channels.

BSS/SSID/BSSID



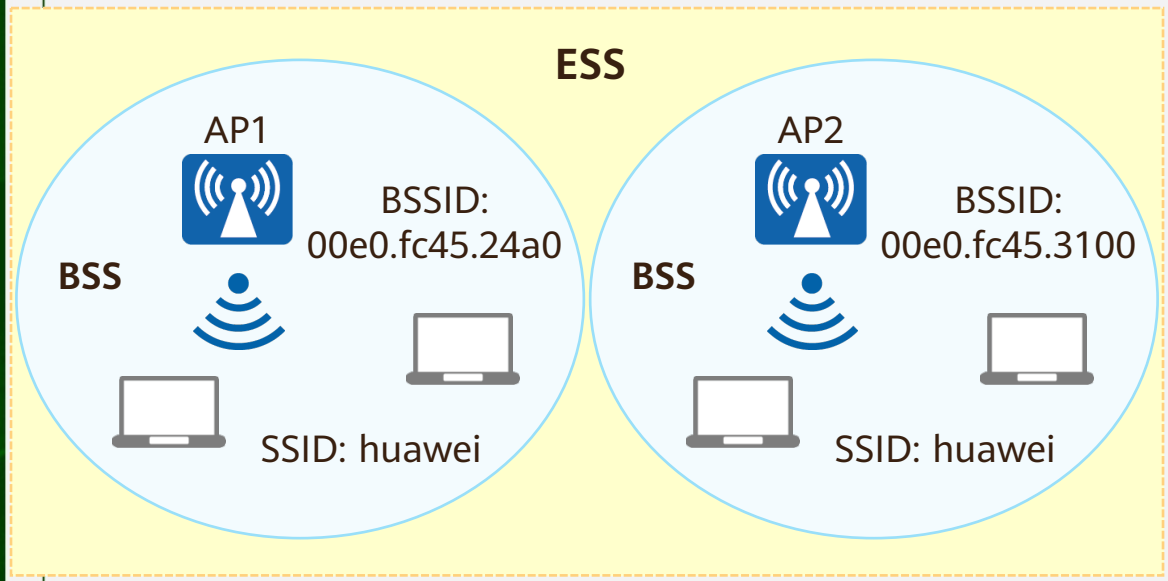
- Basic service set (BSS):
  - An area covered by an AP.
  - STAs in a BSS can communicate with each other.
- Basic service set identifier (BSSID):
  - An identifier of a WLAN, which is represented by the AP's MAC address.
- Service set identifier (SSID):
  - An identifier of a WLAN, which is represented by a string of characters.
  - SSIDs can replace BSSIDs to help users identify different WLANs.

VAP



- In the early stage, APs support only one BSS. If multiple BSSs are deployed in a space, we must also deploy multiple APs, which increases costs and occupies channel resources. To resolve this problem, APs now support creation of multiple virtual access points (VAPs).
- VAP:
  - A physical AP can be virtualized into multiple VAPs, each of which provides the same functions as the physical AP.
  - Each VAP corresponds to one BSS. In this way, one AP may provide multiple BSSs that can have different SSIDs specified.

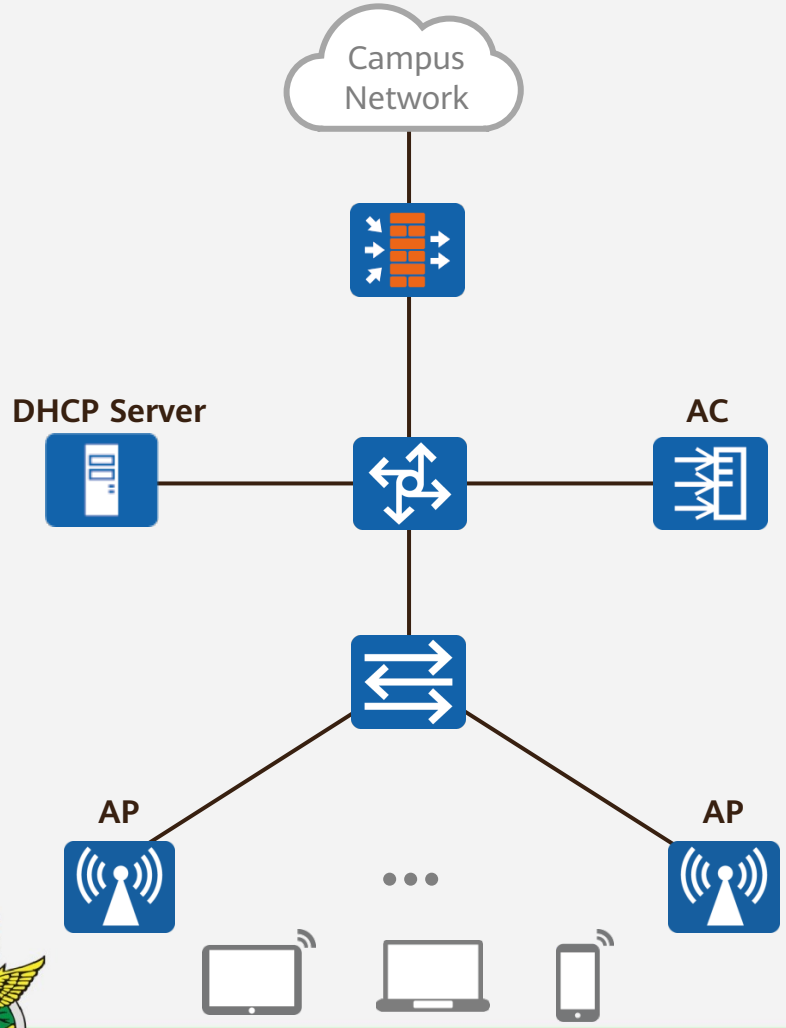
ESS



- The coverage of a BSS is limited. An extended service set (ESS) can be used to expand the coverage. When a STA moves from one BSS to another BSS, an ESS ensures that the STA does not sense the change of the SSID.
- ESS:
  - A larger-scale virtual BSS that consists of multiple BSSs with the same SSID.

Contents

WLAN Working Process Overview



WLAN Working Process

1. AP onboarding

An AP obtains an IP address, discovers an AC, and sets up a connection with the AC.

2. WLAN service configuration delivery

The AC delivers WLAN service configurations to the AP.

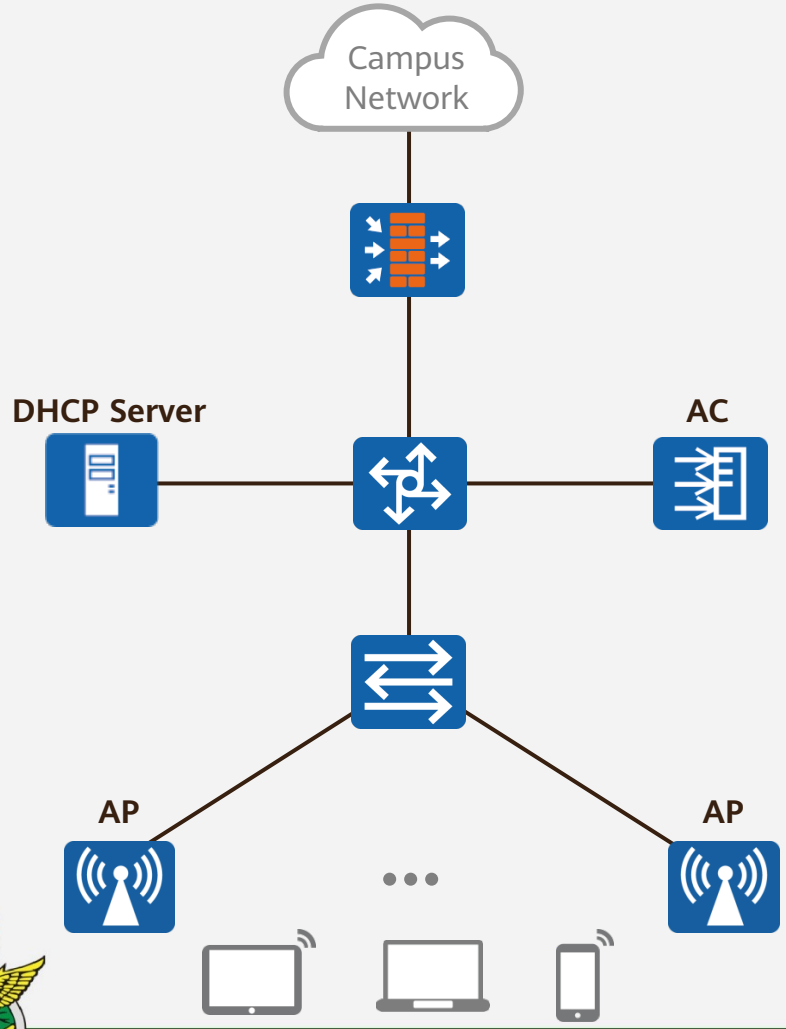
3. STA access

STAs find the SSID transmitted by the AP, connect to the network, and go online.

4. WLAN service data forwarding

The WLAN starts to forward service data.

WLAN Working Process: Step 1



WLAN Working Process

1 AP onboarding

The AC can manage and control Fit APs in a centralized manner and deliver services only after they go online. The procedure is as follows:

1. An AP obtains an IP address.
2. The AP discovers the AC and establishes a CAPWAP tunnel with it.
3. AP access control
4. AP upgrade
5. CAPWAP tunnel maintenance

2 WLAN service configuration delivery

3 STA access

4 WLAN service data forwarding

APs Obtain IP Addresses

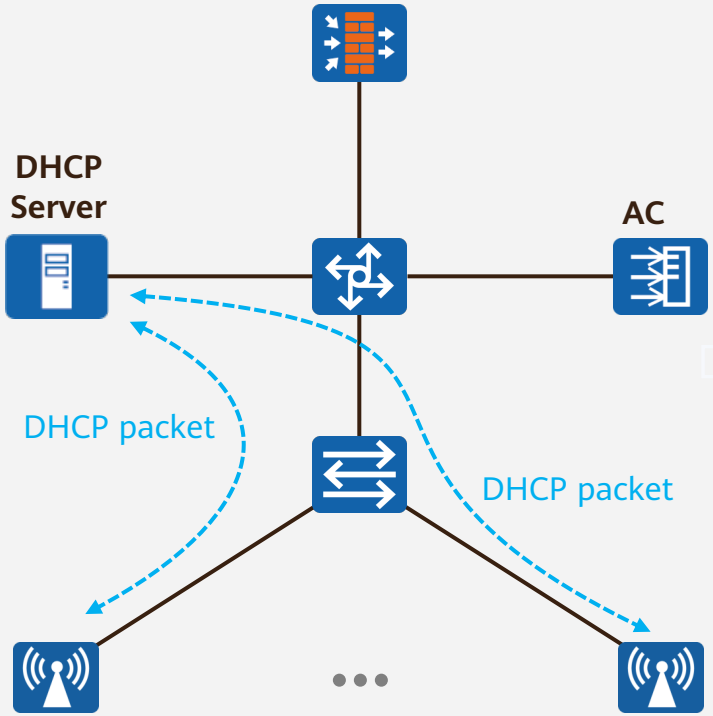
- An AP can communicate with an AC only after obtaining an IP address.

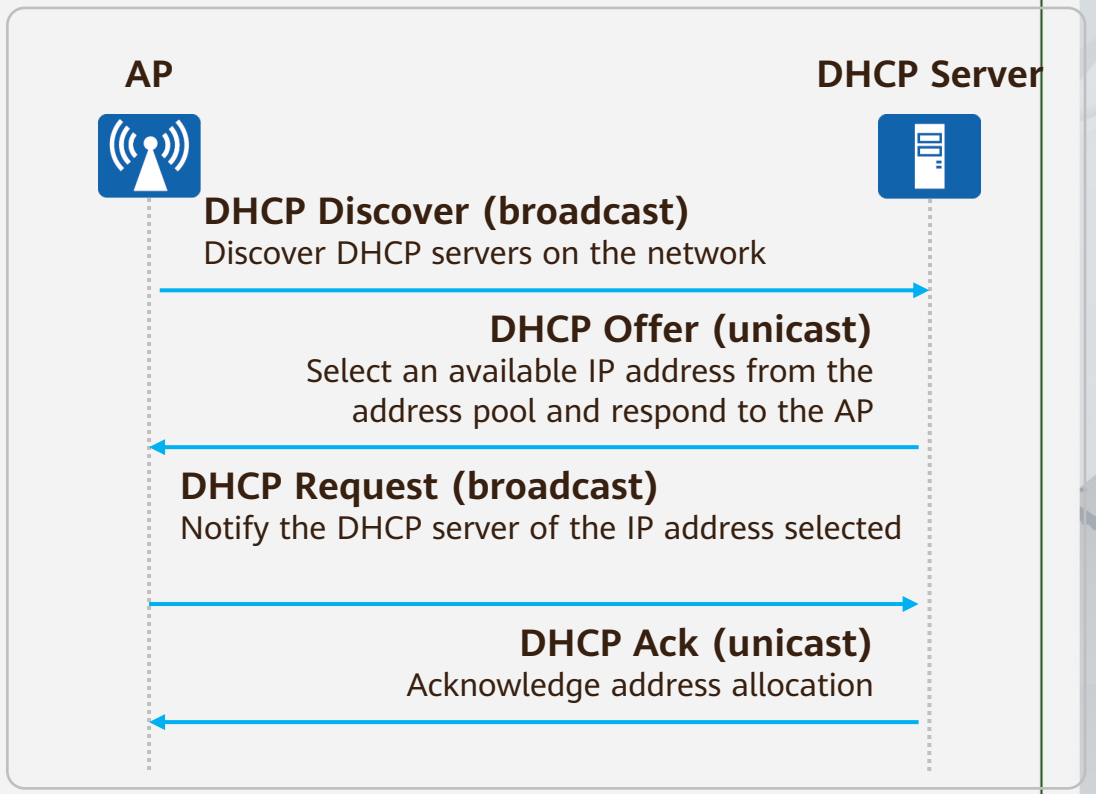
IP Address Allocation

- An AP can obtain an IP address in either of the following modes:
  - Static mode: A user logs in to the AP and configures its IP address.
  - DHCP mode: The AP serves as a DHCP client and requests an IP address from a DHCP server.
- Typical solutions:
  - Deploy a dedicated DHCP server to assign IP addresses to APs.
  - Configure the AC to assign IP addresses to APs.
  - Use a device on the network, such as a core switch, to assign IP addresses to APs.

DHCP IP Address Allocation

- IP address allocation
- CAPWAP tunnel establishment
- AP access control
- AP upgrade (Optional)
- CAPWAP tunnel maintenance





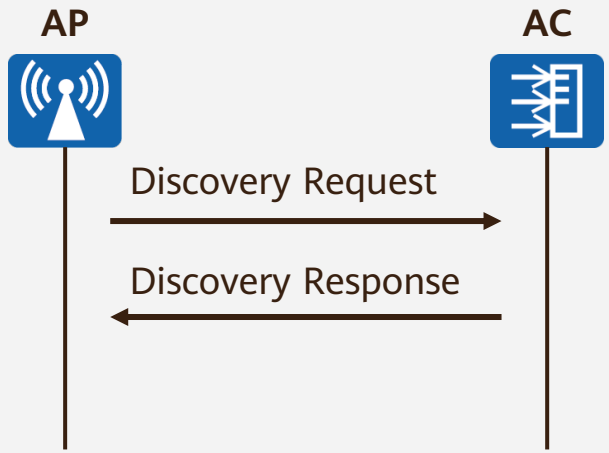
CAPWAP Tunnel Establishment

- IP address allocation
- **CAPWAP tunnel establishment**
- AP access control
- AP upgrade (Optional)
- CAPWAP tunnel maintenance

- The AC manages and controls APs in a centralized manner through CAPWAP tunnels.

Step 1: AC Discovery

- An AP sends a Discovery Request packet to find an available AC.
- APs can discover an AC in either of the following ways:
  - Static: AC IP address list preconfigured on the APs
  - Dynamic: DHCP, DNS, and broadcast



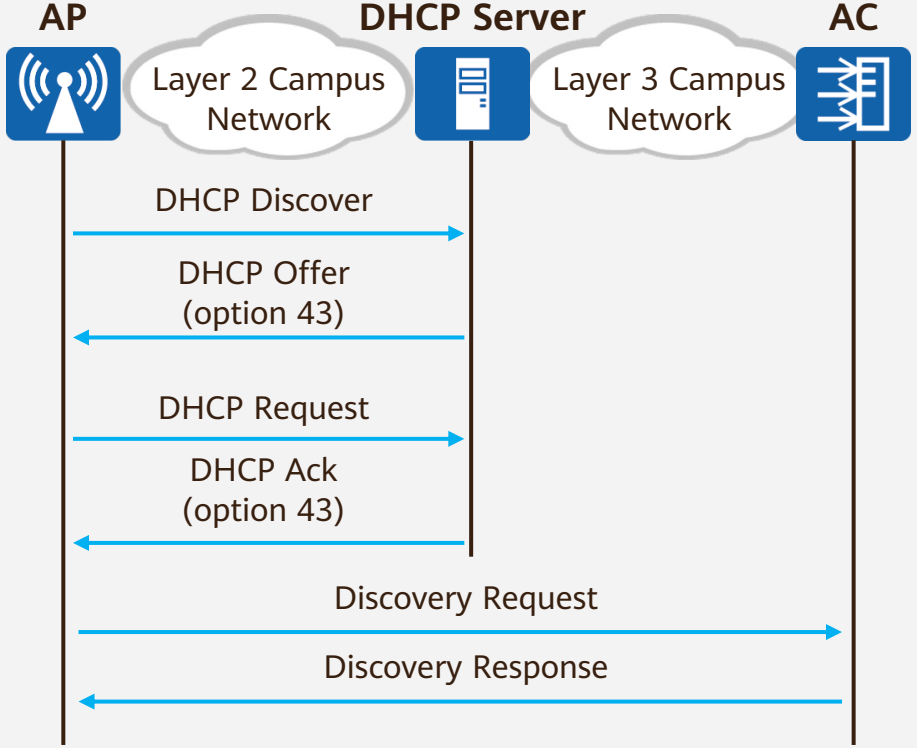
Step 2: CAPWAP Tunnel Establishment

- APs associate with the AC and establish CAPWAP tunnels, including data tunnels and control tunnels.
  - Data tunnel: transmits service data packets from APs to the AC for centralized forwarding.
  - Control tunnel: transmits control packets between the AC and APs.

Step 1: APs Dynamically Discover the AC

- IP address allocation
- **CAPWAP tunnel establishment**
- AP access control
- AP upgrade (Optional)
- CAPWAP tunnel maintenance

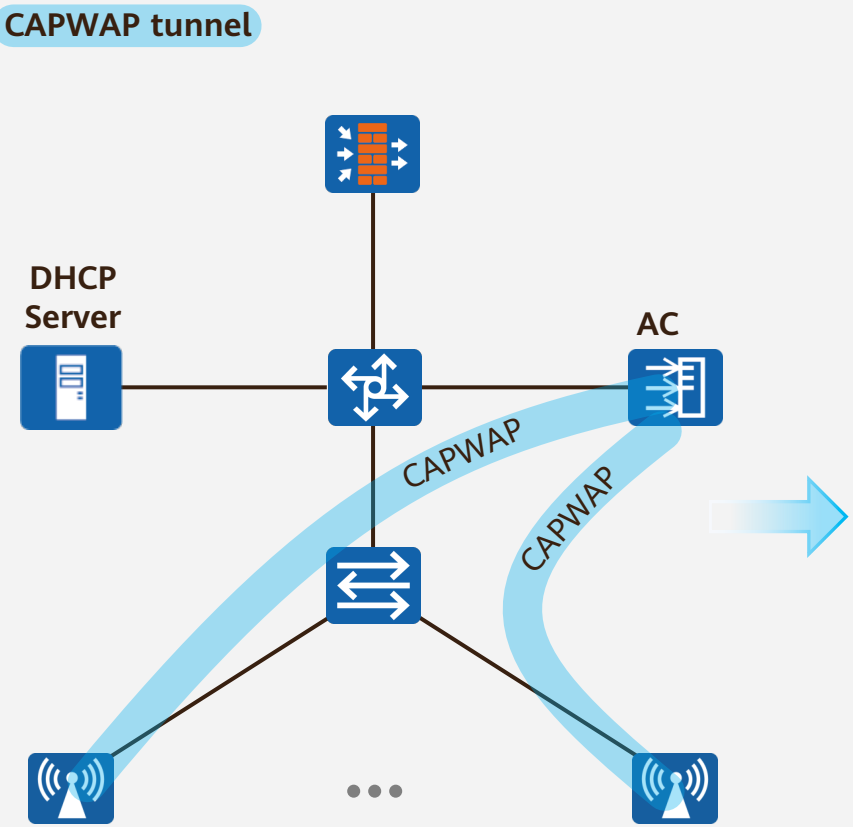
DHCP Mode (Layer 3 Networking)



Broadcast Mode (Layer 2 Networking)

Step 2: CAPWAP Tunnel Establishment

- IP address allocation
- **CAPWAP tunnel establishment**
- AP access control
- AP upgrade (Optional)
- CAPWAP tunnel maintenance



Step 2: CAPWAP Tunnel Establishment

- APs associate with the AC and establish CAPWAP tunnels, including data tunnels and control tunnels.

  Data tunnel: transmits service data packets from APs to the AC for centralized forwarding. Datagram Transport Layer Security (DTLS) encryption can be enabled over the data tunnel to ensure security of CAPWAP data packets. Subsequently, CAPWAP data packets will be encrypted and decrypted using DTLS.

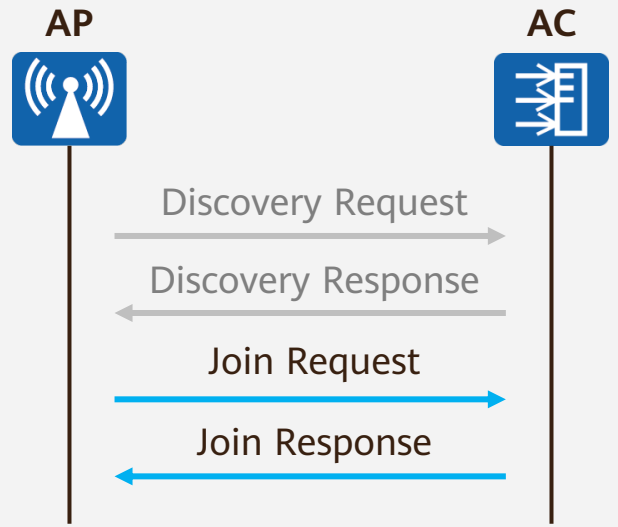
  Control tunnel: transmits control packets between the AC and APs. DTLS encryption can be enabled over the control tunnel to ensure security of CAPWAP control packets. Subsequently, CAPWAP control packets will be encrypted and decrypted using DTLS.

AP Access Control

- IP address allocation
- CAPWAP tunnel establishment
- **AP access control**
- AP upgrade (Optional)
- CAPWAP tunnel maintenance

AP Access Control

- After discovering and AC, the AP sends a Join Request packet to the AC. The AC then determines whether to allow the AP access and sends a Join Response packet to the AP.
- The AC supports three AP authentication modes: MAC address authentication, SN authentication, and non-authentication.



AP Upgrade

- IP address allocation
- CAPWAP tunnel establishment
- AP access control
- **AP upgrade (Optional)**
- CAPWAP tunnel maintenance

AP Upgrade

- The AP determines whether its system software version is the same as that specified on the AC according to parameters in the received Join Response packet. If they are different, the AP sends an Image Data Request packet to request the software package and then upgrades its software version in AC, FTP, or SFTP mode.
- After the software version is updated, the AP restarts and repeats steps 1 to 3.

CAPWAP Tunnel Maintenance

- IP address allocation
- CAPWAP tunnel establishment
- AP access control
- AP upgrade (Optional)
- **CAPWAP tunnel maintenance**

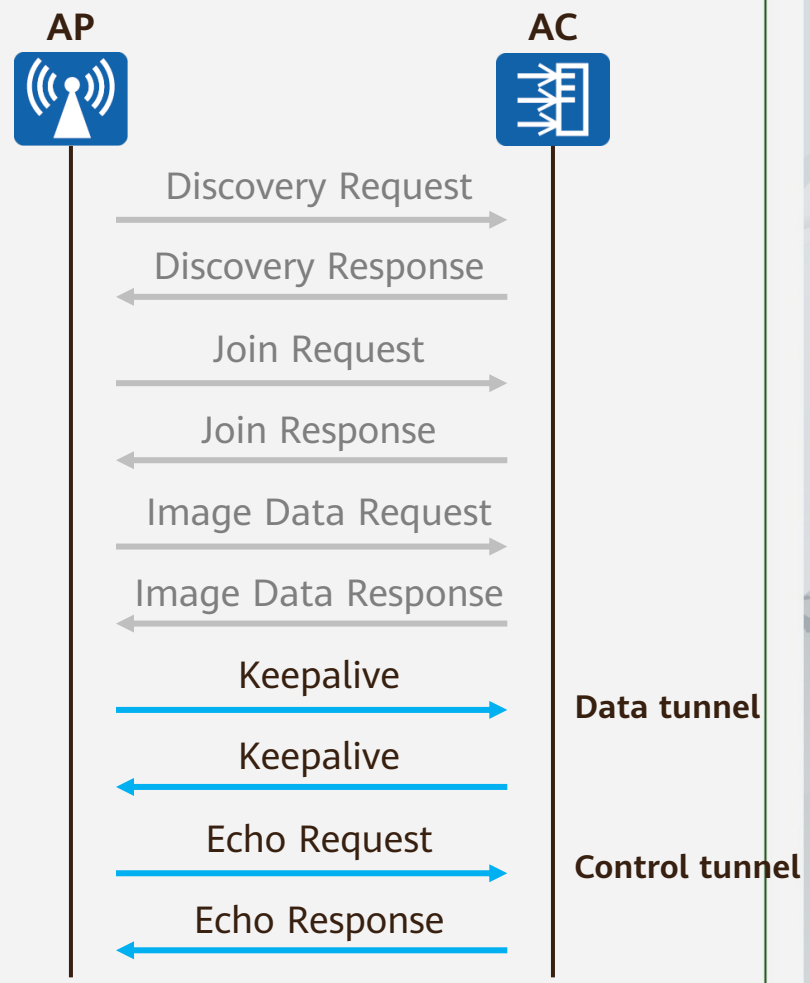
CAPWAP Tunnel Maintenance

- Data tunnel maintenance:

  The AP and AC exchange Keepalive packets to detect the data tunnel connectivity.

- Control tunnel maintenance:

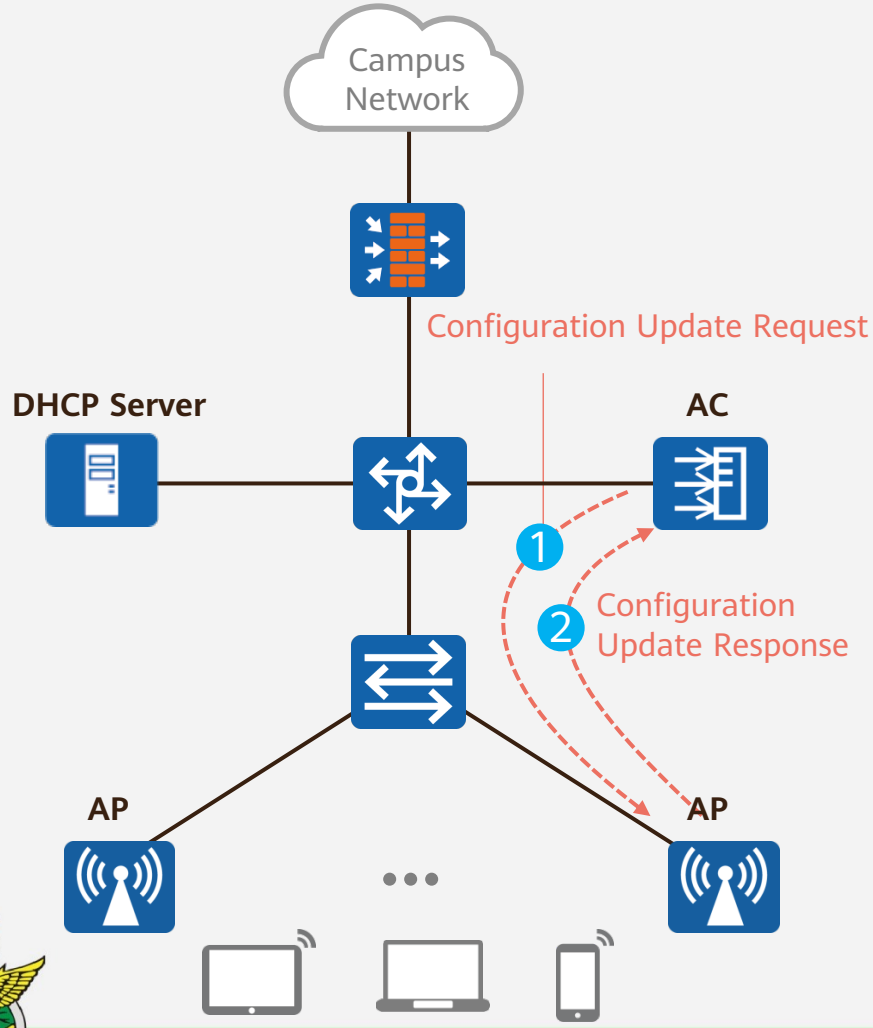
  The AP and AC exchange Echo packets to detect the control tunnel connectivity.



Preconfigurations on the AC for APs to Go Online

Configure network connectivity	• Configure DHCP servers to assign IP addresses to APs and STAs. The AC can function as a DHCP server. • Configure network connectivity between APs and the DHCP server, and between APs and the AC.
Create an AP group	Each AP will be added and can be added to only one AP group. In most cases, we configure an AP group to provide the same configurations for multiple APs.
Configure the country code on the AC (regulatory domain profile)	A country code identifies the country in which the APs are deployed. Country codes regulate different AP radio attributes, including the transmit power and supported channels.
Configure a source interface or address (for establishing CAPWAP tunnels with APs)	Specify a unique source IP address or source interface on each AC. APs must learn the specified source IP address or the IP address of the source interface to communicate with the AC and establish CAPWAP tunnels.
(Optional) Configure the automatic AP upgrade	In automatic upgrade mode, an AP checks whether its version is the same as that configured on the AC, SFTP server, or FTP server when going online. If the two versions are different, the AP upgrades its version, restarts, and goes online again. If the two versions are the same, the AP does not upgrade its version.
Add APs (configure the AP authentication mode)	You can add APs by importing them in offline mode, automatic discovery, and manual confirmation.

WLAN Working Process: Step 2



WLAN Working Process

① AP onboarding

② WLAN service configuration delivery

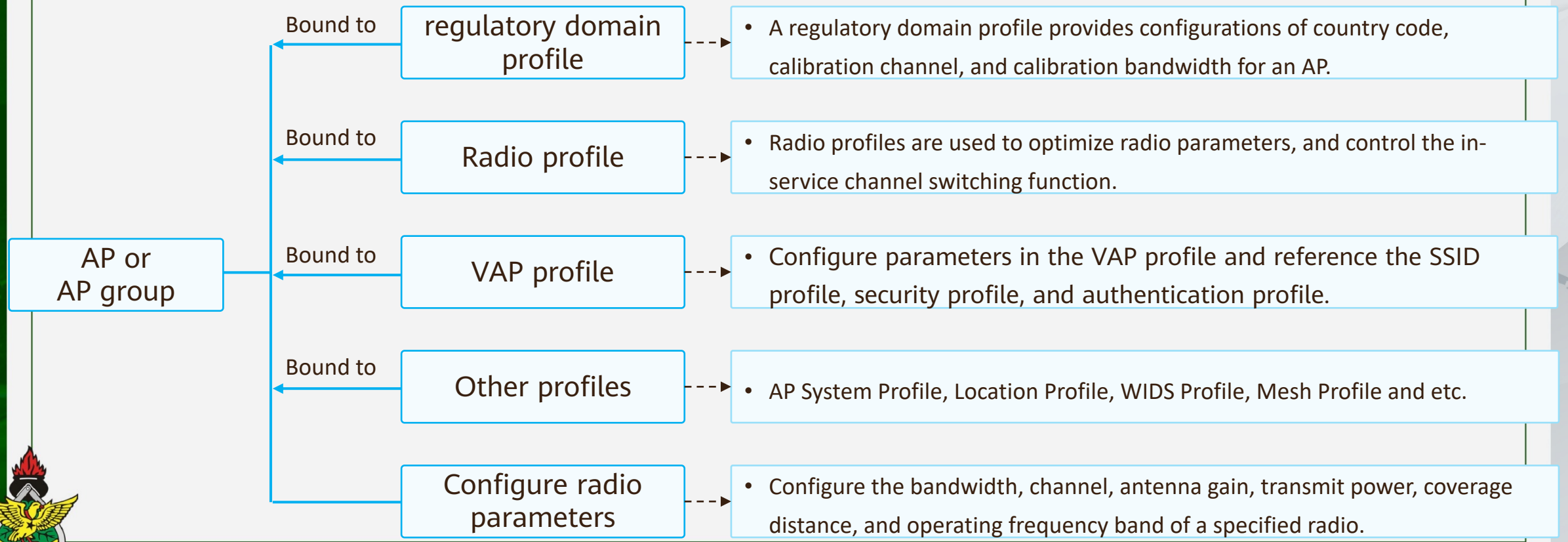
The AC sends a Configuration Update Request to an AP. If the AC receives a Configuration Update Response from the AP, the AC then delivers service configuration to the AP.

③ STA access

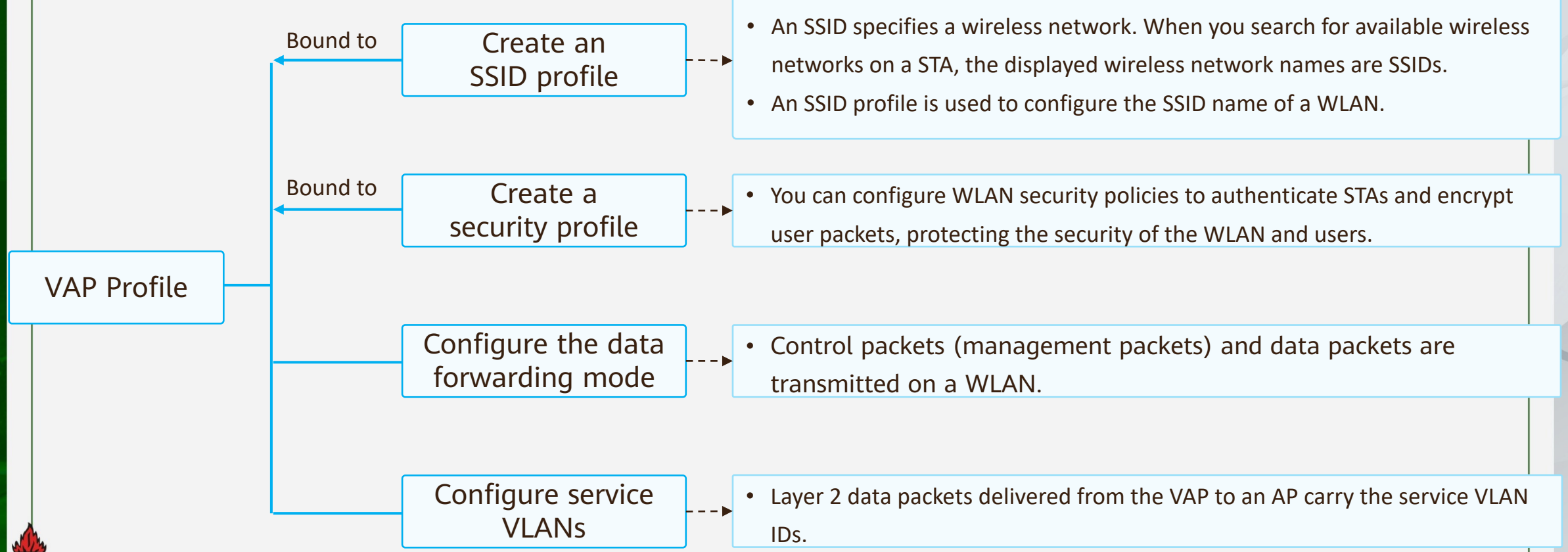
④ WLAN service data forwarding

WLAN Profiles

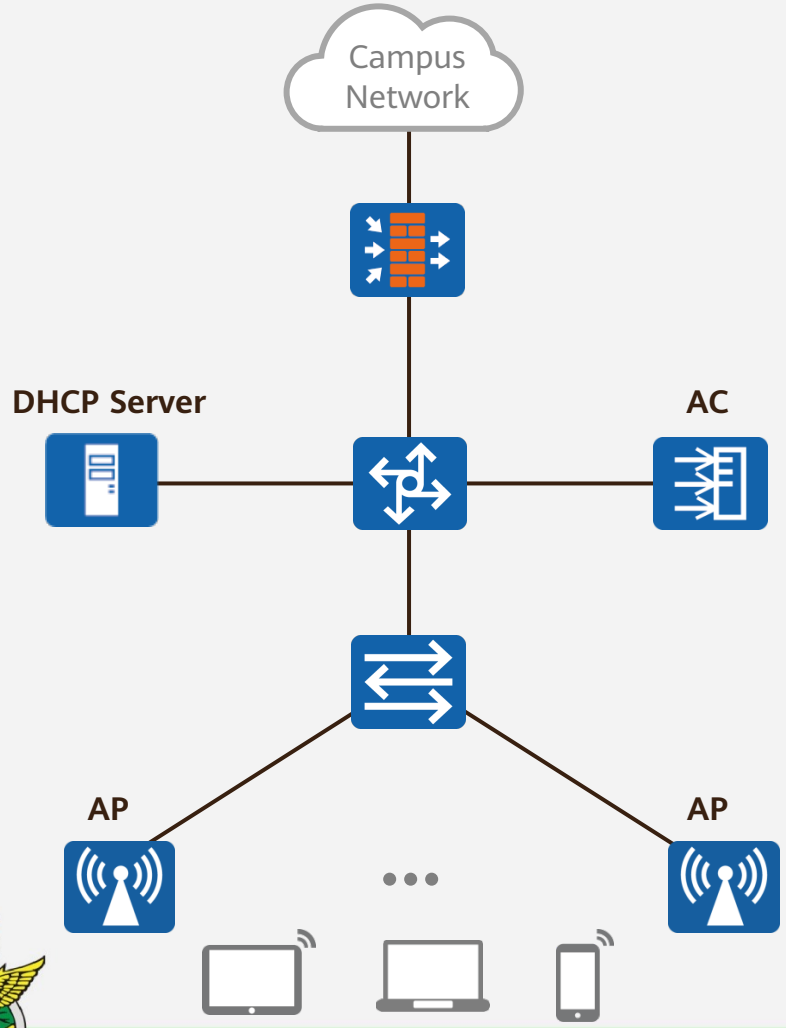
- Various profiles are designed based on different functions and features of WLAN networks to help users configure and maintain functions of WLAN networks. These profiles are called WLAN profiles.



VAP Profile



WLAN Working Process: Step 3



WLAN Working Process

① AP onboarding

② WLAN service configuration delivery

③ STA access

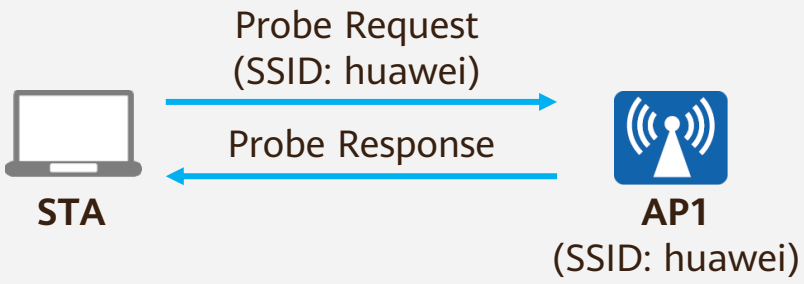
STAs can access a WLAN after CAPWAP tunnels are established.
The STA access process consists of six phases: scanning, link authentication, association, access authentication, DHCP, and user authentication.

④ WLAN service data forwarding

Scanning

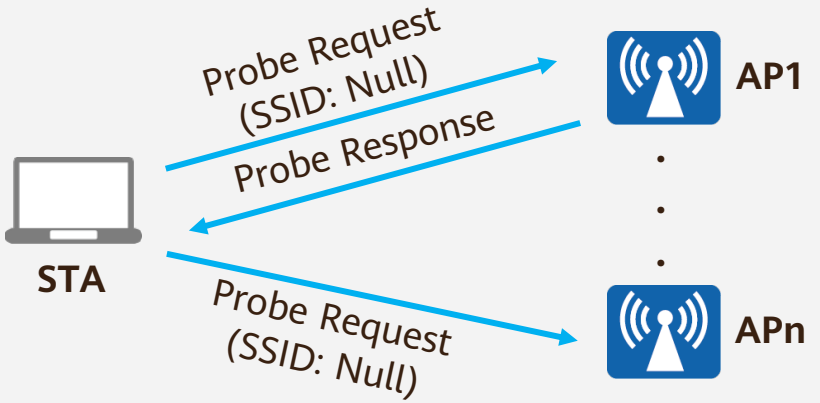
- In active scanning, a STA periodically searches for nearby wireless networks.
- The STA can send two types of Probe Request frames: probes containing an SSID and probes that do not contain an SSID.

Active Scanning by Sending a Probe Request Frame Containing an SSID



- The STA sends a Probe Request containing an SSID on each channel to search for the AP with the same SSID. Only the AP with the same SSID will respond to the STA.

Active Scanning by Sending a Probe Request Frame Containing No SSID



- The STA periodically broadcasts a Probe Request frame that does not contain an SSID on the supported channels. The APs return Probe Response frames to notify the STA of the wireless services they can provide.

WLAN Security Protocols

- As WLAN technologies use radio signals to transmit service data, service data can be easily intercepted or tampered with by attackers when being transmitted on open wireless channels. Ensuring WLAN security is crucial to building safe and effective wireless networks.
- Common security policy:

Scanning

Link authentication

Association

Access authentication

DHCP

User authentication

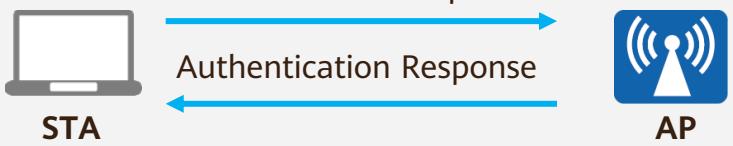
Security Policy	Link Authentication	Access Authentication	Data Encryption	Description
WEP	Open system	N/A	No encryption or WEP	Insecure policy
	Shared-key Authentication	N/A	WEP	Insecure policy
WPA/WPA2-802.1X	Open system	802.1X (EAP)	TKIP or CCMP	A more secure policy, applicable to large enterprises
WPA/WPA2-PSK	Open system	PSK	TKIP or CCMP	More secure policy, applicable to small- and medium-sized enterprises or household users

Link Authentication

- To ensure wireless link security, an AP needs to authenticate STAs that attempt to access the AP.
- IEEE 802.11 defines two authentication modes: open system authentication and shared key authentication.

Scanning
Link authentication
Association
Access authentication
DHCP
User authentication

Open System Authentication



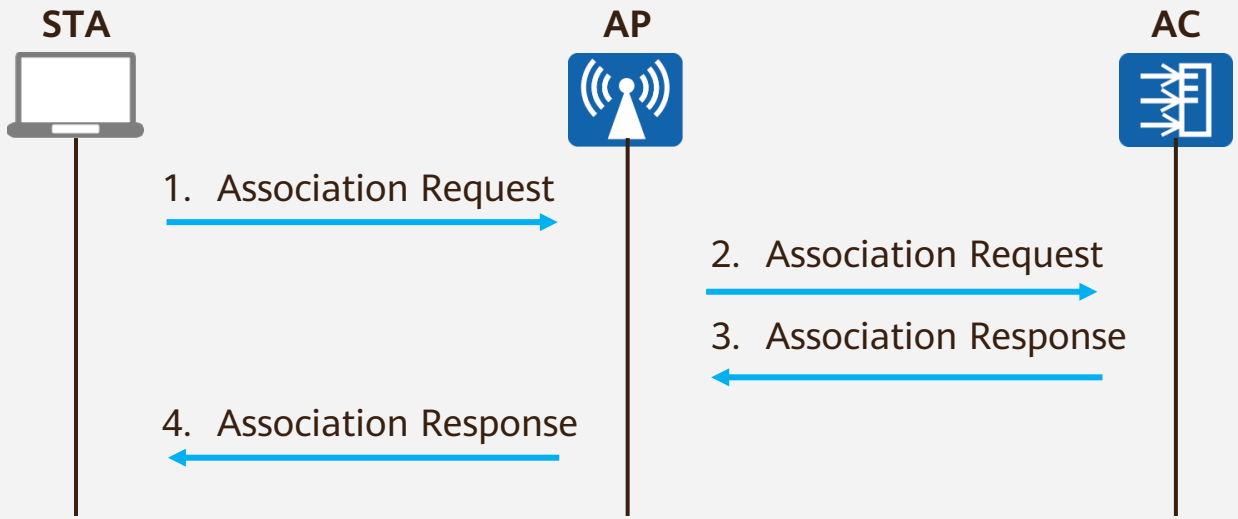
- Open system authentication requires no authentication, allowing any STA to be successfully authenticated.

Shared Key Authentication

- Shared key authentication requires that the STA and AP have the same shared key preconfigured. The AP checks whether a STA has the same shared key to determine the authentication result. If the STA has the same shared key as the AP, the STA is authenticated. Otherwise, STA authentication fails.

Association

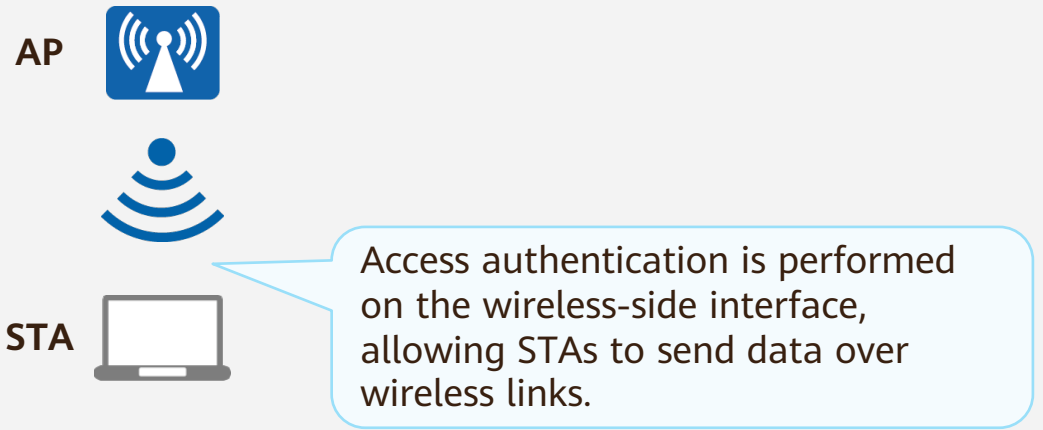
- After link authentication is complete, a STA initiates link service negotiation using Association packets.
- The STA association process is actually a link service negotiation process, during which the supported rate, channel, and the like are negotiated.



Access Authentication

- User access authentication differentiates users and controls access rights of users. Compared with link authentication, access authentication is more secure.
- Major access authentication modes include PSK authentication and 802.1X authentication.

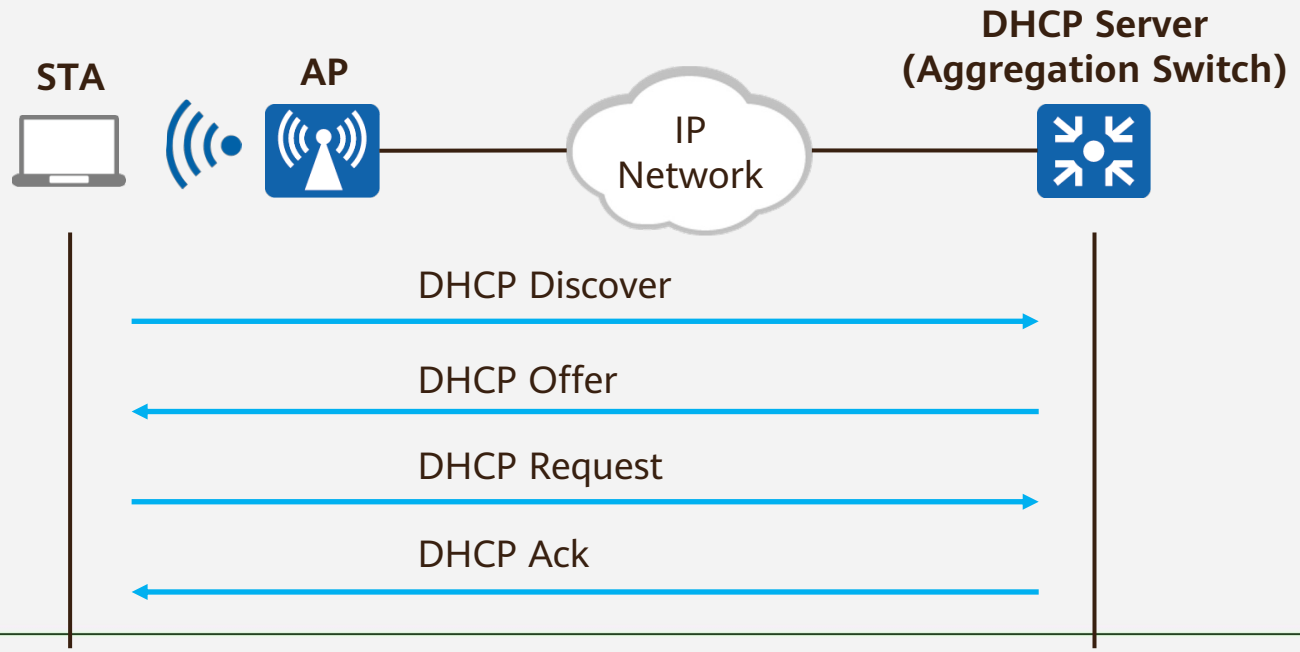
Scanning
Link authentication
Association
Access authentication
DHCP
User authentication



STA Address Allocation

- Scanning
- Link authentication
- Association
- Access authentication
- **DHCP**
- User authentication

- The prerequisite for APs and STAs to go online properly is that they have obtained IP addresses.
- If STAs obtain IP addresses through DHCP, the AC or aggregation switch can function as a DHCP server to assign IP addresses to the STAs. In most cases, the aggregation switch is used as the DHCP server.



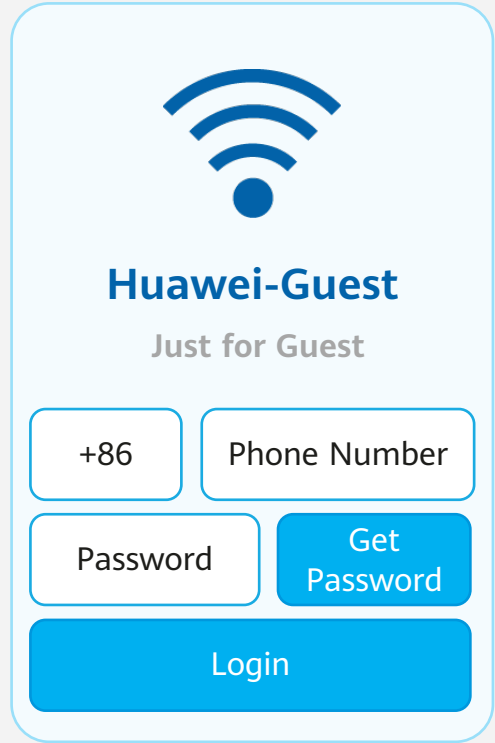
User Authentication

- User authentication is an end-to-end security architecture, supporting 802.1X, MAC address, and Portal authentication modes.

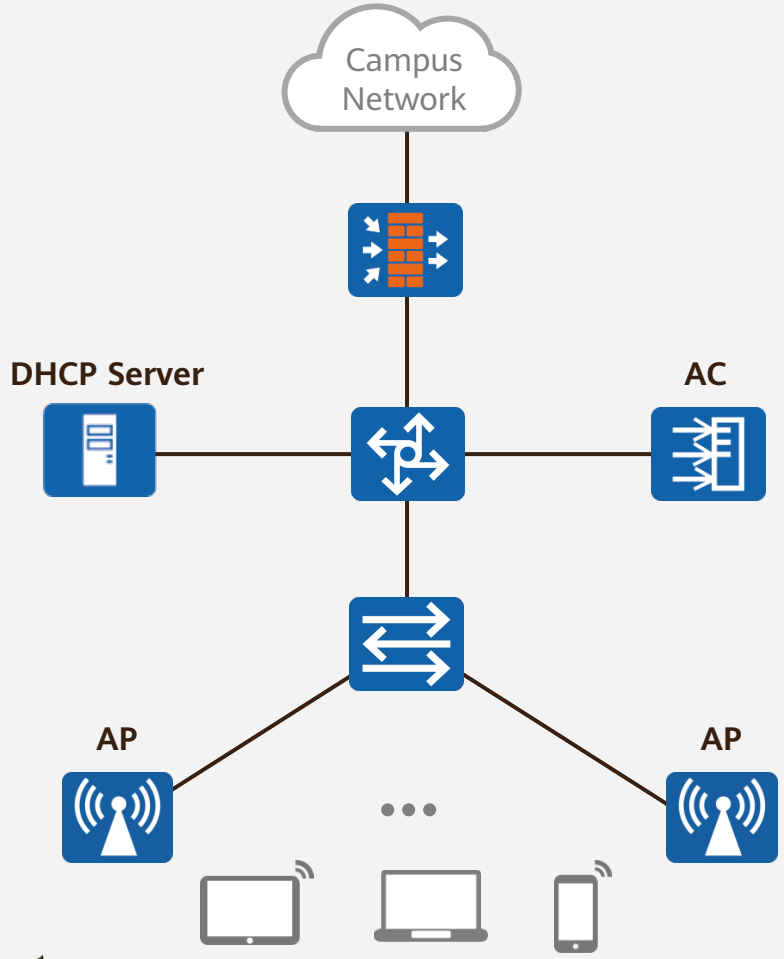
Scanning
Link authentication
Association
Access authentication
DHCP
User authentication

Portal Authentication

- Portal authentication is also known as web authentication. Portal authentication websites are referred to as web portals.
- To access the Internet, users must be authenticated on web portals. The users can access network resources only after successful authentication.



WLAN Working Process: Step 4



WLAN Working Process

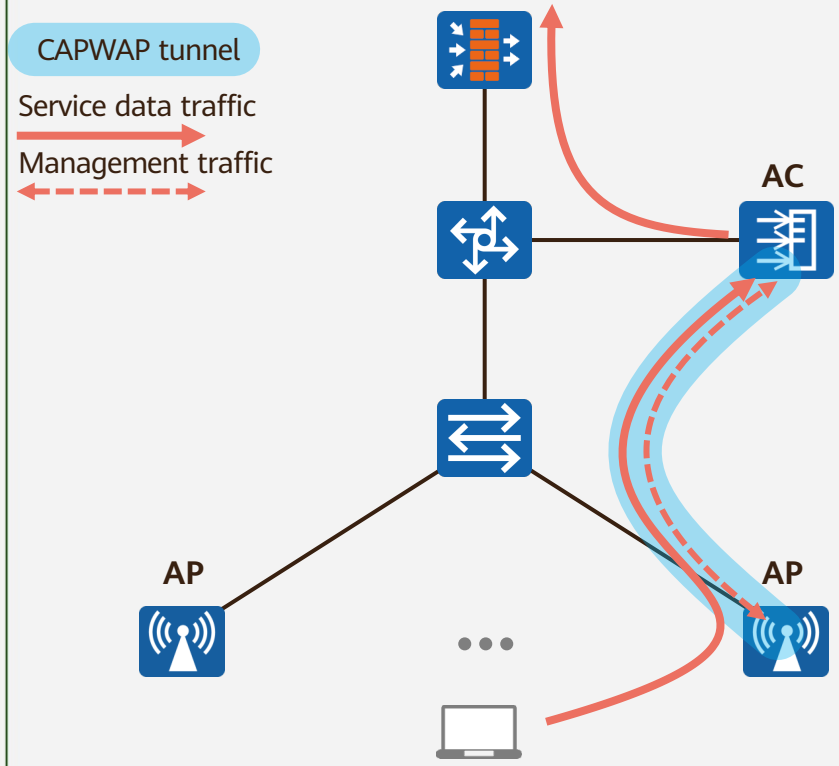
1. AP onboarding
2. WLAN service configuration delivery
3. STA access
4. WLAN service data forwarding

Control packets (management packets) and data packets are transmitted over CAPWAP tunnels.

- Control packets are forwarded through the CAPWAP control tunnel.
- User data packets can be forwarded in tunnel forwarding (centralized forwarding) or direct forwarding (local forwarding) mode.

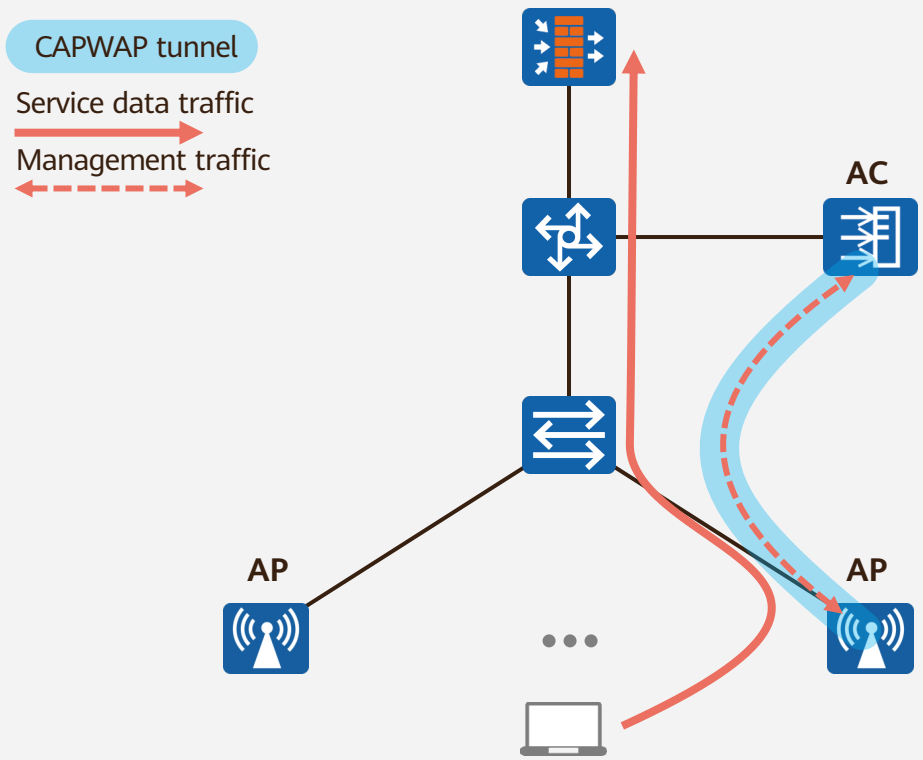
Data Forwarding Mode

Tunnel Forwarding



- In tunnel forwarding mode, APs encapsulate user data packets over a CAPWAP data tunnel and send them to an AC. The AC then forwards these packets to an upper-layer network.

Direct Forwarding



- In direct forwarding mode, an AP directly forwards user data packets to an upper-layer network without encapsulating them over a CAPWAP data tunnel.

Contents

Basic WLAN Configuration Commands: Configuring an AP to Go Online (1)

1. Configure the AC as a DHCP server and configure the Option 43 field.

[AC-ip-pool-pool1] **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address*

Configure the user-defined option that a DHCP server assigns to a DHCP client.

2. Create a regulatory domain profile and configure the country code.

[AC] **wlan**
[AC-wlan-view]

Enter the WLAN view.

[AC-wlan-view] **regulatory-domain-profile name** *profile-name*
[AC-wlan-regulate-domain-profile-name]

Create a regulatory domain profile and enter the regulatory domain profile view, or enter the view of an existing regulatory domain profile.

[AC-wlan-regulate-domain-profile-name] **country-code** *country-code*

Configure the country code.

Basic WLAN Configuration Commands: Configuring an AP to Go Online (2)

[AC-wlan-view] **ap-group name** *group-name*
[AC-wlan-ap-group-group-name]

Create an AP group and enter the AP group view, or enter the view of an existing AP group.

[AC-wlan-ap-group-group-name] **regulatory-domain-profile** *profile-name*

Bind the regulatory domain profile to an AP or AP group.

3. Configure a source interface or address.

[AC] **capwap source interface** { **loopback** *loopback-number* | **vlanif** *vlan-id* }

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

[AC] **capwap source ip-address** *ip-address*

Configure the source IP address on the AC.

Basic WLAN Configuration Commands: Configuring an AP to Go Online (3)

4. Add APs in offline mode.

```
[AC-wlan-view] ap auth-mode { mac-auth | sn-auth }
```

Set the AP authentication mode to MAC address or SN authentication. By default, MAC address authentication is used.

```
[AC-wlan-view] ap-id ap-id [ [ type-id type-id | ap-type ap-type ] { ap-mac ap-mac | ap-sn ap-sn | ap-mac ap-mac ap-sn ap-sn } ]
[AC-wlan-ap-ap-id] ap-name ap-name
```

Manually add an AP in offline mode or enter the AP view, and configure the name of a single AP.

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] ap-group ap-group
```

Add the AP to an AP group.

5. Verify the configuration.

```
[AC] display ap { all | ap-group ap-group }}
```

Check AP information.

Basic WLAN Configuration Commands: Configuring Radios (1)

1. Enter the radio view.

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] radio radio-id
[AC-wlan-radio-0]
```

2. Configure the working bandwidth and channel for a radio.

```
[AC-wlan-radio-0/0] channel { 20mhz | 40mhz-minus | 40mhz-plus | 80mhz | 160mhz } channel
Warning: This action may cause service interruption. Continue?[Y/N]y
```

```
[AC-wlan-radio-0/0] channel 80+80mhz channel1 channel2
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Configure the working bandwidth and channel for all APs in an AP group or for a specified radio of a single AP.

3. Configure the antenna gain.

```
[AC-wlan-radio-0/0] antenna-gain antenna-gain
```

Configure the antenna gain for all APs in an AP group or for a specified radio of a single AP.

Basic WLAN Configuration Commands: Configuring Radios (2)

4. Configure the transmit power for a radio.

```
[AC-wlan-radio-0/0] eirp eirp
```

Configure the transmit power for all APs in an AP group or for a specified radio of a single AP.

5. Configure the radio coverage distance.

```
[AC-wlan-radio-0/0] coverage distance distance
```

Configure the radio coverage distance for all APs in an AP group or for a specified radio of a single AP.

6. Configure the operating frequency for a radio.

```
[AC-wlan-radio-0/0] frequency { 2.4g | 5g }
```

Basic WLAN Configuration Commands: Configuring Radios (3)

7. Create a radio profile.

[AC-wlan-view] **radio-2g-profile name** *profile-name*

Create a 2G radio profile and enter the 2G radio profile view, or enter the view of an existing 2G radio profile.

8. Bind the radio profile.

[AC-wlan-view] **ap-group name** *group-name*
[AC-wlan-ap-group-group-name] **radio-2g-profile** *profile-name* **radio** { *radio-id* | **all** }

Bind the specified 2G radio profile to the 2G radio in the AP group.

Basic WLAN Configuration Commands: Configuring VAPs (1)

1. Create a VAP profile.

```
[AC-wlan-view] vap-profile name profile-name
[AC-wlan-vap-prof-profile-name]
```

Create a VAP profile and enter the VAP profile view, or enter the view of an existing VAP profile.

2. Configure the data forwarding mode.

```
[AC-wlan-vap-prof-profile-name] forward-mode { direct-forward | tunnel }
```

Set the data forwarding mode in the VAP profile to direct or tunnel.

3. Configure service VLANs.

```
[AC-wlan-vap-prof-profile-name] service-vlan { vlan-id vlan-id | vlan-pool pool-name }
```

Configure service VLANs configured for the VAP.

Basic WLAN Configuration Commands: Configuring VAPs (2)

4. Configure a security profile.

[AC-wlan-view] **security-profile name** *profile-name*
[AC-wlan-sec-prof-profile-name]

Create a security profile and enter the security profile view.

By default, security profiles **default, default-wds**, and **default-mesh** are available in the system.

[AC-wlan-view] **vap-profile name** *profile-name*
[AC-wlan-vap-prof-profile-name] **security-profile** *profile-name*

Bind the security profile to the VAP profile.

Basic WLAN Configuration Commands: Configuring VAPs (3)

5. Configure an SSID profile.

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

Create an SSID profile and enter the SSID profile view, or enter the view of an existing SSID profile.

By default, the system provides the SSID profile **default**.

```
[AC-wlan-ssid-prof-profile-name] ssid ssid
```

Configure an SSID for the SSID profile.

By default, the SSID **HUAWEI-WLAN** is configured in an SSID profile.

```
[AC-wlan-view] vap-profile name profile-name
[AC-wlan-vap-prof-profile-name] ssid-profile profile-name
```

Bind the SSID profile to the VAP profile.

Basic WLAN Configuration Commands: Configuring VAPs (4)

6. Bind the VAP profile.

[AC-wlan-view] **ap-group name** *group-name*
[AC-wlan-ap-group-group-name] **vap-profile** *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** } [**service-vlan** { **vlan-id** *vlan-id* | **vlan-pool** *pool-name* }]

Bind the specified VAP profile to radios in an AP group.

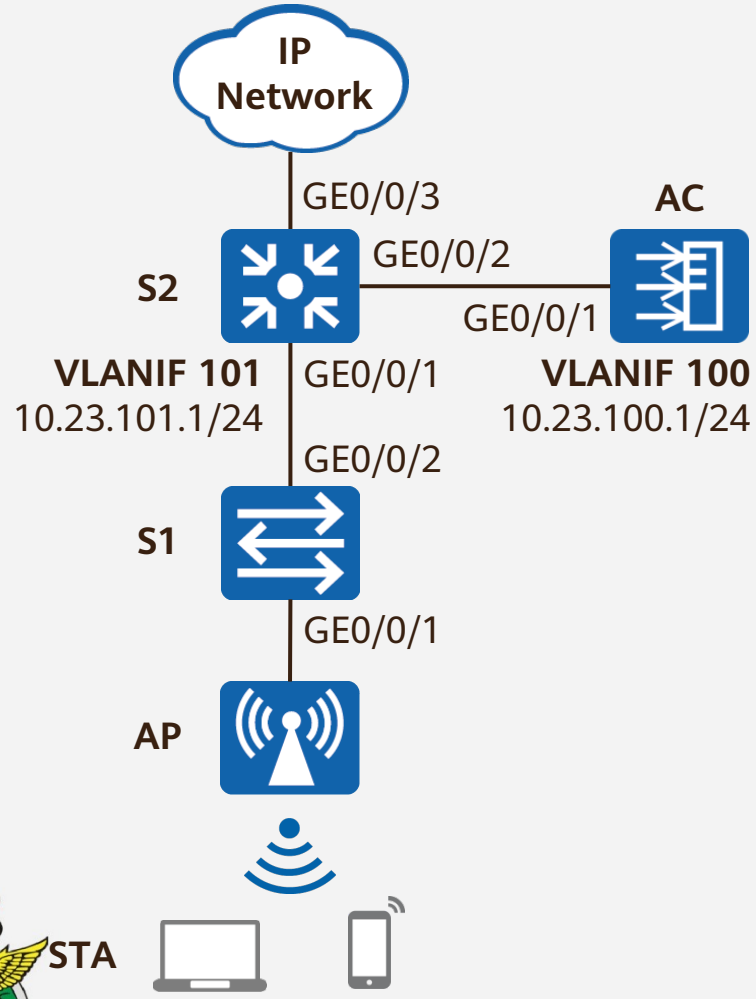
7. Check VAP information.

[AC] **display vap** { **ap-group** *ap-group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }
[**ssid** *ssid*]

[AC] **display vap** { **all** | **ssid** *ssid* }

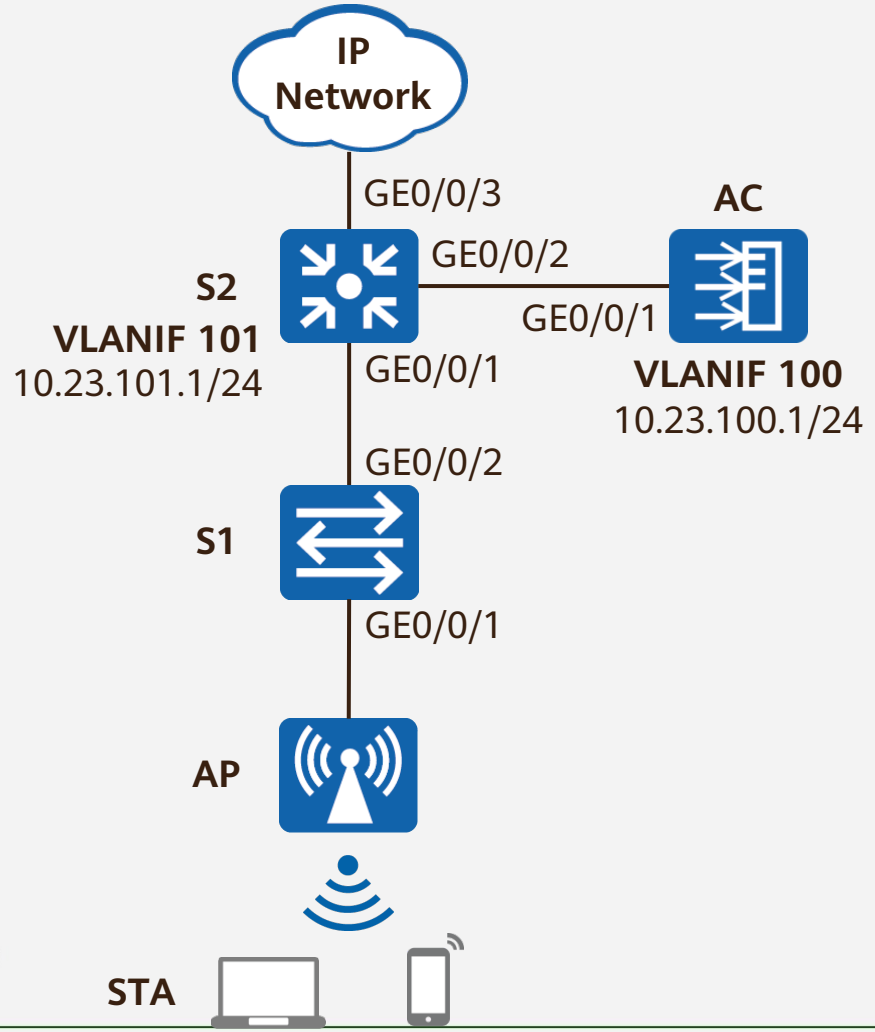
Display information about service VAPs.

Example for Configuring Layer 2 Tunnel Forwarding in Off-Path Mode



Data	Configuration
Management VLAN for APs	VLAN 100
Service VLAN for STAs	VLAN 101
DHCP server	The AC functions as a DHCP server to assign IP addresses to APs. The aggregation switch S2 functions as a DHCP server to assign IP addresses to STAs. The default gateway address of STAs is 10.23.101.1.
IP address pool for APs	10.23.100.2–10.23.100.254/24
IP address pool for STAs	10.23.101.2–10.23.101.254/24
IP address of the AC's source interface	VLANIF 100: 10.23.100.1/24
AP group	Name: ap-group1 Referenced profiles: VAP profile **wlan-net** and regulatory domain profile
Regulatory domain profile	Name: default Country code: CN
SSID profile	Name: wlan-net SSID name: wlan-net
Security profile	Name: wlan-net Security policy: WPA-WPA2+PSK+AES Password: a1234567
VAP profile	Name: wlan-net Forwarding mode: tunnel forwarding Service VLAN: VLAN 101 Referenced profiles: SSID profile **wlan-net** and security profile **wlan-net**

Configuring Network Connectivity



1. Create VLANs and interfaces on S1, S2, and AC.
2. Configure DHCP servers to assign IP addresses to APs and STAs.

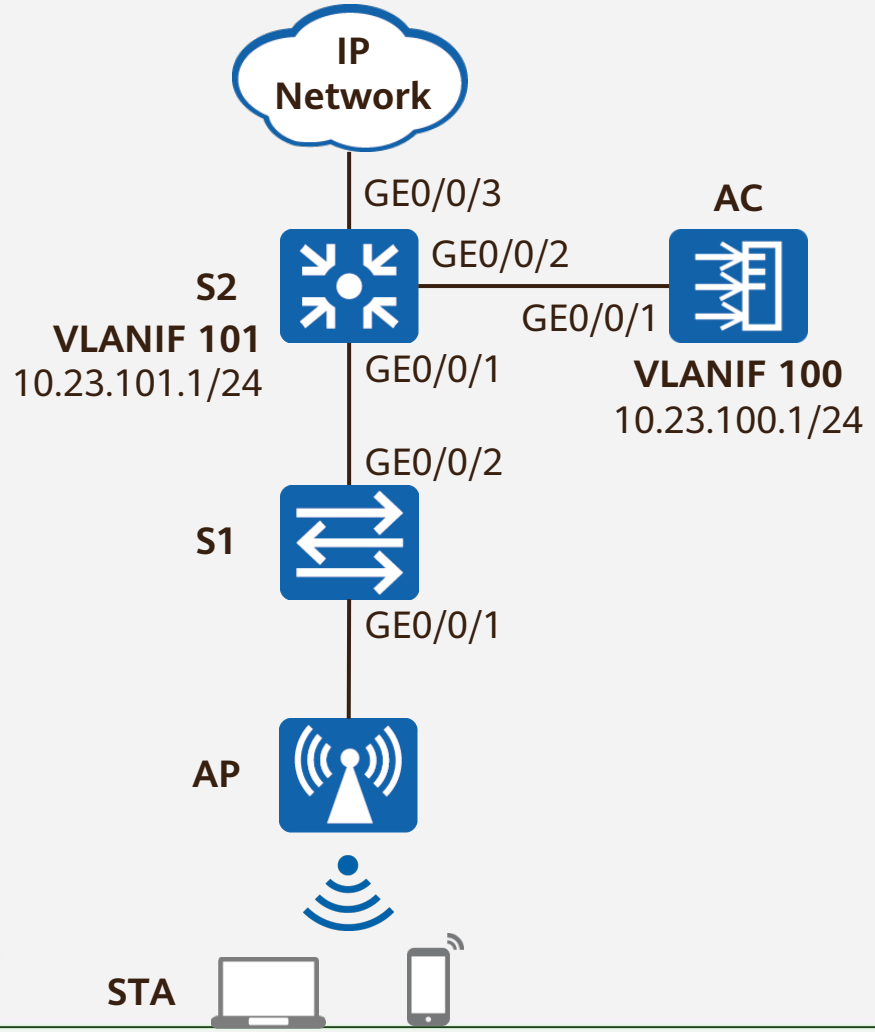
Configure VLANIF 100 on the AC to assign IP address to APs.

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
```

Configure VLANIF 101 on S2 to assign IP addresses to STAs and specify 10.23.101.1 as the default gateway address of the STAs.

```
[S2] dhcp enable
[S2] interface vlanif 101
[S2-Vlanif101] ip address 10.23.101.1 24
[S2-Vlanif101] dhcp select interface
```

Configuring APs to Go Online (1)



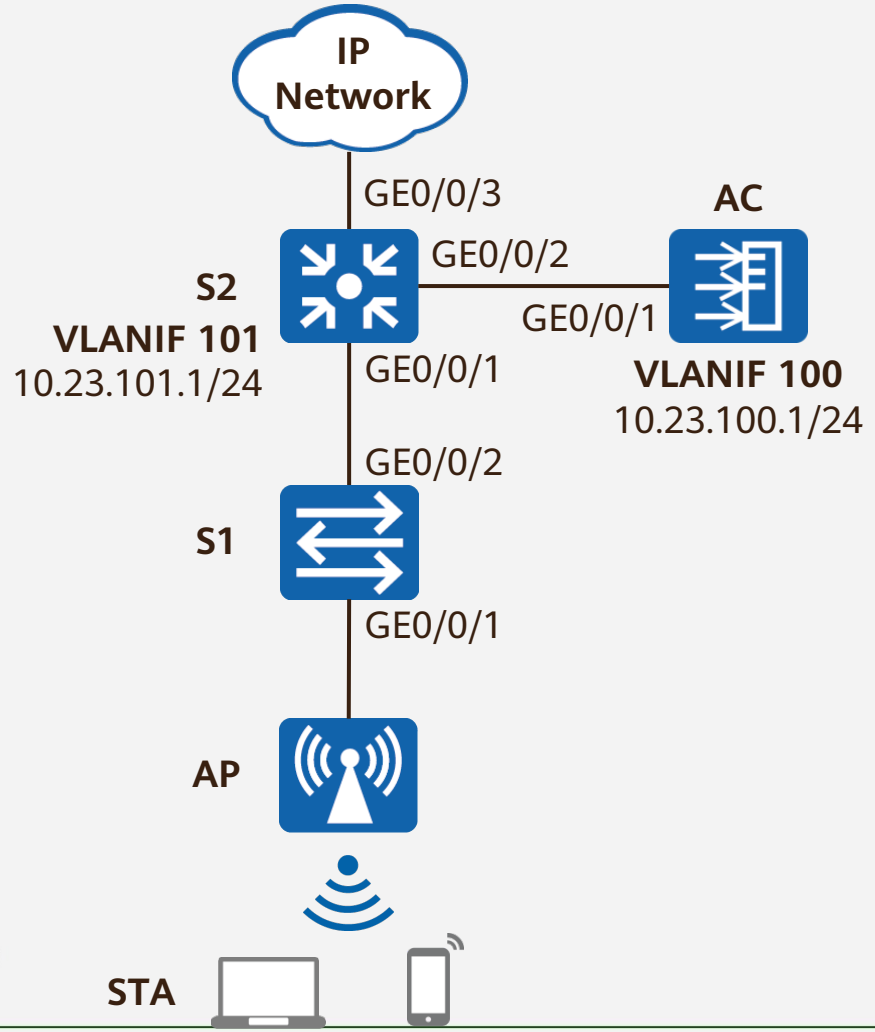
1. Create an AP group.

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

2. Create a regulatory domain profile and configure the country code.

```
AC-wlan-view] regulatory-domain-profile name default
[AC-wlan-regulate-domain-default] country-code cn
[AC-wlan-regulate-domain-default] quit
[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. Continu
e?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

Configuring APs to Go Online (2)



3. Configure the AC's source interface.

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

4. Import an AP in offline mode on the AC.

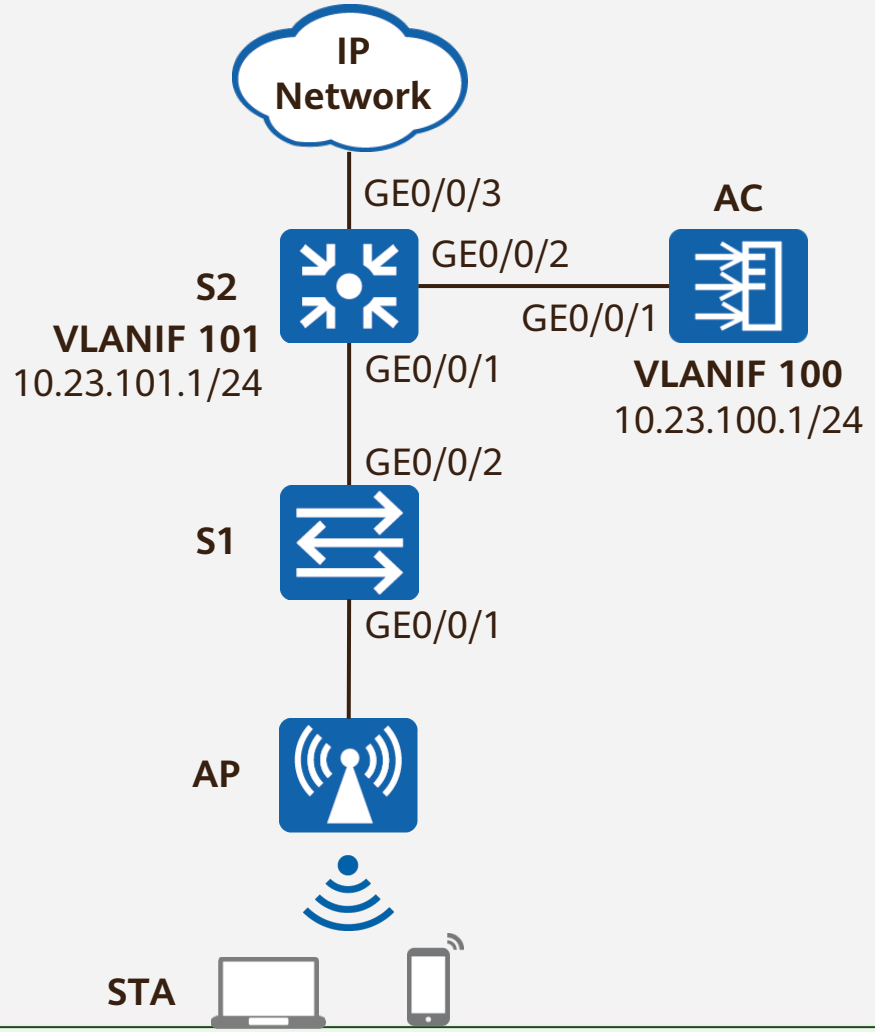
```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 60de-4476-e360
[AC-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
```

Verifying the AP Onboarding Configuration

- After the AP is powered on, run the **display ap all** command to check the AP state. If the **State** field displays **nor**, the AP has gone online.

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
Extra information:
P  : insufficient power supply
------------------------------------------------------------------------------------------------------------------
ID   MAC                Name       Group      IP              Type         State STA Uptime      ExtraInfo
------------------------------------------------------------------------------------------------------------------
0    60de-4476-e360     area_1     ap-group1  10.23.100.254   AP5030DN     nor   0   10S         -
------------------------------------------------------------------------------------------------------------------
Total: 1
```

Configuring WLAN Service Parameters (1)



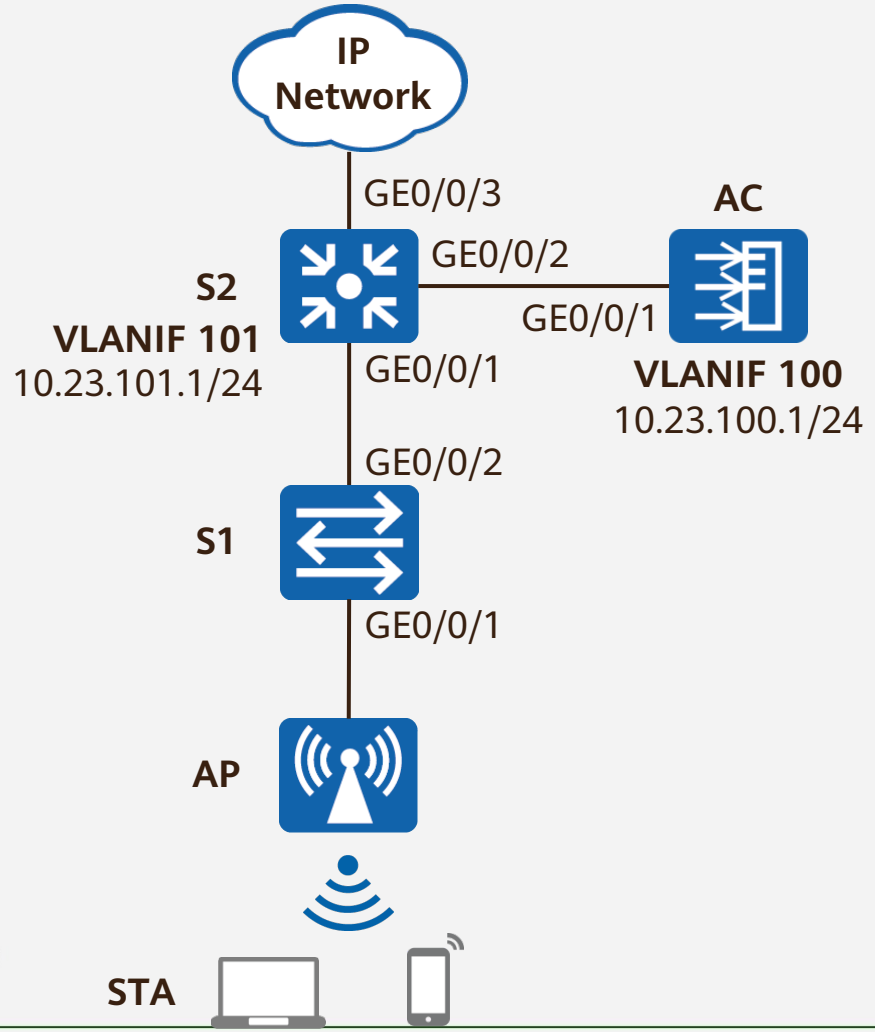
1. Create security profile **wlan-net** and configure a security policy.

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

2. Create SSID profile **wlan-net** and set the SSID name to **wlan-net**.

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

Configuring WLAN Service Parameters (2)



3. Create VAP profile **wlan-net**, set the data forwarding mode and service VLAN, and bind the security profile and SSID profile to the VAP profile.

```
[AC-wlan-view] vap-profile name wlan-net
[AC-wlan-vap-prof-wlan-net] forward-mode tunnel
[AC-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-net] security-profile wlan-net
[AC-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[AC-wlan-vap-prof-wlan-net] quit
```

4. Bind the VAP profile to the AP group and apply configurations in VAP profile **wlan-net** to radio 0 and radio 1 of the APs in the AP group.

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
```

Checking VAP Profile Information

- The AC automatically delivers WLAN service configuration to the AP. After the service configuration is complete, run the **display vap ssid wlan-net** command. If **Status** in the command output is displayed as **ON**, the VAPs have been successfully created on AP radios.

```
[AC-wlan-view] display vap ssid wlan-net
WID : WLAN ID
------------------------------------------------------------------------------------------------
AP ID      AP name    RfID  WID  BSSID           Status  Auth type        STA  SSID
------------------------------------------------------------------------------------------------
0          area_1     0     1    60DE-4476-E360  ON      WPA/WPA2-PSK     0    wlan-net
0          area_1     1     1    60DE-4476-E370  ON      WPA/WPA2-PSK     0    wlan-net
------------------------------------------------------------------------------------------------
Total: 2
```

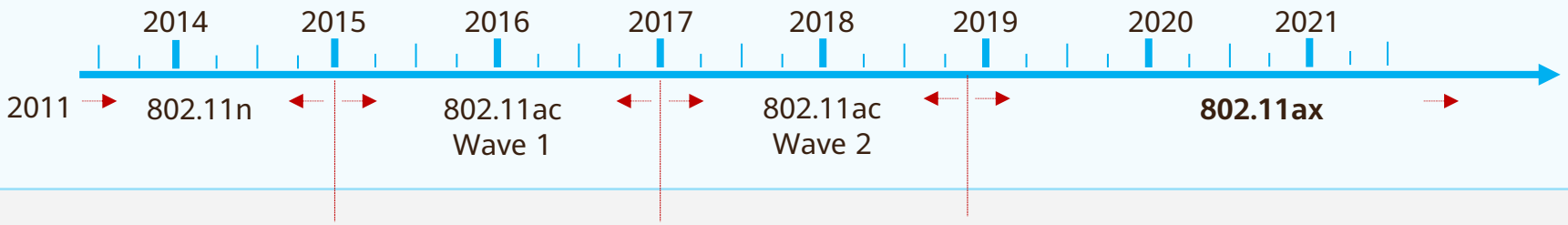
Contents

Huawei WLAN Solutions Meet Future Wireless Network Construction Requirements

All-scenario	• Use scenario-based customized solutions for complex and diversified application scenarios • Complete WLAN deployment and management solutions for campus networks and branch networks
High bandwidth	• 802.11ac Wave 2 protocol, dual-5G radio coverage, and up to 3.46 Gbps wireless access bandwidth • Huawei is a key contributor to the next-generation 802.11ax standard (Wi-Fi 6) with a single 5 GHz radio rate of up to 9.6 Gbps. • Roaming and multiple wireless QoS protocols such as Wi-Fi multimedia (WMM) to ensure QoS
High security	• Mainstream authentication and encryption modes, such as WPA, WPA2, WPA3, and WAPI • Wireless intrusion detection • Portal and 802.1X authentication, protecting intranet security
Easy deployment	• APs support plug-and-play, automatic upgrade, automatic channel selection, dynamic rate and power adjustment, and load balancing. • IoT APs and APs with built-in high-density antennas, simplifying installation and enabling fast deployment • APs support cloud management and can work in dual-stack mode to smoothly switch between the cloud and local management modes.

Dual Drivers (Technology Advances + Application Development) Promote the Arrival of the Wi-Fi 6 Era

Technology



Wi-Fi standards are upgraded **every four to five years**.

Wi-Fi 4	Wi-Fi 5	Wi-Fi 6

October 2018
New Wi-Fi naming convention released by the WFA

Application

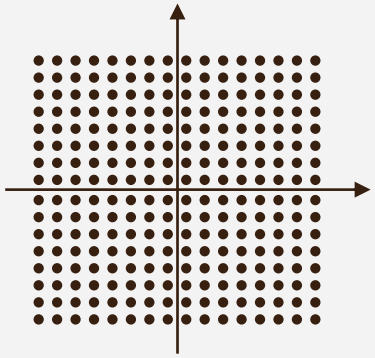
Bandwidth per user:
2 to 4 Mbps
Latency < 50 ms

Bandwidth per user: 4 to 12 Mbps
Latency < 30 ms

Bandwidth per user > 50 Mbps
Latency < 10 ms

Wi-Fi 6 Vs. Wi-Fi 5

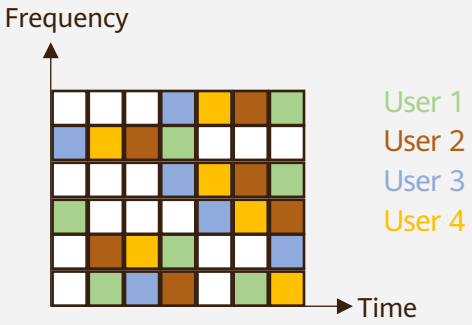
High Bandwidth



1024-QAM
8x8 MU-MIMO

- Rate of up to **9.6** Gbps
- Bandwidth increased by **4** times

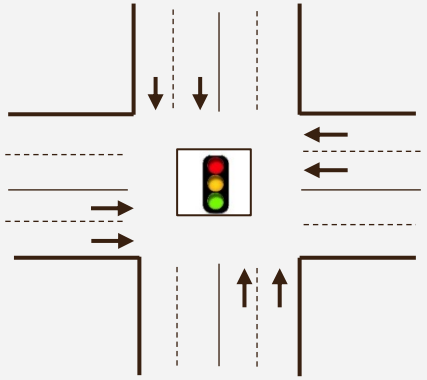
High Concurrency Rate



UL/DL OFDMA
UL/DL MU-MIMO

- Access of **1024** STAs per AP
- Number of concurrent users increased by **4** times

Low Latency



OFDMA
Spatial Reuse

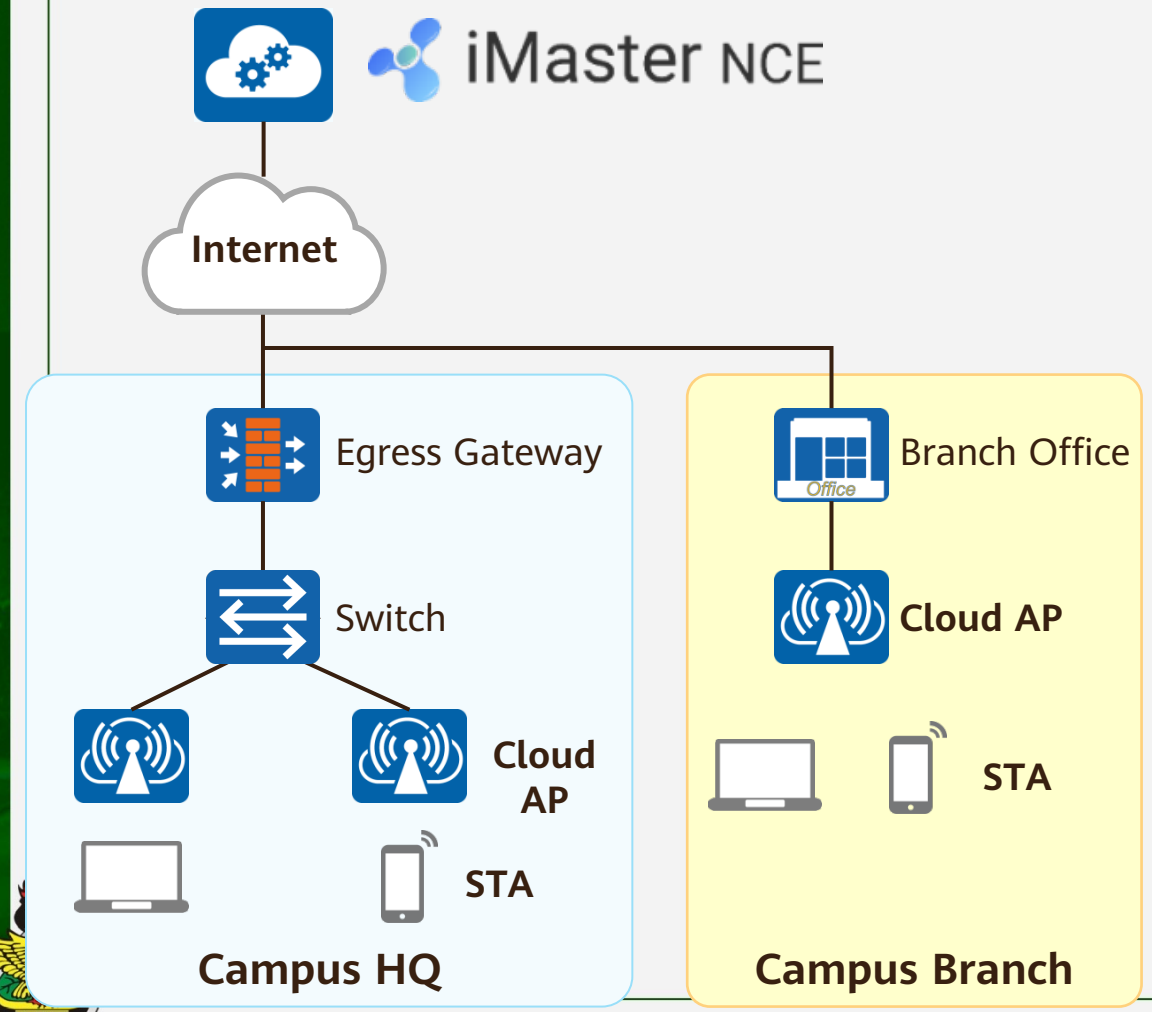
- Service latency reduced to **20 ms**
- Average latency reduced by **30%**

Low Power Consumption

TWT
20 MHz-Only

- Target wakeup time (TWT) mechanism
- STA power consumption reduced by **30%**

Next-Generation Campus Network: Intent-Driven Campus (Small- and Medium-Sized)



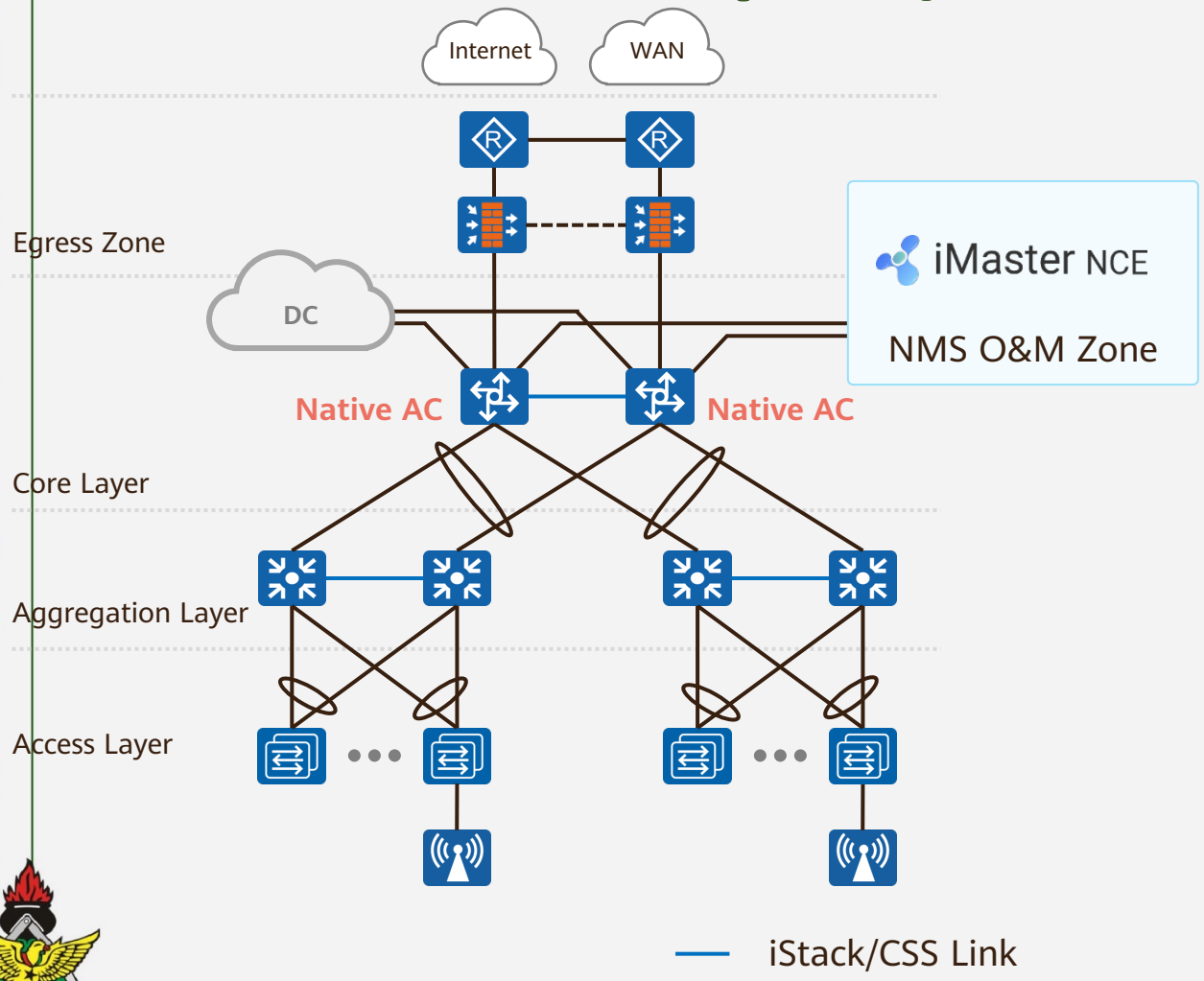
Basic Concepts

- The cloud management platform allows centralized management and maintenance of devices at any place, greatly reducing network deployment and O&M costs.
- Applicable scope: small- and medium-sized enterprises

Advantages (Compared with the AC + Fit AP Architecture)

- Plug-and-play and automatic deployment reduce network deployment costs.
- All network elements (NEs) are monitored and managed on the cloud management platform in a unified manner.
- Cloud solutions usually provide various tools on the cloud, reducing costs.

Next-Generation Campus Network: Intent-Driven Campus (Medium- and Large-Sized)



Architecture Characteristics

- iMaster NCE manages and configures APs in a unified manner and provides various functions. By further integrating with wired networks and leveraging Big Data and AI technologies, this architecture implements simplified, intelligent, and secure campus networks.
- Applicable scope: medium- and large-sized enterprises

Quiz

1. What are the advantages and disadvantages of in-path and off-path networking modes?
2. (Multiple) Which of the following methods are supported by Fit APs to discover an AC?( )
   A. Static discovery
   B. Dynamic discovery through DHCP
   C. Dynamic discovery through FTP
   D. Dynamic discovery through DNS

Summary

- WLAN technology allows users to easily access a wireless network and freely move around within the coverage of the wireless network, eliminating the constraints of wired networks.
- In this course, we have learned WLAN technologies on enterprise networks, including the basic concepts, fundamentals, network architectures, configuration implementation, and development trend of WLAN technologies.

THANK YOU

Kwame Nkrumah University of Science and Technology, Kumasi | Leaders In Change

Visit us at www.knust.edu.gh

uro@knust.edu.gh | Follow KNUST on: