# WLAN Overview

# 1 WLAN Overview

## 1.1 WLAN Overview

### 1.1.1 Basics of WLAN

- Constructed using wireless technologies like Wi-Fi, infrared, Bluetooth, ZigBee.

> - **Infrared**: A wireless communication technology that uses infrared(light below red) light waves to transmit data over short distances, typically used in remote controls for TVs and other devices.
> - **ZigBee**: A low-power, low-data-rate wireless communication protocol designed for creating personal area networks with small, low-power digital radios, often used in home automation and IoT devices.

- **Operates at high frequencies:** 2.4 GHz or 5 GHz.

> 2.4 GHz and 5 GHz are frequency bands used in wireless communications because they are internationally designated for

> unlicensed use, allowing for widespread compatibility with many devices without the need for individual licenses.

- Provides mobility within wireless network coverage.

### 1.1.2 Components of a WLAN

- **Router**: Connects networks and directs data traffic.
- **Switch**: Filters and forwards data to devices within the network.
- **Access Point (AP)**: Extends wireless coverage and connects devices to the network.

### 1.1.3 Classification of Wireless Networks

1. `WPAN` : Personal area network (Bluetooth, ZigBee).
2. `WLAN` : Local area network (Wi-Fi).
3. `WMAN` : Metropolitan area network (WiMAX).
4. `WWAN` : Wide area network (GSM, LTE).

### 1.1.4 Advantages of WLAN

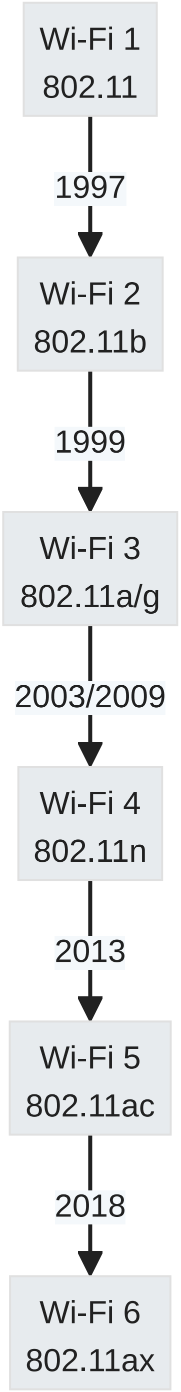
> High mobility and flexible deployment make WLANs suitable for environments with moving users or where cable deployment is difficult.

### 1.1.5 IEEE 802 Standards & Wi-Fi Generations

### 1.1.5.1 IEEE 802.11 Standards

- Defines standards for WLANs by IEEE as (IEEE 802.11).
- Located on the lower two layers of TCP/IP model: Data link layer & Physical layer.

### 1.1.5.2 Wi-Fi Generations



### 1.1.5.2.1 Frequency Bands & Throughput by Standard

| Frequency Band | Throughput | Standard | Wi-Fi | Released In |
|---|---|---|---|---|
| 2.4 GHz | 2 Mbit/s | 802.11 | Wi-Fi 1 | 1997 |
| 2.4 GHz | 11 Mbit/s | 802.11b | Wi-Fi 2 | 1999 |

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

## 1.1.6 Evolution of Wireless in Office Scenarios

### 1.1.6.1 Mobile Office Phases

#### 1.1.6.1.1 Phase 1: Initial Mobile Office Era

> Wireless networks were Add-ons to wired networks with limited requirements on security and capacity.

#### 1.1.6.1.2 Phase 2: Wireless Office Era

> Integration of wired and wireless networks became essential; higher bandwidth required due to services like video and voice.

#### 1.1.6.1.3 Phase 3: All-Wireless Office Era

> Preference for wireless over wired networks; offices covered entirely by Wi-Fi; emergence of high-bandwidth services on wireless networks (e.g., telepresence conference, VR/AR).

# 1.2 Basic Concepts of WLAN

## 1.2.1 Enterprise WLAN Products

### 1.2.1.1 Access Point (AP)

- **Modes:**
  - **Fat AP**: Standalone, simple functions, cost-effective.

> usually, used in wireless router for home network

- **Fit AP**: Managed by AC, Multiple uses, requires skilled persons.
- **Cloud AP**: Managed by cloud platform, supports plug-and-play.

### 1.2.1.2 Access Controller (AC)

- Deployed in network aggregation layer.
- Manages Fit APs providing large capacity and performance.

### 1.2.1.3 PoE Switch

- Supplies power over Ethernet to devices like APs.

## 1.2.2 Basic WLAN Networking Architecture

### 1.2.2.1 Fat AP Architecture

Independently working Fat APs with limited scalability due to management difficulties.

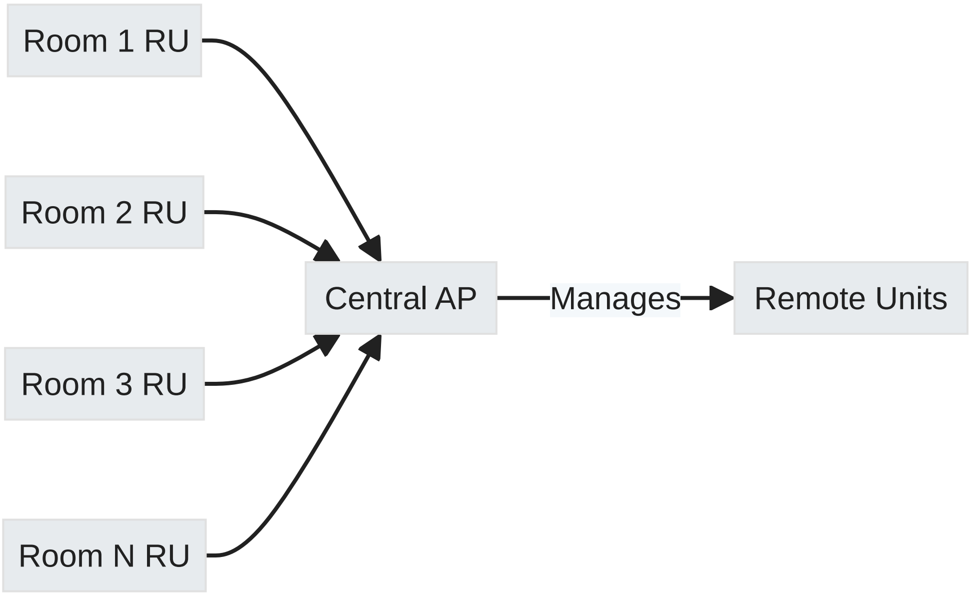
### 1.2.2.2 AC + Fit AP Architecture

Centralized control through an AC managing multiple Fit APs; scalable for larger enterprises.

**Communication Protocols**

- **AP uses**
  - Wired Side
    - Ethernet Protocols
  - Wireless Side
    - 802.11 Standards

## 1.2.3 Agile Distributed Architecture



- Divides an AP into a **central** unit managing **multiple** remote **units**.

## 1.2.4 CAPWAP Tunnels

| Function | Description |
|---|---|
| Management | Allows the AC to manage and control the APs. |
| Data Transfer | Facilitates data exchange between STAs and the network through CAPWAP tunnels. |

> **CAPWAP** is a system that helps manage wireless networks by securely linking each access point to a main controller, making it easier to handle data sent by devices like phones and laptops.

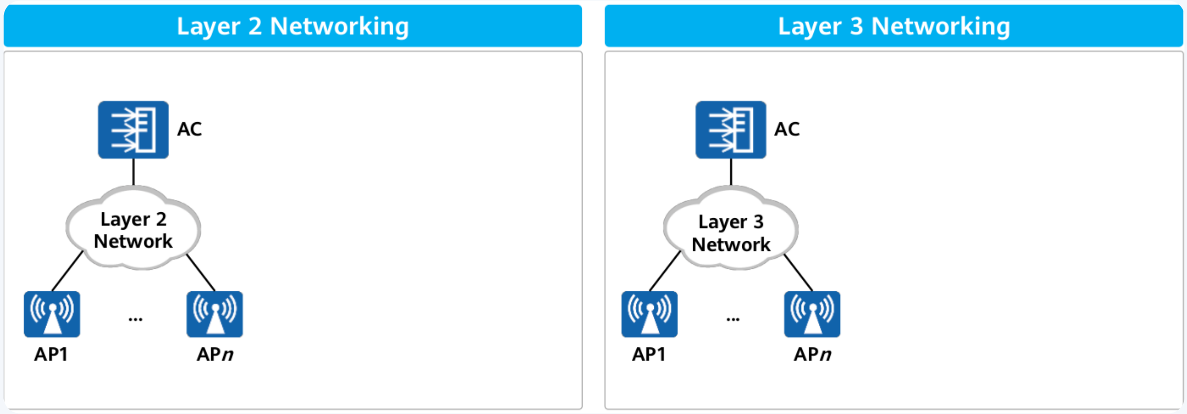
> **A station (STA)** in the context of 802.11 wireless networking refers to any device, like a laptop or smartphone, that has the capability to connect to a Wi-Fi

**CAPWAP Port**

- CAPWAP is an application-layer protocol based on **UDP** transmission.
- UDP port 5246 for transmitting control packets

- UDP port 5247 for transmitting data packets

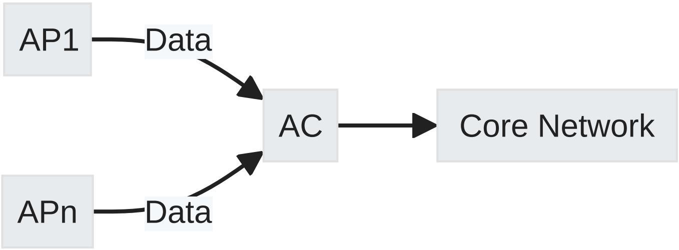
## 1.2.5 Networking Modes



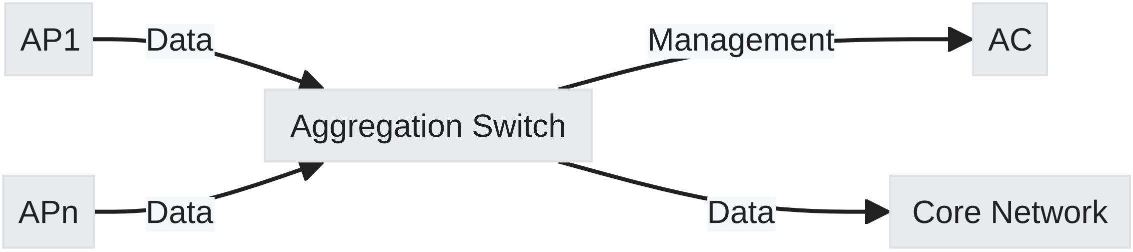
- Layer 2 networking: Access points (APs) connect directly or through a simple network to a controller, making setup fast and suitable for basic or short-term networks.
- Layer 3 networking: Access points (APs) connect through a more complex network to a controller, which is better for managing many APs over larger, more intricate networks.

## 1.2.6 AC Connection Mode

**In-Path Connection Mode:**
In in-path mode, the Access Controller (AC) is placed directly in the line of network traffic, meaning all user data flows through the AC.

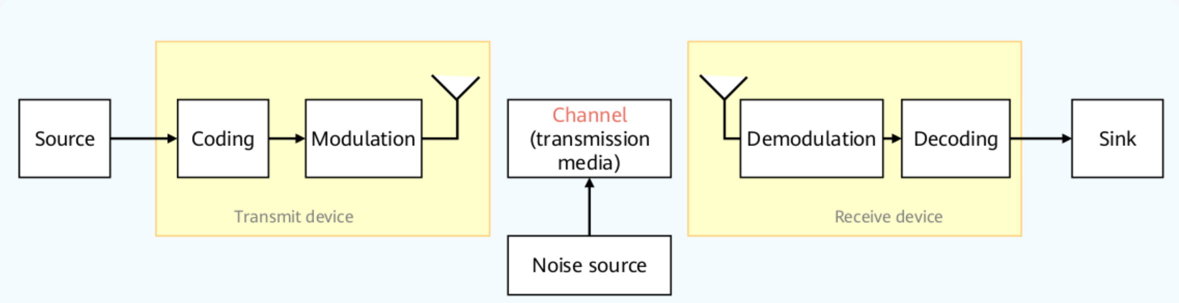


**Off-Path Connection Mode:**
In off-path mode, the Access Controller (AC) manages the network but does not handle data traffic; instead, data bypasses the AC and goes straight to the core network.



## 1.2.7 Wireless Communications System

### 1.2.7.1 Coding & Modulation Process:



Wireless Communications System

Convert raw information into digital signals (source coding), then into radio waves through channel coding and modulation for transmission over air interfaces.

### 1.2.7.2 Radio Wave Spectrum Utilization

- 2.4 GHz frequency band (2.4–2.4835 GHz)

> - 5 GHz frequency band (5.15–5.35 GHz, 5.725–5.85 GHz)

**For WLAN:**

- **2.4 GHz Frequency Band:** Channels overlap; used for protocols like IEEE 802.11b/g/n/ax.
- **5 GHz Frequency Band:** Richer spectrum; supports wider channels; used for IEEE protocols including ac/ax.

> Radio channels are specific frequencies used to send information. To avoid interference, these frequencies are carefully divided. The 2.4 GHz band has 14 channels that can be close together and interfere (like channels 1 and 2) or far apart and not interfere (like channels 1 and 6). The 5 GHz band offers more options, including wider channels for more data.

## 1.2.8 BSS/SSID/BSSID Concepts

- **BSS (Basic Service Set):** A network area covered by a single access point (AP) where devices can connect and communicate wirelessly.
- **SSID (Service Set Identifier):** The name of a wireless network that helps users identify and connect to different WLANs.
- **BSSID (Basic Service Set Identifier):** The unique MAC address of an access point that distinguishes one WLAN from another within the same area.
- **ESS (Extended Service Set):** is a network of multiple Wi-Fi access points with the same SSID (network name) that allows devices to move around freely without losing their connection.

> Each BSS is identified by BSSID (MAC of the respective AP) while SSID is a human-readable identifier of a wireless network spanning across one or more BSSs forming an ESS for seamless roaming capability.

### 1.2.9 Virtual Access Points (VAP)

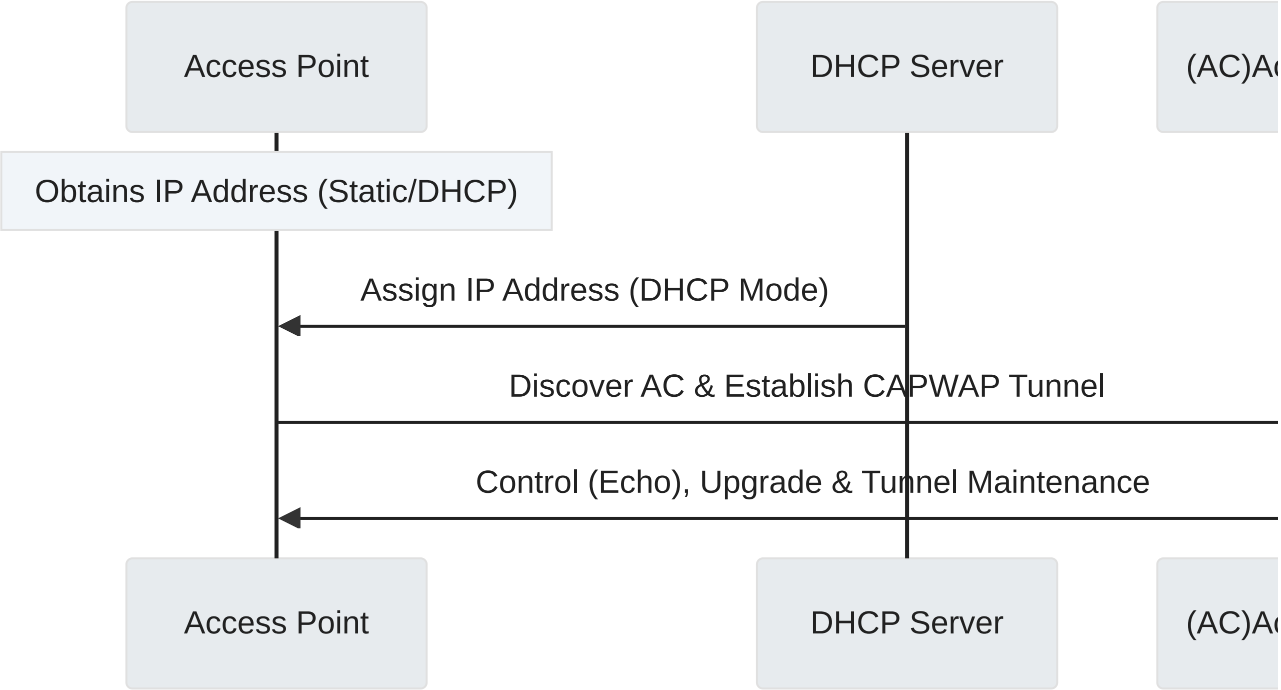
A single physical AP can be virtualized into multiple VAPs each serving different user groups with unique SSIDs but sharing hardware resources of the base physical unit.

## 1.3 WLAN Fundamentals

### 1.3.1 WLAN Working Process Overview

#### 1.3.1.1 1. AP Onboarding

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


Access Point
DHCP Server
(AC)Ac
Obtains IP Address (Static/DHCP)
Assign IP Address (DHCP Mode)
Discover AC & Establish CAPWAP Tunnel
Control (Echo), Upgrade & Tunnel Maintenance
Access Point
DHCP Server
(AC)Ac

#### 1.3.1.1.1 Steps:

1. Obtain IP Address.

> Access Points (APs) must first obtain an **IP** address, either **statically** or via **DHCP** from a **server**, **controller**, or **network device**. Once assigned an IP, the AP can communicate with the network controller to facilitate wireless connectivity and data management.

2. Discover AC & CAPWAP Tunnel Establishment.

**Discover AC & CAPWAP**

1. **AP Discovery**: APs locate an AC by either cycling through pre-configured AC IPs (**Static**) or using network services like **DHCP**, **DNS**, or **broadcasts** to find one (Dynamic).
2. **CAPWAP Tunnel Establishment**: APs and ACs establish a Data tunnel for device traffic and a Control tunnel for management communication via the CAPWAP protocol
   - **Data tunnel:** transmits service data packets from APs to the AC Datagram Transport Layer AP access control Security (DTLS) encryption can be enabled over the data tunnel to ensure security.
   - **Control tunnel:** transmits control packets between the AC and APs. DTLS encryption can be enabled over the control tunnel to ensure security

**DHCP Mode Steps**:

- DHCP Discover
- DHCP Offer (option 43)
- DHCP Request
- DHCP Ack (option 43)

In the absence of advanced DHCP or DNS services, the AP broadcasts discovery requests within the Layer 2 network to find any ACs ready to respond.

3. AP Access Control (Authentication).

**Authentication**

- APs request to join an AC by sending a **Join Request**, and the AC responds after authenticating the AP using **MAC address**, **serial number** (SN), or **no authentication**. If authenticated successfully, the AC establishes a connection with the AP either through **Manual configuration** , **automatic discovery** of whitelisted APs, or **manual confirmation**.
  - **Manual configuration:** Preconfigure MAC addresses and serial numbers (SNs) of APs on the AC for automatic connection when APs match the preset credentials in offline mode.
  - **Automatic discovery:** The AC automatically discovers and connects to APs that are set to non-authentication mode or whitelisted under MAC or SN authentication.
  - **Manual confirmation:** If the AP uses MAC or SN authentication and isn't imported offline or whitelisted, it's listed as unauthorized by the AC, requiring manual confirmation to activate.

4. Optional AP Upgrade.

**AP Upgrade**

The AP communicates with the AC to verify software version and, if an update is required, it requests and receives it automatically or through FTP/SFTP based on security requirements, followed by a restart and recheck for version.

**There are different ways to upgrade:**

- **Automatic upgrade:** This happens as soon as the AP connects to the AC for the first time or after being restarted once upgrade settings are in place.
- **AC mode:** Used for a few APs, where they get updates directly from the AC.
- **FTP mode:** Used when security isn't a major concern; updates are downloaded from an FTP server in plain text.
- **SFTP mode:** Used when security is important; updates are downloaded from an SFTP server with encryption and security protections.
- **In-service upgrade:** For APs that are already online and providing Wi-Fi service without interrupting that service too much.
- **Scheduled upgrade:** Also for online APs, done during times when network use is low to avoid disrupting users.

5. CAPWAP Tunnel Maintenance.

✎ **CAPWAP Maintenance**

- **Data tunnel maintenance:**
  - The AP and AC exchange Keepalive packets (through the UDP port **5247**) to detect the data tunnel connectivity.
- **Control tunnel maintenance:**
  - The AP and AC exchange Echo packets (through the UDP port **5246**) to detect the control tunnel connectivity.

#### 1.3.1.1.1.1 Preconfigurations on AC for AP Onboarding:

- Configure network connectivity.

> AC can function as a DHCP server.

- Create an AP group.

> Group similar APs together in an AP group for easier management.

- Configure country code (regulatory domain profile).
- Configure source interface/address for establishing CAPWAP with AP.

### 1.3.1.2 2. WLAN Service Configuration Delivery

**After AP goes online:**

- AC sends a Configuration Update Request to the AP.
- Upon response, AC delivers service configurations to the AP.

#### 1.3.1.2.1 WLAN Profiles:

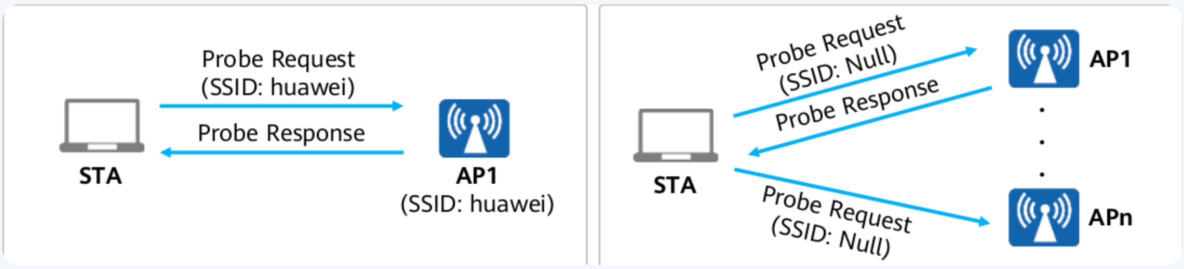
Profiles include regulatory domain profile, radio profile, VAP profile, etc.

- **Regulatory Domain Profile:** Configures country code and radio attributes.
- **Radio Profile:** Optimizes radio parameters like channel and power settings.
- **VAP Profile:** Creates Virtual Access Points with SSID and security settings.

### 1.3.1.3 3. STA Access

**STA access process involves:**

1. Scanning for SSID.



### Scanning

- **Active Scanning**: A STA searches for wireless networks by broadcasting Probe Request frames.
  - **With SSID**: Searches for an AP with a matching SSID.
  - **Without SSID**: Broadcasts to find what wireless services are available.
- **Passive Scanning**: A STA listens for Beacon frames from APs to discover networks.

> APs send Beacon frames at intervals of 100 TUs (1 TU = 1024 microseconds) by default.

2. Link authentication with the network.

### authentication modes:

- Involves two modes:
  - **Open System Authentication**: No actual authentication, any STA can connect.
  - **Shared Key Authentication**: Requires a pre-configured shared key on both STA and AP.

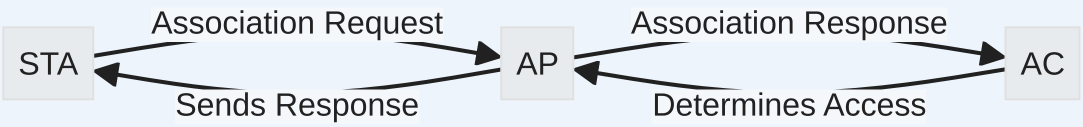
### TIP

link authentication is about establishing a basic connection between your device and the network, whereas access authentication involves proving your identity and securing communication within that network after you're connected.

3. Association with the wireless network (SSID).

### Association

- Occurs after successful link authentication.
- It's a service negotiation process (rate, channel, etc.).



> like agreeing on the rules of conversation before starting to chat

4. Access authentication process (like WPA/WPA2).

### Note

- Differentiates users and controls access rights, more secure than link authentication.
- **Modes:** PSK authentication, 802.1X authentication.
- Ensures data security through encryption (e.g., WEP, WPA/WPA2).

5. Obtaining IP address via DHCP.

### IP

- STAs need IP addresses to connect properly.
- DHCP servers assign IP addresses.

> AC or aggregation switch can function as a DHCP server

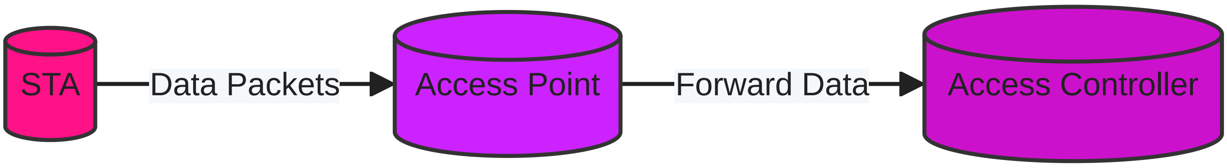
> Previous steps doesn't need ip to communication its need just MAC

6. User authentication for network access control if applicable.

> ✎ **User Authentication**
>
> Users must authenticate on web portals before accessing the Internet.

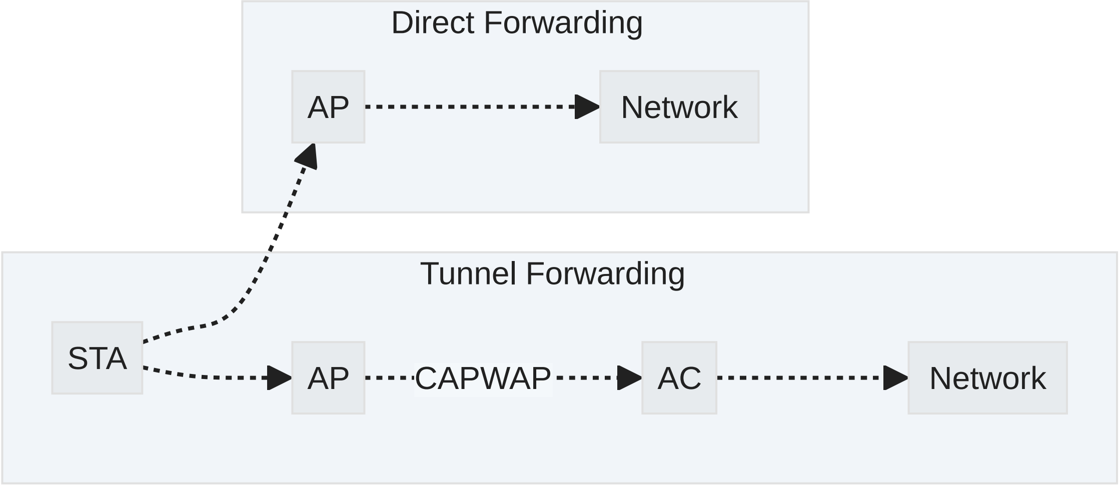
| Policy | Link Auth | Access Auth | Data Encryption | Description |
|---|---|---|---|---|
| WEP | Open system | N/A | No encryption or WEP | Insecure |
| WEP | Shared-key Authentication | N/A | WEP | Insecure |
| WPA/WPA2-802.1X | Open system | 802.1X (EAP) | TKIP or CCMP | A more secure policy, applicable 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 |

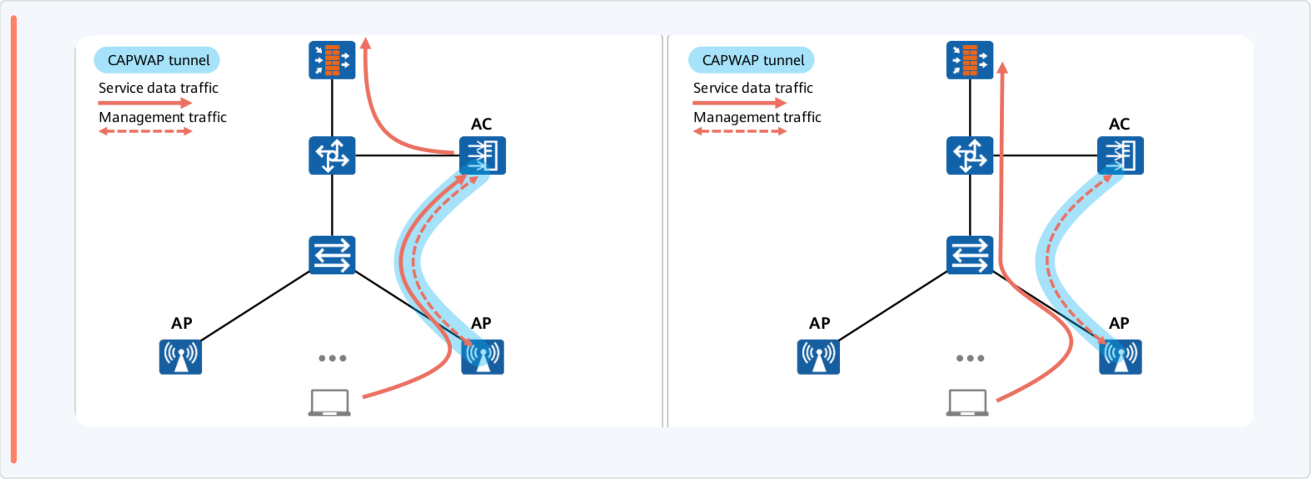
### 1.3.1.4 4. WLAN Service Data Forwarding



### 1.3.1.4.1 Data Forwarding Modes:

---





#### Tunnels Forwarding :

- All data packets are forwarded through an AC.
- More secure but less efficient due to added Load on AC.

#### Direct Forwarding:

- More efficient as it bypasses the AC for data forwarding since data sent directly upper layer network without encapsulating them over a CAPWAP data tunnel.

# 1.4 WLAN Configuration Implementation

## 1.4.1 Basic WLAN Configuration Commands

### 1.4.1.1 Configuring an AP to Go Online

#### 1.4.1.1.1 AP Onboarding

- Configure the AC as a DHCP server with Option 43.

  Markdown

  ```
  [AC-ip-pool-pool1] option <code> sub-option <sub-code> ascii <ascii-string>||hex <hex-string>||cipher <cipher-string>||ip-address <ip-address>
  ```

**More Details**

- `<code>`
  - You're telling the DHCP server (the AC in this case) to include additional configuration information (Option 43) in its responses.
- `<sub-code>`
  - Within this extra information, you can have various pieces each tagged with a different sub-option code.
- `<ascii-string>`
  - The actual content of these pieces can be written out as readable text using ASCII encoding.

- Create a regulatory domain profile and set the country code.

```
[AC-wlan-view] regulatory-domain-profile name <profile-name>
[AC-wlan-regulate-domain-profile-name] country-code <country-code>
```

> Profile name It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

> Country code such as CN (default value): China , AU: Australia ,etc

- Create an AP group and bind regulatory domain profile.

```
[AC-wlan-view] ap-group name <group-name>
[AC-wlan-ap-group-group-name] regulatory-domain-profile <profile-name>
```

> **group name:** It cannot contain question marks (?), slashes (/), or spaces, and cannot start or end with double quotation marks (").

- Configure source interface or address for CAPWAP.

```
[AC] capwap source interface loopback <loopback-number>||vlanif <vlan-id>
```

```
[AC] capwap source ip-address <ip-address>
```

- AP authentication

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

> AP authentication by default, MAC address authentication is used.

- Add APs in offline mode using MAC or SN authentication.

```
[AC-wlan-view] ap-id <ap-id> type-id <type-id>||ap-type <ap-type> ap-mac <ap-mac>||ap-sn <ap-sn>
[AC-wlan-ap-ap-id] ap-name <ap-name>
```

> **ap-id:** ranges from 0 to 8191.

> **type-id:** ranges from 0 to 255.

> **ap-type:** ranges from 1 to 31 characters.

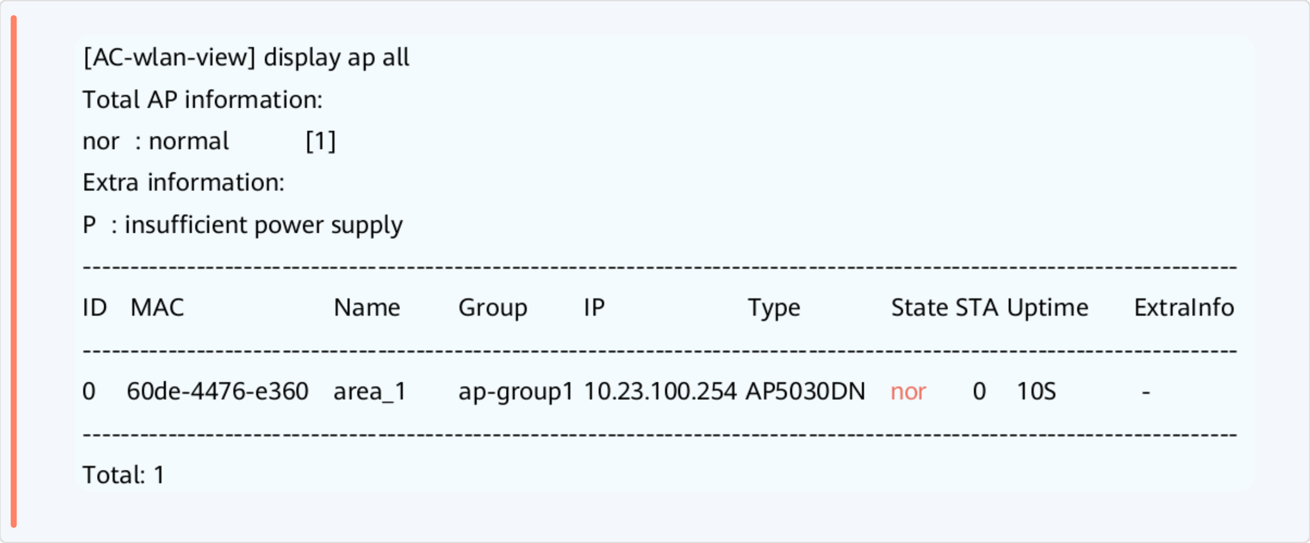
> **ap-sn:** ranges from 1 to 31 characters, and can contain only letters and digits.

- Add the AP to an AP group.

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

- Verifying Configuration

```
[AC] display ap all||ap-group <ap-group>
```



```
[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
```

**AP State**

- **State:** AP state.
  - **normal:** An AP has gone online on an AC and is working properly.
  - **commit-failed:** WLAN service configurations fail to be delivered to an AP after it goes online on an AC.
  - **download:** An AP is in upgrade state.
  - **fault:** An AP fails to go online.
  - **idle:** It is the initialization state of an AP before it establishes a link with the AC for the first time.

## 1.4.1.2 Configuring Radios

- Enter Radio View

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

- Configure Bandwidth and Channel

```
[AC-wlan-radio-0/0] channel <20mhz>||<40mhz-minus>||<40mhz-plus>||<80mhz>||<160mhz> <channel_number>
```

- Set Antenna Gain

```
[AC-wlan-radio-0] antenna-gain <antenna-gain-in-dB>
```

> **antenna-gain:** ranges from 0 to 30, in dB.

- Configure the transmit power for a radio.

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

> eirp ranges from 1 to 127, in dBm.

- Configure the radio coverage distance.

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

> distance ranges from 1 to 400, in 100 meters.

- Configure the operating frequency for a radio.

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

> By default, radio 0 works on the 2.4 GHz frequency band, and radio 2 works on the 5 GHz frequency band.

- Create a radio profile.

```markdown
[AC-wlan-view] radio-2g-profile name <profile-name>
```

> **profile name:** It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

- Bind the radio profile.

```markdown
[AC-wlan-view] ap-group name <group-name>
[AC-wlan-ap-group-group-name] radio-2g-profile <profile-name> radio <radio-id>||all
```

> **radio-id:** can be 0 or 2.

### 1.4.1.3 Configuring VAPs (Virtual Access Points)

---

- Create VAP Profile

```markdown
[AC-wlan-view] vap-profile name <profile-name>
```

- Set Data Forwarding Mode

```markdown
```

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

- Configure service VLANs

```markdown
[AC-wlan-vap-prof-profile-name] service-vlan vlan-id <vlan-id>||vlan-pool <pool-name>
```

- Configure a security profile.

```markdown
[AC-wlan-view] security-profile name <profile-name>
```

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

```markdown
[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.

- Configure an SSID profile

```markdown
[AC-wlan-view] ssid-profile name <profile-name>
```

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

```markdown
[AC-wlan-ssid-prof-profile-name] ssid <ssid>
```

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

> string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters.

> **Note**
>
> To create a Wi-Fi name that begins with a space, put it in quotes like " hello". Quotes count as two extra symbols. To start with a quote, use a backslash before it, like "hello. The backslash counts as one extra symbol.

```
[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.

- Bind the VAP profile

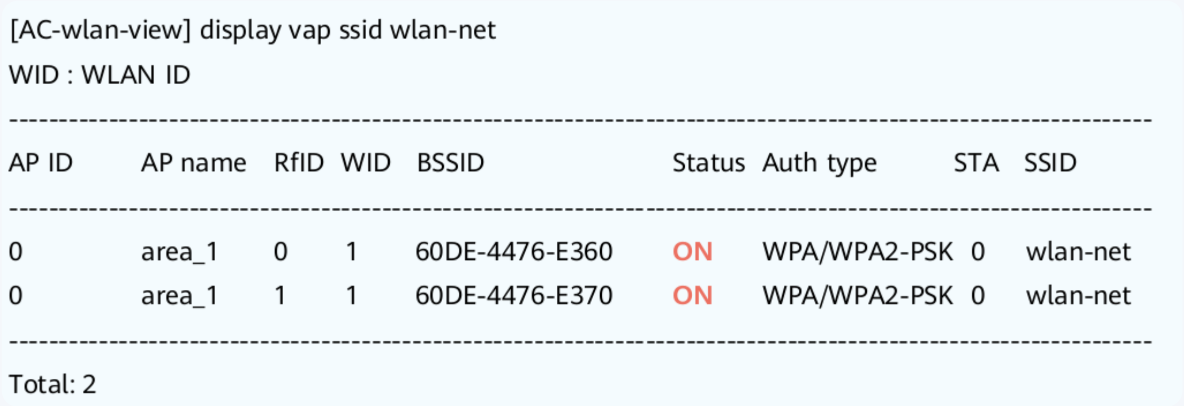
```
[AC-wlan-view] ap-group name <group-name>
[AC-wlan-ap-group-group-name] vap-profile <profile-name> wlan <wlan-id> radio <radio-id>||all service-vlan vlan-id <vlan-id>||vlan-pool <pool-name>
```

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

- 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>
```



```
[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
```

> Display information about service VAPs.

# 1.5 Next-Generation WLAN Solutions

## 1.5.1 Huawei WLAN Solutions Overview

### 1.5.1.1 All-scenario Solutions

- Customized solutions for varied application scenarios.
- Comprehensive deployment and management for campus and branch networks.

### 1.5.1.2 High Bandwidth

- Support for 802.11ac Wave 2 protocol.
- Dual-5G radio coverage with wireless access bandwidth up to 3.46 Gbps.
- Enhancements to Wi-Fi 6 with single 5 GHz radio rate up to 9.6 Gbps.

- Roaming support and multiple wireless QoS protocols like WMM.

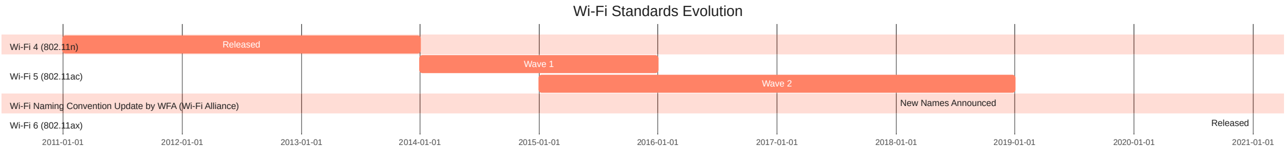
#### 1.5.1.3 High Security

- Mainstream authentication and encryption modes, such as WPA, WPA2, WPA3, and WAPI

#### 1.5.1.4 Easy Deployment

- APs support plug-and-play, automatic upgrade, and dynamic adjustments. Also compatible with IoT integration and offer cloud management capabilities.

### 1.5.2 Wi-Fi Generations Timeline



#### 1.5.2.1 Application Development & Bandwidth Requirements

| Year | Applications | Bandwidth/User | Latency |
|---|---|---|---|
| Pre-2018 | HD Video/Social Networking | 2-4 Mbps | <50 ms |
| Pre-2020 | Video Surveillance/E-Classroom | 4-12 Mbps | <30 ms |
| Post- | Interactive VR/AR/4K Video | >50 Mbps | <10 ms |

| Year | Applications | Bandwidth/User | Latency |
|---|---|---|---|
| 2020 | Conferencing | | |

### 1.5.2.2 Comparison: Wi-Fi 6 Vs. Wi-Fi 5

| Feature | Wi-Fi 5 (802.11ac) | Wi-Fi 6 (802.11ax) |
|---|---|---|
| Maximum Bandwidth | Up to 3.5 Gbps | Up to 9.6 Gbps |
| Concurrency Rate | Supports up to ~100 devices per access point | Supports up to ~400 devices per access point |
| Latency | Average latency about 30 ms | Service latency reduced to ~20 ms |
| Power Consumption | Standard power consumption | Up to 30% reduction in power consumption with TWT |
| Frequency | Primarily operates on 5 GHz band | Operates on both 2.4 GHz and 5 GHz bands |
| Modulation | Up to 256-QAM | Up to 1024-QAM |
| MU-MIMO | Supports MU-MIMO for downlink only | Supports MU-MIMO for both uplink and downlink |
| OFDMA | Not supported | UL/DL OFDMA supported |
| Spatial Reuse | Limited | Enhanced with BSS Coloring |
| Target Wake Time (TWT) | Not supported | Supported |

**Note**

> **Power Consumption**: The introduction of TWT in Wi-Fi 6 helps devices conserve power by scheduling wake times.

> **Modulation**: Higher-QAM allows for denser data transmission in good signal conditions.

> **MU-MIMO**: Multi-user, multiple-input, multiple-output technology enables more efficient data transmission for multiple devices concurrently.

> **OFDMA**: Orthogonal frequency division multiple access allows the splitting of channels into smaller sub-channels, improving efficiency particularly in dense environments.

> **Spatial Reuse**: Techniques like BSS Coloring in Wi-Fi 6 help reduce interference from neighboring networks.

> **Target Wake Time (TWT)**: This feature helps manage when clients need to wake up and communicate with the AP, reducing power usage.

## 1.5.3 Next-generation Campus Networks

### 1.5.3.1 Small-and-Medium-Sized Intent-driven Campus

#### 1.5.3.1.1 Cloud Management Platform Benefits:

- Using a cloud management platform makes it easier and cheaper to handle all your devices from one place.

#### 1.5.3.1.2 Advantages over AC + Fit AP Architecture:

- Cloud-based Wi-Fi architecture makes setting up and managing networks easier and cheaper by offering simple setup, centralized control, and built-in tools.

## 1.5.3.2 Medium-and-Large-Sized Intent-driven Campus

### 1.5.3.2.1 Native AC Architecture Characteristics:

- iMaster NCE Simplifies the management of wireless access points and wired networks using advanced data analysis and artificial intelligence to create easy-to-use, smart, and secure networks for medium to large businesses.