WLAN Overview



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

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

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

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



Contents

[1 WLAN Overview 1](#_Toc60149112)

[1.1 Foreword 1](#_Toc60149113)

[1.2 Objectives 1](#_Toc60149114)

[1.3 WLAN Overview 2](#_Toc60149115)

[1.3.1 Introduction to WLAN 2](#_Toc60149116)

[1.3.2 IEEE 802.11、WLAN and Wi-Fi 3](#_Toc60149117)

[1.3.3 Wi-Fi Development Trends in Office Scenarios 4](#_Toc60149118)

[1.4 Basic Concepts of WLAN 6](#_Toc60149119)

[1.4.1 WLAN Devices 6](#_Toc60149120)

[1.4.2 Basic WLAN Networking Architecture 7](#_Toc60149121)

[1.4.3 Basic WLAN Concepts 9](#_Toc60149122)

[1.4.4 CAPWAP 10](#_Toc60149123)

[1.4.5 AP-AC Networking 11](#_Toc60149124)

[1.4.6 AC Connection Mode 12](#_Toc60149125)

[1.4.7 Wireless Communications System 13](#_Toc60149126)

[1.4.8 Radio Wave 14](#_Toc60149127)

[1.4.9 Radio Channel 14](#_Toc60149128)

[1.4.10 BSS/SSID/BSSID 16](#_Toc60149129)

[1.4.11 VAP 17](#_Toc60149130)

[1.4.12 ESS 18](#_Toc60149131)

[1.5 WLAN Fundamentals 19](#_Toc60149132)

[1.5.1 WLAN Working Process Overview 19](#_Toc60149133)

[1.5.2 WLAN Working Process: Step 1 20](#_Toc60149134)

[1.5.3 WLAN Working Process: Step 2 29](#_Toc60149135)

[1.5.4 WLAN Working Process: Step 3 32](#_Toc60149136)

[1.5.5 WLAN Working Process: Step 4 39](#_Toc60149137)

[1.6 WLAN Configuration Implementation 40](#_Toc60149138)

[1.6.1 Basic WLAN Configuration Commands: Configuring an AP to Go Online 40](#_Toc60149139)

[1.6.2 Basic WLAN Configuration Commands: Configuring Radios 43](#_Toc60149140)

[1.6.3 Basic WLAN Configuration Commands: Configuring VAPs 45](#_Toc60149141)

[1.6.4 Example for Configuring Layer 2 Tunnel Forwarding in Off-Path Mode 47](#_Toc60149142)

[1.6.5 Configuring Network Connectivity 49](#_Toc60149143)

[1.6.6 Configuring APs to Go Online 49](#_Toc60149144)

[1.6.7 Verifying the AP Onboarding Configuration 50](#_Toc60149145)

[1.6.8 Configuring WLAN Service Parameters 51](#_Toc60149146)

[1.6.9 Checking VAP Profile Information 52](#_Toc60149147)

[1.7 Next-Generation WLAN Solutions 53](#_Toc60149148)

[1.7.1 Huawei WLAN Solutions Meet Future Wireless Network Construction Requirements 53](#_Toc60149149)

[1.7.2 Dual Drivers (Technology Advances + Application Development) Promote the Arrival of the Wi-Fi 6 Era 54](#_Toc60149150)

[1.7.3 Wi-Fi 6 Vs. Wi-Fi 5 54](#_Toc60149151)

[1.7.4 Next-Generation Campus Network: Intent-Driven Campus (Small- and Medium-Sized) 56](#_Toc60149152)

[1.7.5 Next-Generation Campus Network: Intent-Driven Campus (Medium- and Large-Sized) 58](#_Toc60149153)

[1.8 Summary 59](#_Toc60149154)

[1.9 Quiz 60](#_Toc60149155)

# WLAN Overview

## 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.

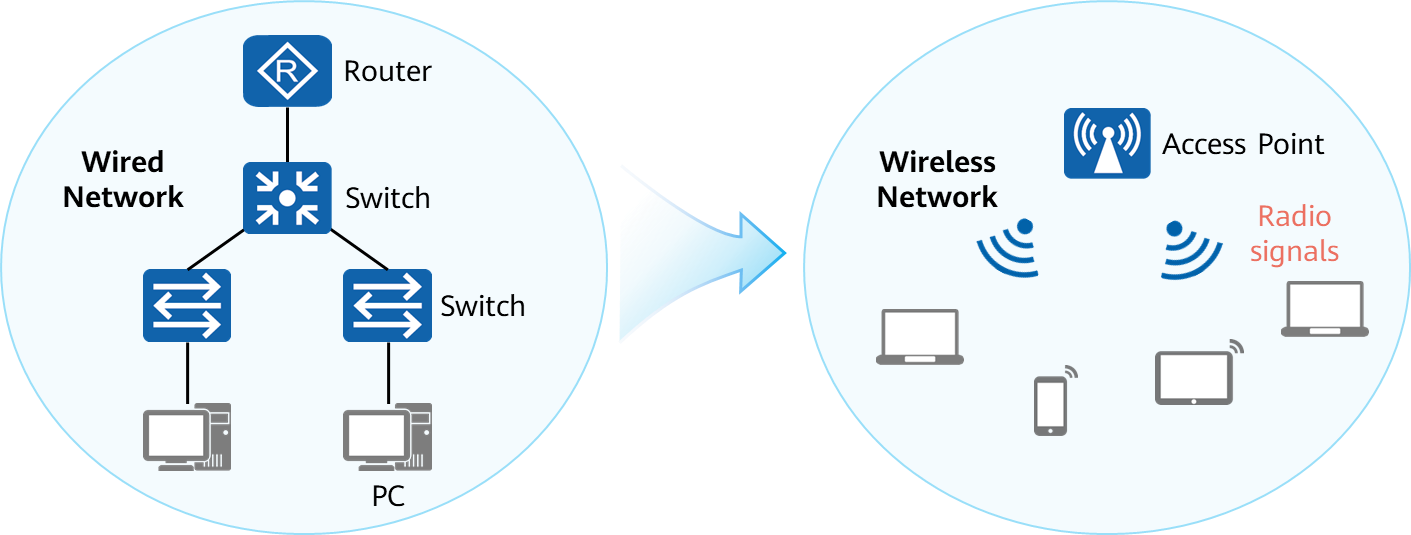
Distinguish between different WLAN networking architectures.

Understand the WLAN working process.

Complete basic WLAN configurations.

## WLAN Overview

### Introduction to WLAN



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.

Wireless technologies mentioned here include not only Wi-Fi, but also infrared, Bluetooth, and ZigBee.

WLAN technology allows users to easily access a wireless network and move around within the coverage of the wireless network.

Wireless networks can be classified into WPAN, WLAN, WMAN, and WWAN based on the application scope:

* Wireless personal area network (WPAN): Bluetooth, ZigBee, NFC, HomeRF, and UWB technologies are commonly used.
* Wireless local area network (WLAN): The commonly used technology is Wi-Fi. WPAN-related technologies may also be used in WLANs.
* Wireless metropolitan area network (WMAN): Worldwide Interoperability for Microwave Access (WiMAX) is commonly used.
* Wireless wide area network (WWAN): GSM, CDMA, WCDMA, TD-SCDMA, LTE, and 5G technologies are commonly used.

Advantages of WLAN:

* High network mobility: WLANs are easily connected, and are not limited by cable and port positions. This makes WLANs most suitable for scenarios where users are often moving, such as in office buildings, airport halls, resorts, hotels, stadiums, and cafes.
* Flexible network deployment: WLANs provide wireless network coverage in places where cables are difficult to deploy, such as subways and highways. WLANs reduce the number of required cables, offer low-cost, simplify deployment, and have high scalability.

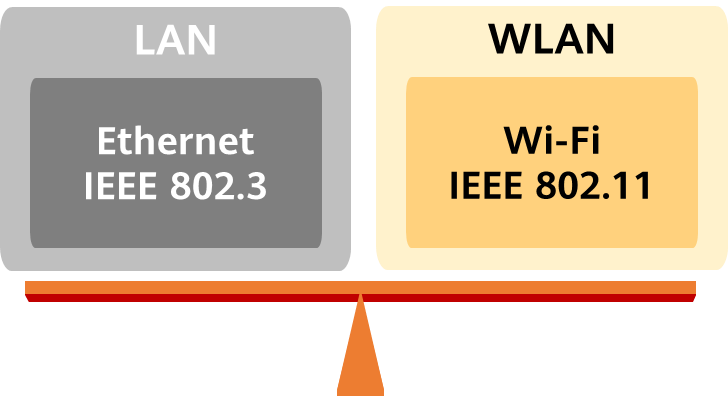
WLAN technology allows users to easily access a wireless network and move around within the coverage of the wireless network.

Note: WLAN technology described in this document is implemented based on 802.11 standards. That is, a WLAN uses high-frequency (2.4 GHz or 5 GHz) signals as transmission media.

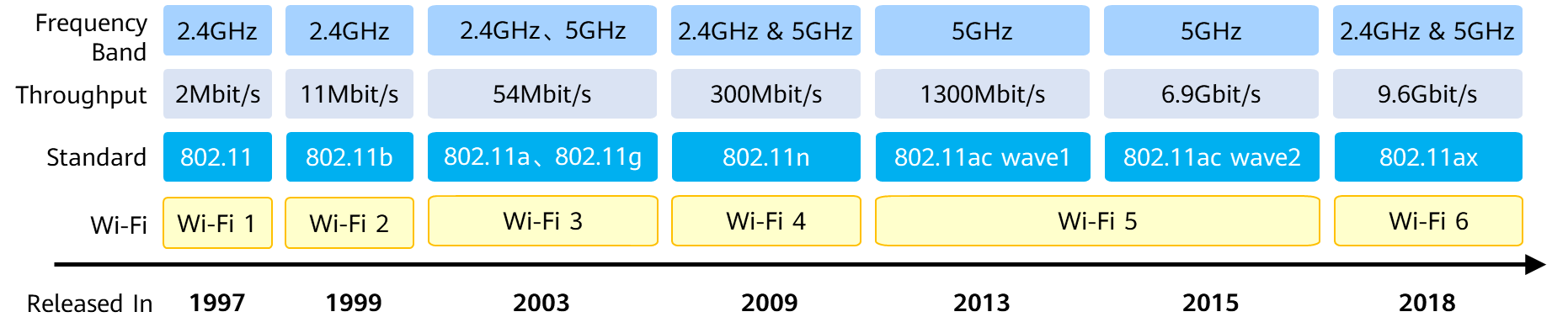
### IEEE 802.11、WLAN and Wi-Fi

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.



.LAN and WLAN



IEEE 802.11 Standards and Wi-Fi Generations

IEEE 802.11 standards are located on the lower two layers of the equivalent TCP/IP model.

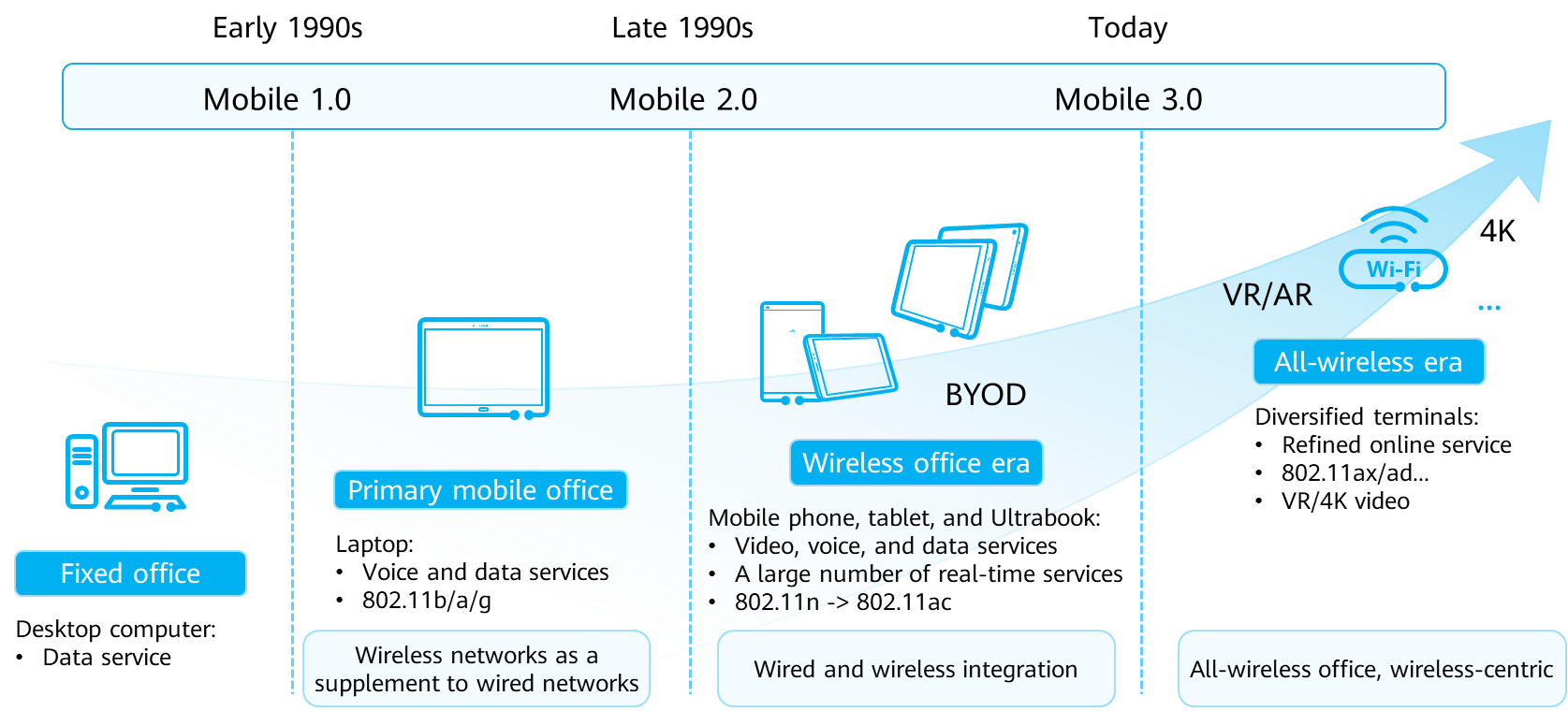
* Data link layer: provides channel access, addressing, data frame check, error detection, and security mechanisms.
* Physical layer: transmits bit streams over an air interface, for example, specifying the frequency band.

When created in 1999, the Wi-Fi Alliance was called the Wireless Ethernet Compatibility Alliance (WECA) at that time. In October 2002, the WECA was renamed Wi-Fi Alliance.

The first version of IEEE 802.11 was released in 1997. Since then, more IEEE 802.11-based supplementary standards have been gradually defined. The most well-known standards that affect the evolution of Wi-Fi are 802.11b, 802.11a, 802.11g, 802.11n, and 802.11ac.

When the IEEE 802.11ax standard is released, the Wi-Fi Alliance renames the new Wi-Fi specification to Wi-Fi 6, the mainstream IEEE 802.11ac to Wi-Fi 5, and IEEE 802.11n to Wi-Fi 4. The same naming convention applies to other generations.

### Wi-Fi Development Trends in Office Scenarios



Wi-Fi Development Trends in Office Scenarios

Phase 1: Initial Mobile Office Era — Wireless Networks as a Supplement to Wired Networks

* WaveLAN technology is considered as the prototype of enterprise WLAN. Early Wi-Fi technologies were mainly applied to IoT devices such as wireless cash registers. However, with the release of 802.11a/b/g standards, wireless connections have become increasingly advantageous. Enterprises and consumers are beginning to realize the potential of Wi-Fi technologies, and wireless hotspots are found to be deployed in cafeterias, airports, and hotels.
* The name Wi-Fi was also created during this period. It is the trademark of the Wi-Fi Alliance. The original goal of the alliance was to promote the formulation of the 802.11b standard as well as the compatibility certification of Wi-Fi products worldwide. With the evolution of standards and the popularization of standard-compliant products, people tend to equate Wi-Fi with the 802.11 standard.
* The 802.11 standard is one of many WLAN technologies, and yet it has become a mainstream standard in the industry. When a WLAN is mentioned, it usually is a WLAN using the Wi-Fi technology.
* The first phase of WLAN application eliminated the limitation of wired access, with the goal to enable devices to move around freely within a certain range. That is, WLAN extends wired networks with the utilization of wireless networks. In this phase, WLANs do not have specific requirements on security, capacity, and roaming capabilities. APs are still single access points used for wireless coverage in single-point networking. Generally, an AP using a single access point architecture is called a Fat AP.

Phase 2: Wireless Office Era — Integration of Wired and Wireless Networks

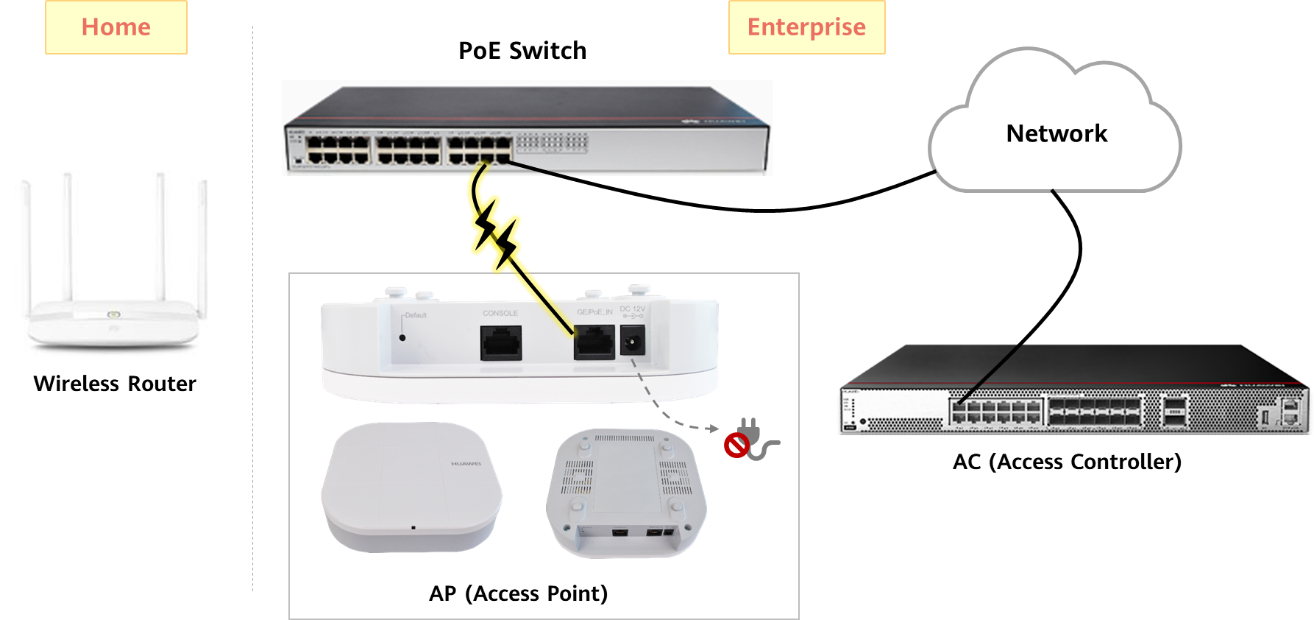
* With the increasing popularity of wireless devices, WLANs have evolved from the supplement of wired networks to necessities.
* In this phase, a WLAN, as a part of the network, needs to provide network access for enterprise guests.
* Numerous large-bandwidth services, such as video and voice, are required in office scenarios, thereby imposing higher bandwidth requirements on WLANs. Since 2012, the 802.11ac standard has become mature and implemented many improvements in the working frequency bands, channel bandwidths, as well as modulation and coding schemes (MCSs). Compared with earlier 802.11 standards, the 802.11ac standard includes higher traffic volumes and less interference, and it allows more users to access networks.

Phase 3: All-Wireless Office Era, Wireless-Centric

* Currently, WLANs have entered the third phase. In office environments, wireless networks are used in preference to wired networks, and each office area is covered entirely by Wi-Fi. Furthermore, office areas do not include a wired network port, making the office environment more open and intelligent.
* In the future, high-bandwidth services, including cloud desktop office, telepresence conference, and 4K video, will be migrated from wired to wireless networks. Likewise, new technologies such as virtual reality (VR)/augmented reality (AR) will be directly deployed on wireless networks. These new application scenarios pose higher requirements on WLAN design and planning.
* The year 2018 marked the release of the next-generation Wi-Fi standard, referred to as Wi-Fi 6 and 802.11ax by the Wi-Fi Alliance and IEEE, respectively. This represents another milestone in Wi-Fi development. In that regard, the core value of Wi-Fi 6 is further improvements in capacity, leading wireless communications into the 10-gigabit era. The concurrent performance has improved fourfold, ensuring excellent service capabilities in high-density access and heavy-load scenarios.

## Basic Concepts of WLAN

### WLAN Devices



WLAN Devices

Huawei WLAN products provide high-speed, secure, and reliable wireless network connections in various scenarios, such as indoor and outdoor scenarios and home and enterprise scenarios.

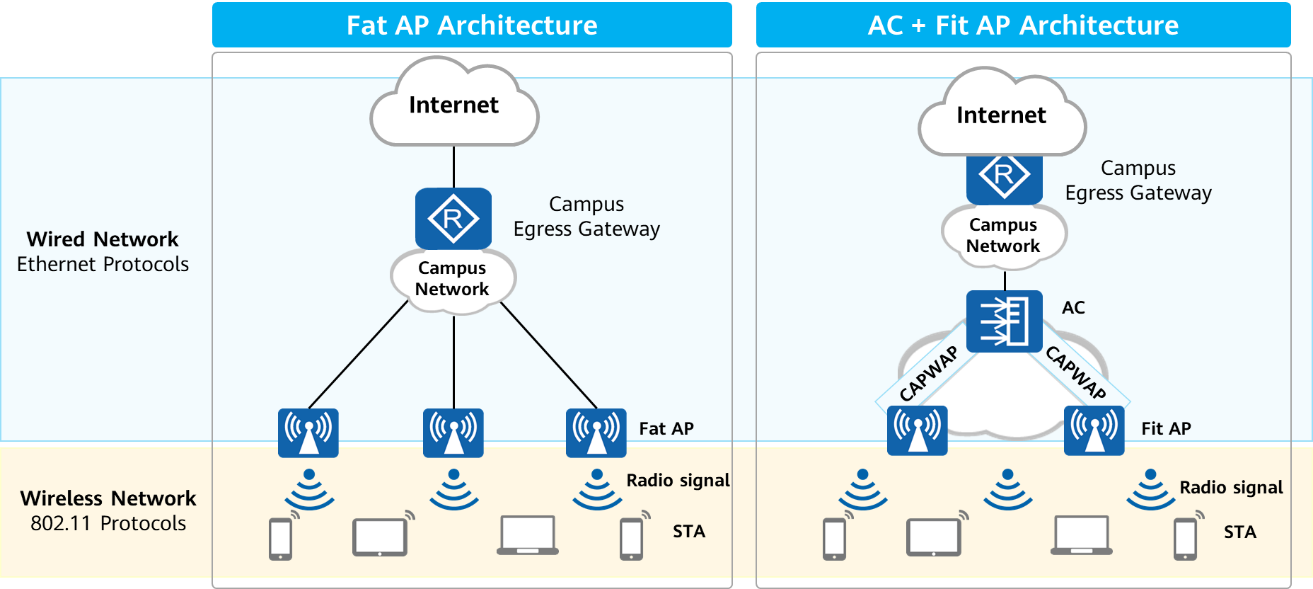
Wireless routers are Fat APs in most cases:

A wireless router converts wired network signals into wireless signals to be received by devices such as home computers and mobile phones so that they can access the Internet in wireless mode.

Enterprise WLAN products:

* AP:
  1. The AP can switch flexibly among the Fat, Fit, and cloud modes based on the network plan.
  2. Fat AP: applies to home WLANs. A Fat AP works independently and requires separate configurations. It provides only simple functions and is cost-effective. The Fat AP independently implements functions such as user access, authentication, data security, service forwarding, and QoS.
  3. Fit AP: applies to medium- and large-sized enterprises. Fit APs are managed and configured by the AC in a unified manner, provide various functions, and have high requirements on network maintenance personnel's skills. Fit APs must work with an AC for user access, AP going-online, authentication, routing, AP management, security, and QoS.
  4. Cloud AP: applies to small- and medium-sized enterprises. Cloud APs are managed and configured by a cloud management platform in a unified manner, provide various functions, support plug-and-play, and have low requirements on network maintenance personnel's skills.
* AC
  1. An AC is usually deployed at the aggregation layer of a network to provide high-speed, secure, and reliable WLAN services.
  2. Huawei ACs provide a large capacity and high performance. They are highly reliable, easy to install and maintain, and feature such advantages as flexible networking and energy conservation.
* PoE Switch
  1. Power over Ethernet (PoE) provides electrical power through the Ethernet. It is also called Power over LAN (PoL) or active Ethernet.
  2. PoE transmits power to terminals through data transmission lines or idle lines.
  3. On a WLAN, a PoE switch can be used to supply power to APs.
  4. PoE can be used to effectively provide centralized power for terminals such as IP phones, APs, portable device chargers, POS machines, cameras, and data collection devices. With PoE, terminals are provided with power when they access the network. Therefore, indoor cabling of power supply is not required.

### Basic WLAN Networking Architecture



Basic WLAN Networking Architecture

A WLAN involves both wired and wireless sides. On the wired side, APs connect to the Internet using Ethernet. On the wireless side, STAs communicate with APs using 802.11 standards.

The wireless side uses the centralized architecture. The original Fat AP architecture evolves to the AC + Fit AP architecture.

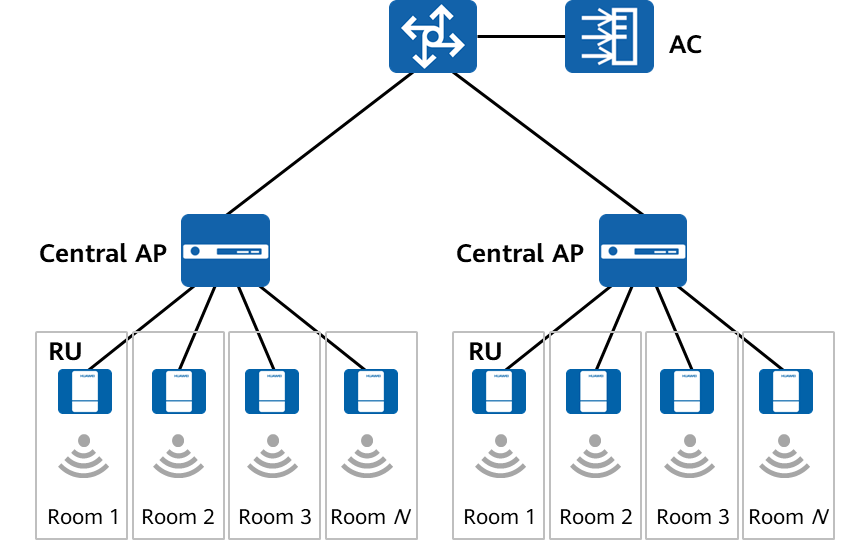
* Fat AP architecture
  1. This architecture is also called autonomous network architecture because it does not require a dedicated device for centralized control. It can implement functions such as connecting wireless users, encrypting service data, and forwarding service data packets.
  2. Applicable scope: home and small-sized enterprises
  3. Characteristics: A Fat AP works independently and is configured separately. It provides only simple functions and is cost-effective.
  4. Disadvantages: The increase in the WLAN coverage area and the number of access users requires more and more Fat APs. No unified control device is available for these independently working Fat APs. Therefore, it is difficult to manage and maintain the Fat APs.
* AC + Fit AP architecture
  1. In this architecture, an AC is responsible for WLAN access control, forwarding and statistics collection, AP configuration monitoring, roaming management, AP network management agent, and security control. A Fit AP encrypts and decrypts 802.11 packets, provides 802.11 physical layer functions, and is managed by an AC.
  2. Applicable scope: medium- and large-sized enterprises
  3. Characteristics: Fit APs are managed and configured by the AC in a unified manner, provide various functions, and have high requirements on network maintenance personnel's skills.

Note: This course uses the AC + Fit AP architecture as an example.

Basic WLAN Concepts:

* Station (STA):02.11-compliant terminal, for example, PC with wireless network interface cards (NICs) or mobile phone that supports WLAN
* AC:ontrols and manages all Fit APs on an AC + Fit AP network. For example, an AC can connect to an authentication server to authenticate WLAN users.
* AP:rovides 802.11-compliant wireless access for STAs. APs connect wired networks to wireless networks.
* Control And Provisioning of Wireless Access Points (CAPWAP):An encapsulation and transmission mechanism defined in RFC 5415 to implement communication between APs and ACs.
* Radio signal (radio electromagnetic wave):High-frequency electromagnetic wave that has long-distance transmission capabilities. Radio signals provide transmission media for 802.11-compliant WLANs. Radio signals described in this course are electromagnetic waves on the 2.4 GHz or 5 GHz frequency band.

### Basic WLAN Concepts

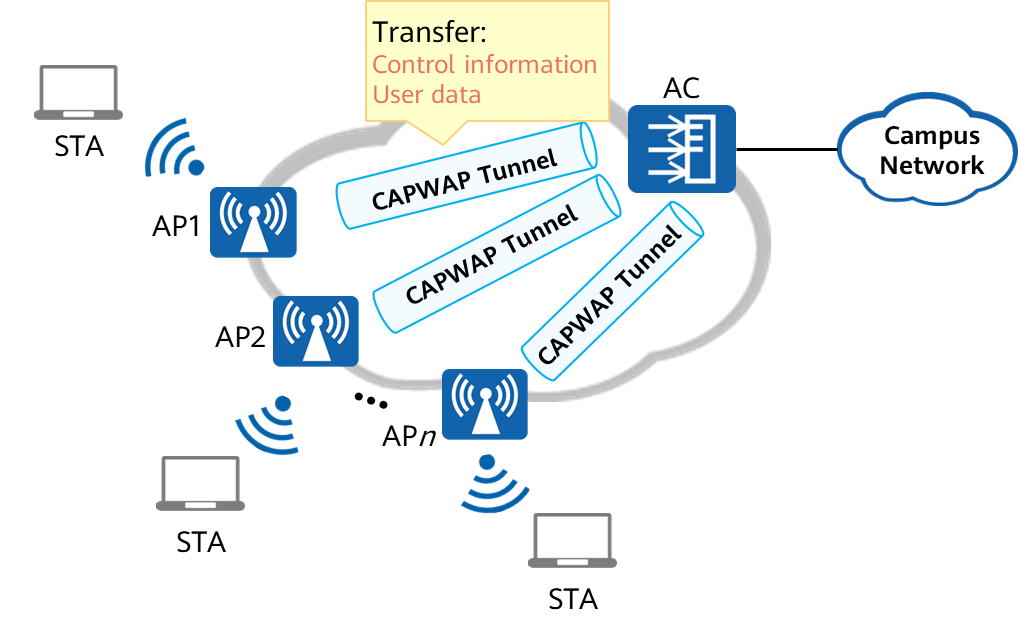


Basic WLAN Concepts

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



CAPWAP

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 Function:

* 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.

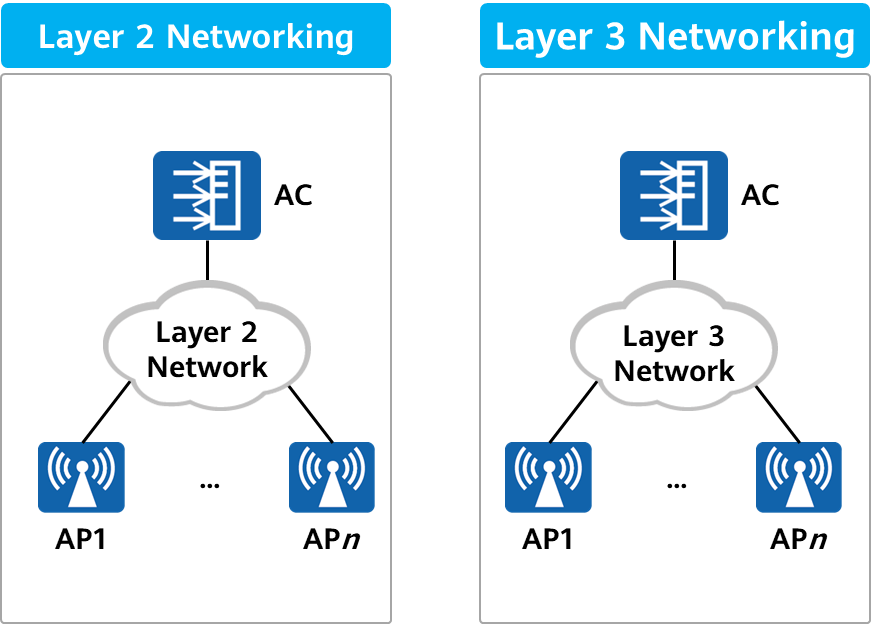
To meet the requirements of large-scale networking and unified management of APs on the network, the Internet Engineering Task Force (IETF) sets up a CAPWAP Working Group and formulates the CAPWAP protocol. This protocol defines how an AC manages and configures APs. That is, CAPWAP tunnels are established between the AC and APs, through which the AC manages and controls the APs.

CAPWAP is an application-layer protocol based on UDP transmission.

* CAPWAP functions in the transmission of two types of messages:
  1. Data messages, which encapsulate wireless data frames through the CAPWAP data tunnel.
  2. Control messages, which are exchanged for AP management through the CAPWAP control tunnel.
* CAPWAP data and control packets are transmitted on different UDP ports:
  1. UDP port 5246 for transmitting control packets
  2. UDP port 5247 for transmitting data packets

### AP-AC Networking

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



AP-AC 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: APs are connected to an AC across a Layer 3 network.

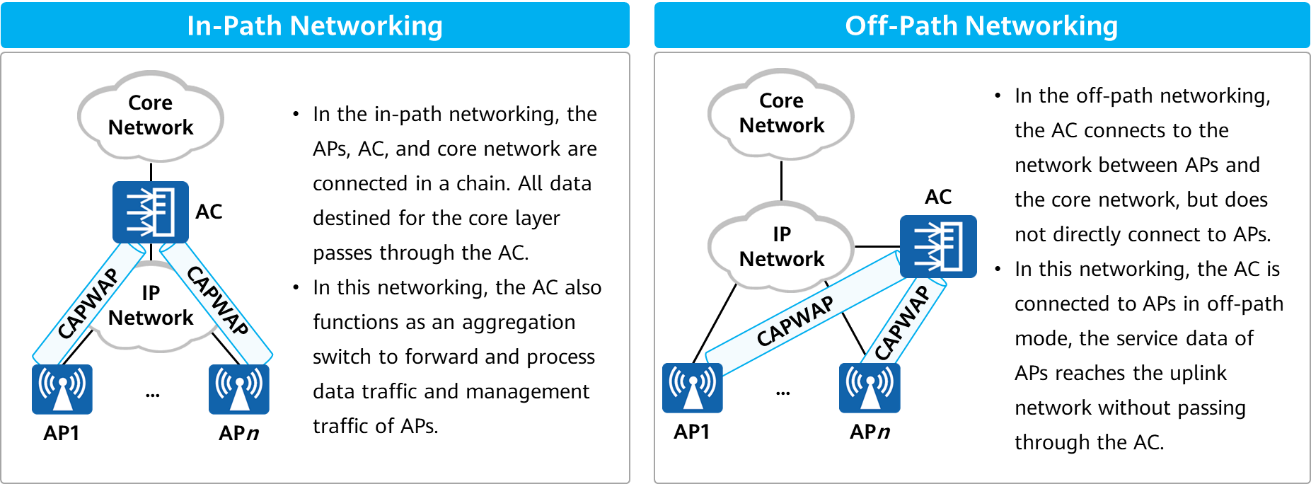
In the actual networking, an AC can connect to dozens or even hundreds of APs, which is usually complex. In most cases, the Layer 3 networking is used on a large network.

AP-AC networking: The Layer 2 or Layer 3 networking can be used between the AC and APs. In the Layer 2 networking, APs can go online in plug-and-play mode through Layer 2 broadcast or DHCP. In the Layer 3 networking, APs cannot directly discover an AC. We need to deploy DHCP or DNS, or manually specify the AC's IP address.

In the actual networking, an AC may connect to dozens or even hundreds of APs, which is complex. For example, on an enterprise network, APs can be deployed in offices, meeting rooms, and guest rooms, and the AC can be deployed in the equipment room. This constructs a complex Layer 3 network between the AC and APs. Therefore, the Layer 3 networking is often used on large-scale networks.

### AC Connection Mode

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



AC Connection Mode

AC connection mode: In in-path mode, the AC is deployed on the traffic forwarding path, and user traffic passes through the AC. This consumes the AC's forwarding capability. In off-path mode, traffic does not pass through the AC.

In-path networking:

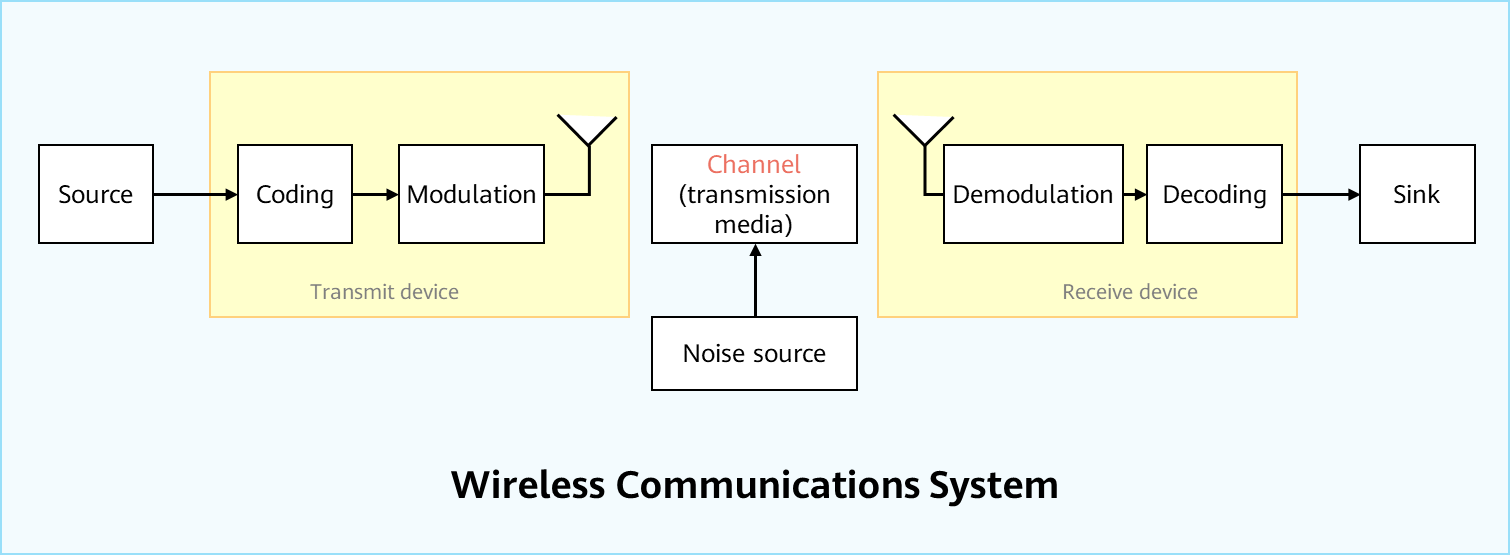
* In the in-path networking, the AC must be powerful in throughput and processing capabilities, or the AC becomes the bandwidth bottleneck.
* This networking has a clear architecture and is easy to deploy.

Off-path networking:

* Most wireless networks are deployed after wired networks are constructed and are not planned in early stage of network construction. The off-path networking makes it easy to expand the wireless network. Customers only need to connect an AC to a network device, for example, an aggregation switch, to manage APs. Therefore, the off-path networking is used more often.
* In the off-path networking, the AC only manages APs, and management flows are encapsulated and transmitted in CAPWAP tunnels. Data flows can be forwarded to the AC over CAPWAP tunnels, or forwarded to the uplink network by the aggregation switch and do not pass 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

Coding:

* Source coding is a process of converting raw information into digital signals by using a coding scheme.
* Channel coding is a technology for correcting and detecting information errors to improve channel transmission reliability. With wireless transmission that is prone to noise interference, information arriving at the receive device may be erroneous. Channel coding is introduced to restore information to the maximum extent on the receive device, thereby reducing the bit error rate.

Modulation is a process of superimposing digital signals on high-frequency signals generated by high-frequency oscillation circuits so that the digital signals be converted into radio waves over antennas and then transmitted.

A channel transmits information, and a radio channel is a radio wave in space.

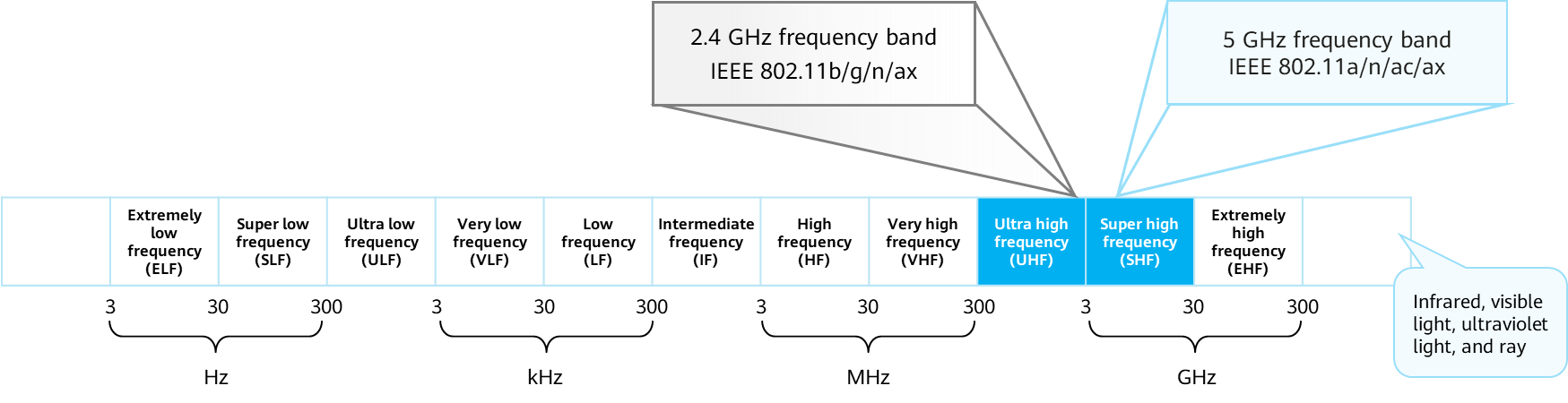
The air interface is used by radio channels. The transmit device and receive device are connected through the air interfaces and channels. The air interfaces in wireless communication are invisible and connected over the air.

### 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:

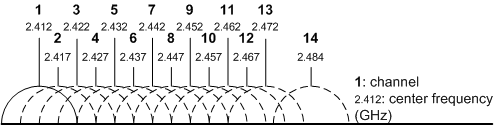
* 2.4 GHz frequency band (2.4–2.4835 GHz)
* 5 GHz frequency band (5.15–5.35 GHz, 5.725–5.85 GHz)



Radio Wave Spectrum

### Radio Channel

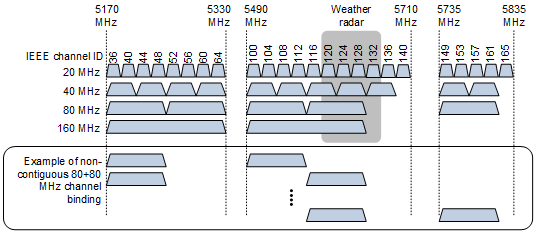
A channel transmits information, and a radio channel is a radio wave in space. Given that radio waves are ubiquitous, the random use of spectrum resources will cause endless interference issues. Therefore, in addition to defining the usable frequency bands, wireless communication protocols must also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



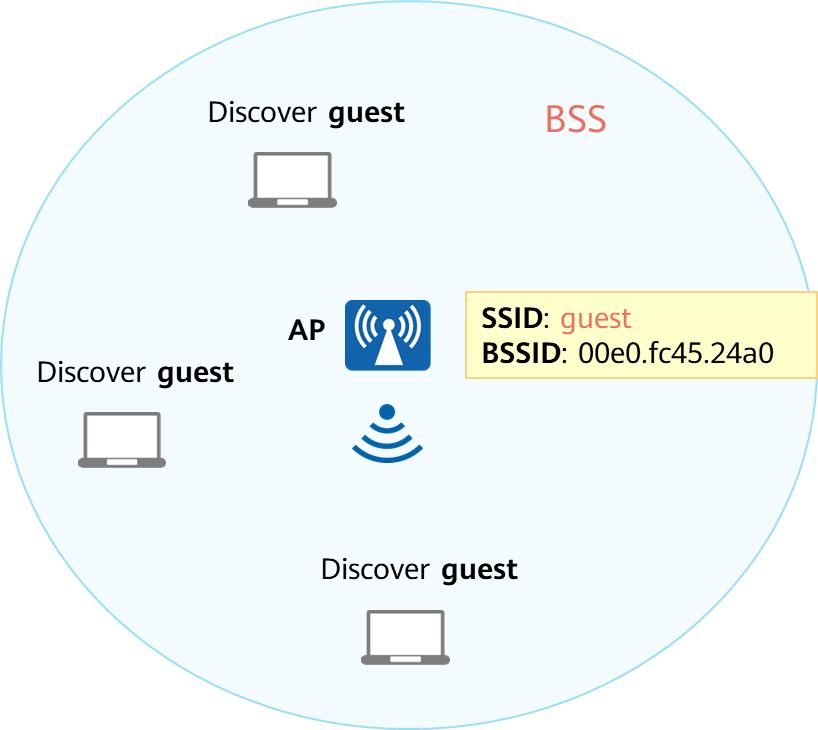
5 GHz Frequency Band

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.

On a WLAN, the operating status of APs is affected by the radio environment. For example, a high-power AP can interfere with adjacent APs if they work on overlapping channels.

In this case, the radio calibration function can be deployed to dynamically adjust channels and power of APs managed by the same AC to ensure that the APs work at the optimal performance.

### BSS/SSID/BSSID



BSS/SSID/BSSID

BSS:

A BSS, the basic service unit of a WLAN, consists of an AP and multiple STAs. The BSS is the basic structure of an 802.11 network. Wireless media can be shared, and therefore packets sent and received in a BSS must carry the BSSID (AP's MAC address).

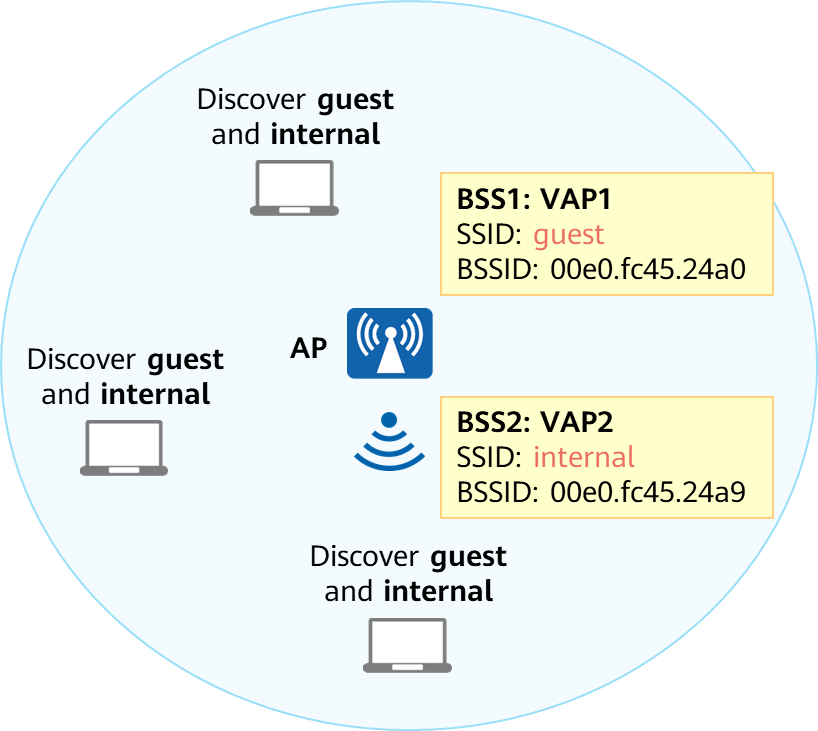
BSSID:

* AP's MAC address on the data link layer.
* STAs can discover and find an AP based on the BSSID.
* Each BSS must have a unique BSSID. Therefore, the AP's MAC address is used to ensure the uniqueness of the BSSID.

SSID:

* A unique identifier that identifies a wireless network. When you search for available wireless networks on your laptop, SSIDs are displayed to identify the available wireless networks.
* If multiple BSSs are deployed in a space, the STA may discover not only one BSSID. You only need to select a BSSID as required. For easier AP identification, a string of characters is configured as the AP name. This character string is the SSID.

### VAP



VAP

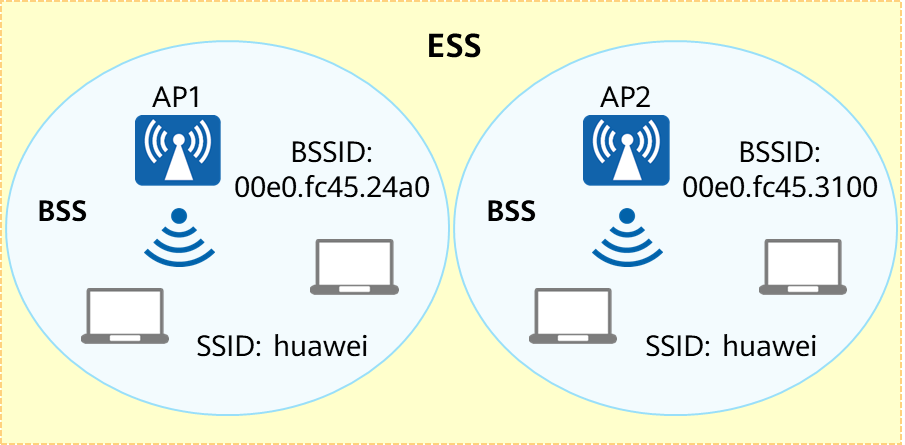
In the early stage, APs support only one BSS. If multiple BSSs are deployed in a space, we must also deploy multiple APs, which increases costs and occupies channel resources. To resolve this problem, APs now support creation of multiple virtual access points (VAPs).

VAP:

* A VAP is a functional entity virtualized on a physical AP. You can create different VAPs on an AP to provide the wireless access service for different user groups.
* 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.

The use of VAPs simplifies WLAN deployment, but it does not mean that we need to configure as many as VAPs. VAPs must be planned based on actual requirements. Simply increasing the number of VAPs will increase the time for STAs to find SSIDs and make AP configuration more complex. Additionally, a VAP is not equivalent to a real AP. All VAPs virtualized from a physical AP share software and hardware resources of the AP, and all users associated with these VAPs share same channel resources. The capacity of an AP will not change or multiply with the increasing number of VAPs.

### ESS



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:

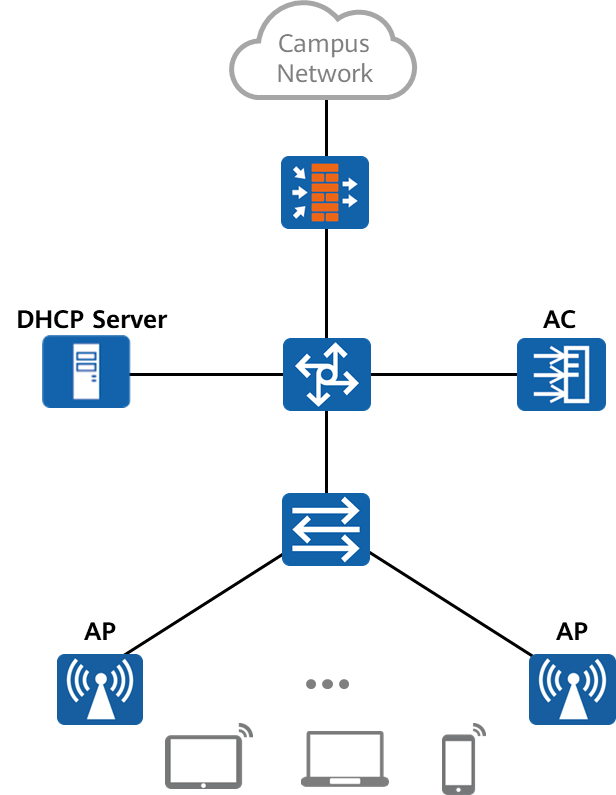
* A larger-scale virtual BSS that consists of multiple BSSs with the same SSID.
* A large-scale virtual BSS consisting of multiple BSSs with the same SSID.
* A STA can move and roam within an ESS and considers that it is within the same WLAN regardless of its location.

WLAN roaming:

* WLAN roaming allows STAs to move within the coverage areas of APs belonging to the same ESS with nonstop service transmission.
* The most obvious advantage of the WLAN is that a STA can move within a WLAN without physical media restrictions. WLAN roaming allows the STA to move within a WLAN without service interruption. Multiple APs are located within an ESS. When a STA moves from an AP to another, WLAN roaming ensures seamless transition of STA services between APs.

## WLAN Fundamentals

### WLAN Working Process Overview



Typical WLAN network topology

In the AC + Fit AP networking architecture, the AC manages APs in a unified manner. Therefore, all configurations are performed on the AC.

WLAN Working Process：

* AP onboarding:An AP obtains an IP address, discovers an AC, and sets up a connection with the AC.
* WLAN service configuration delivery:The AC delivers WLAN service configurations to the AP.
* STA access:STAs find the SSID transmitted by the AP, connect to the network, and go online.
* WLAN service data forwarding:The WLAN starts to forward service data.

### WLAN Working Process: Step 1

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:

* An AP obtains an IP address.
* The AP discovers the AC and establishes a CAPWAP tunnel with it.
* AP access control
* AP upgrade
* CAPWAP tunnel maintenance

#### APs Obtain IP Addresses

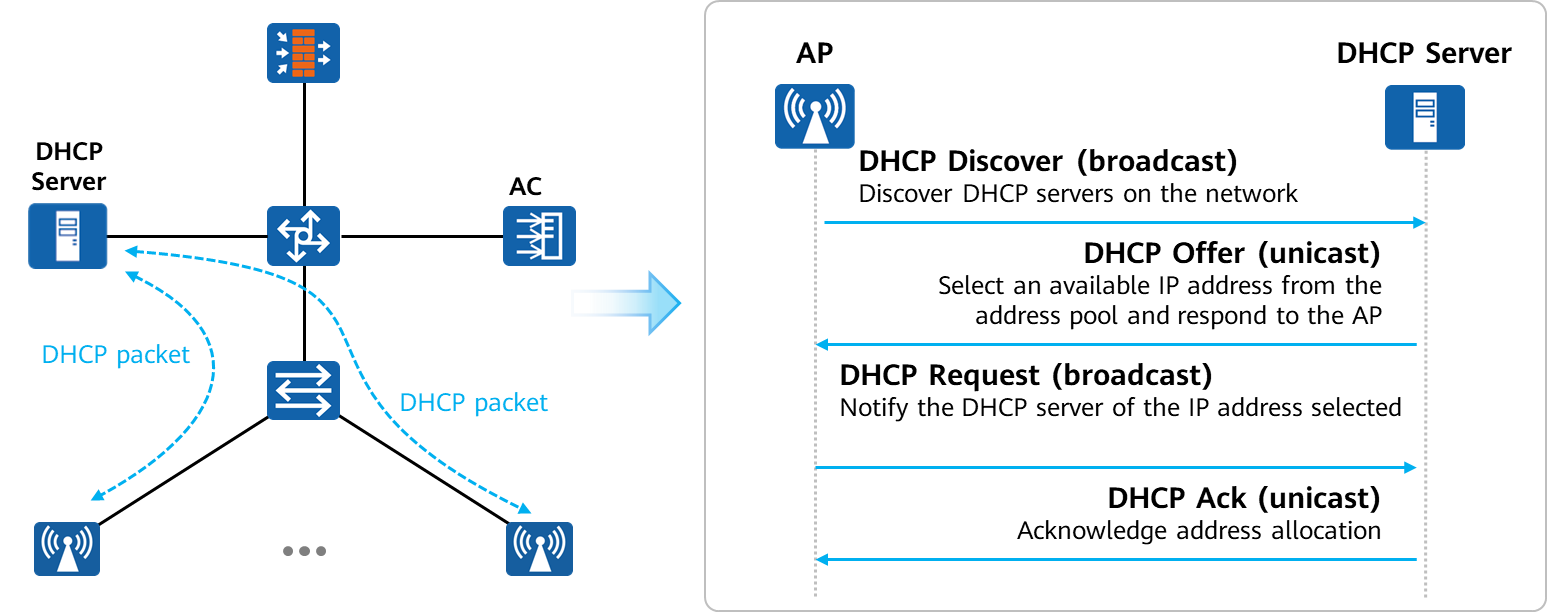
An AP can communicate with an AC only after obtaining an IP address.

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:

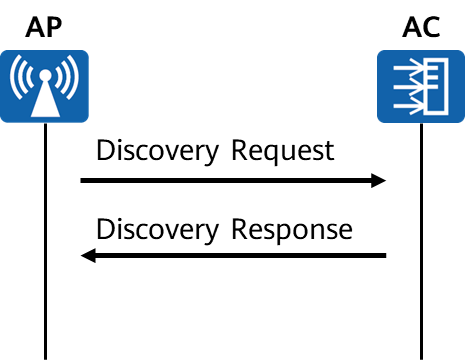
* Deploy a dedicated DHCP server to assign IP addresses to APs.
* Configure the AC to assign IP addresses to APs.
* Use a device on the network, such as a core switch, to assign IP addresses to APs.



DHCP IP Address Allocation

#### CAPWAP Tunnel Establishment

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



CAPWAP Tunnel Establishment

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:
  1. Static: AC IP address list preconfigured on the APs
  2. 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.
  1. Data tunnel: transmits service data packets from APs to the AC for centralized forwarding.
  2. Control tunnel: transmits control packets between the AC and APs.

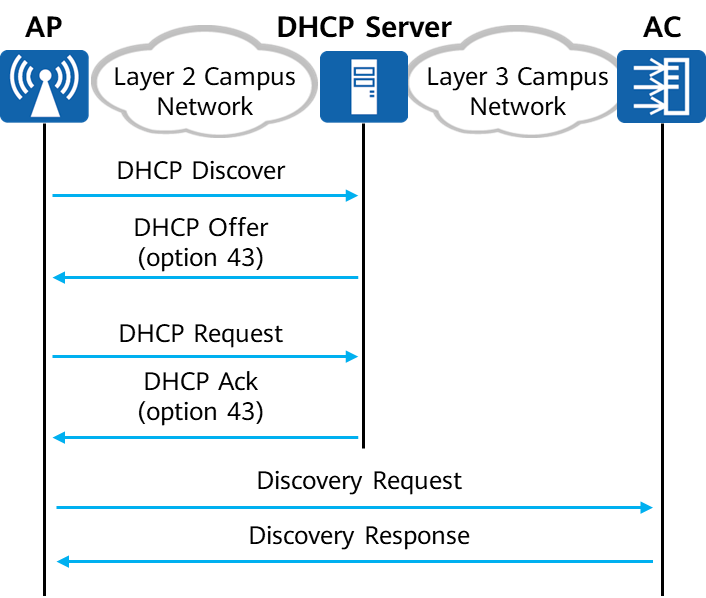
CAPWAP tunnels provide the following functions:

* Maintains the running status of the AC and APs.
* Allows the AC to manage APs and deliver configurations to APs.
* Transmits service data to the AC for centralized forwarding.

AC discovery phase:

* Static: An AC IP address list is preconfigured on the APs. When an AP goes online, the AP unicasts a Discovery Request packet to each AC whose IP address is specified in the preconfigured AC IP address list. After receiving the Discovery Request packet, the ACs send Discovery Response packets to the AP. The AP then selects an AC to establish a CAPWAP tunnel according to the received Discovery Request packets.
* Dynamic: DHCP, DNS, and broadcast. This course describes DHCP and broadcast modes.

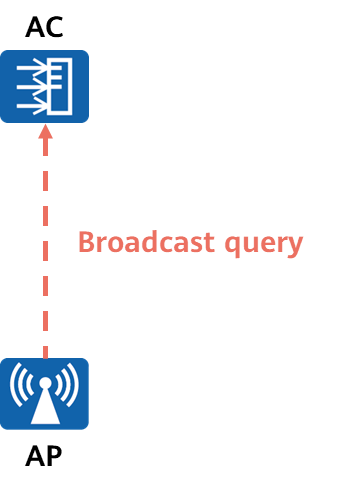
##### APs Dynamically Discover the AC



DHCP Mode (Layer 3 Networking)

In DHCP mode, AP obtain the AC IP address through a four-way DHCP handshake process.

* When no AC IP address list is preconfigured, the AP starts the dynamic AC auto-discovery process. The AP obtains an IP address through DHCP and the AC address list through the Option field in the DHCP packets. (The DHCP server is configured to carry Option 43 in the DHCP Offer packet, and Option 43 contains the AC IP address list.)
* First, the AP sends a DHCP Discover packet to the DHCP server in broadcast mode. When receiving the DHCP Discover packet, the DHCP server encapsulates the first free IP address and other TCP/IP configuration in a DHCP Offer packet containing the lease duration, and sends the packet to the AP.
* A DHCP Offer packet can be a unicast or broadcast packet. When the AP receives DHCP Offer packets from multiple DHCP servers, it selects only one DHCP Offer packet (usually the first DHCP Offer packet) and broadcasts a DHCP Request packet to all DHCP servers. Then, the AP sends a DHCP Request packet to the specified server from which will allocate an IP address.
* When the DHCP server receives the DHCP Request packet, it responds with a DHCP Ack packet, which contains the IP address for the AP, lease duration, gateway information, and DNS server IP address. By now, the lease contract takes effect and the DHCP four-way handshake is completed.
* The AC discovery mechanism allows APs to associate with the AC.
  1. After obtaining the AC's IP address from the DHCP server, the AP finds available ACs through the AC discovery mechanism and decides to associate with the optimal AC and establish CAPWAP tunnels.
  2. The AP starts the CAPWAP protocol discovery mechanism and sends unicast or broadcast request packets to attempt to associate with an AC. The ACs respond to the Discovery Request packets with unicast discovery response packets, containing the AC priority and the number of APs. The AP determines to associate with the appropriate AC based on the AC priority and the number of APs.

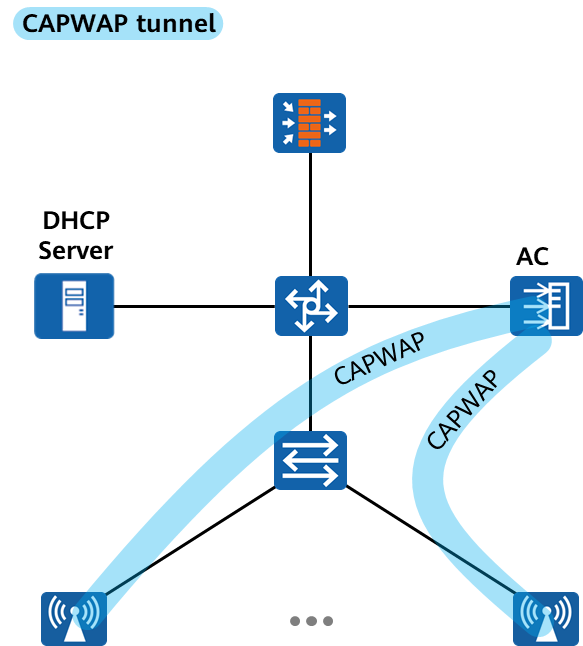


Broadcast Mode (Layer 2 Networking)

Broadcast mode:

* After an AP is started, if DHCP-based and DNS-based AC discovery procedures fail, the AP initiates a broadcast AC discovery procedure and broadcasts an AC discovery request.
* The AC receiving discovery request packets checks whether the AP is authorized to access (or whether the AP has authorized MAC addresses or sequence numbers). If so, the AC returns a discovery response to the AP. If not, the AC rejects its discovery request.
* Broadcast AC discovery is applicable to a Layer 2 network between the AP and the AC.

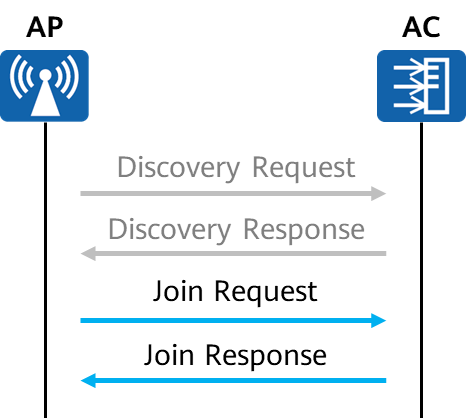
##### Establish CAPWAP Tunnel



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



Join process

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.

After receiving the Join Request packet from an AP, an AC authenticates the AP. If authentication is successful, the AC adds the AP.

The AC supports the following AP authentication modes:

* MAC address authentication
* SN authentication
* Non-authentication

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

* Manual configuration: Specify the MAC addresses and SNs of APs in offline mode on the AC in advance. When APs are connected the AC, the AC finds that their MAC addresses and SNs match the preconfigured ones and establish connections with them.
* Automatic discovery: If the AP authentication mode is set to non-authentication, or the AP authentication mode is set to MAC or SN authentication and the AP is whitelisted, the AC automatically discovers connected APs and establish connections with them.
* Manual confirmation: If the AP authentication mode is set to MAC or SN authentication and the AP is not imported offline or whitelisted, the AC adds the AP to the list of unauthorized APs. You can manually confirm the identity of such an AP to bring it online.

#### AP Upgrade(Optional)



Upgrade AP’s software by using image data packet

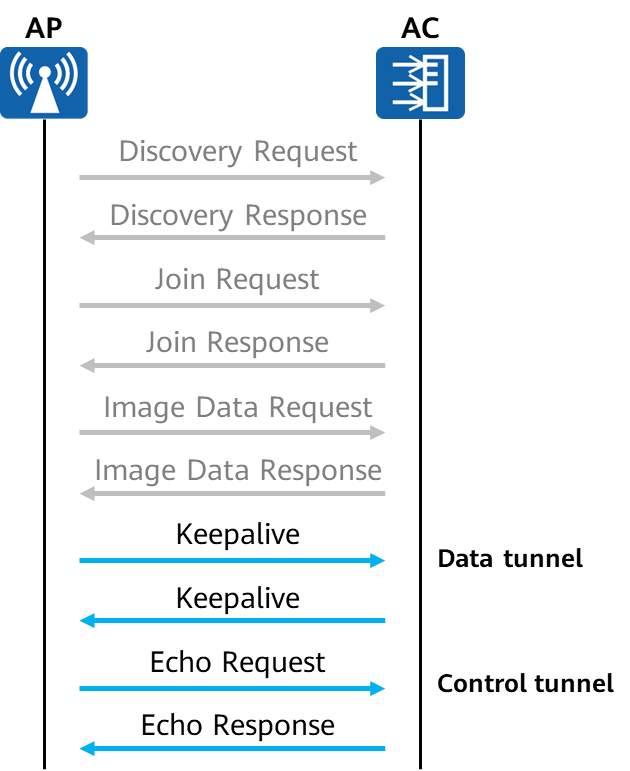
The AP determines whether its system software version is the same as that specified on the AC according to parameters in the received Join Response packet. If they are different, the AP sends an Image Data Request packet to request the software package and then upgrades its software version in AC, FTP,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

After the software version is updated, the AP restarts and repeats steps 1 to 3.

APs can be upgraded on an AC in the following modes:

* Automatic upgrade: mainly used when APs have not gone online on an AC. In this mode, we need to configure the automatic upgrade parameters for APs to go online before configuring AP access. Then the APs are automatically upgraded when they go online. An online AP will be automatically upgraded after the automatic upgrade parameters are configured and the AP is restarted in any mode. Compared with the automatic upgrade mode, the in-service upgrade mode reduces the service interruption time.
  1. AC mode: applies when a small number of APs are deployed. APs download the upgrade file from the AC during the upgrade.
  2. FTP mode: applies to file transfer without high network security requirements. APs download the upgrade file from an FTP server during the upgrade. In this mode, data is transmitted in clear text, which brings security risks.
  3. SFTP mode: applies to scenarios that require high network security and provides strict encryption and integrity protection for data transmission. APs download the upgrade file from an SFTP server during an upgrade.
* In-service upgrade: mainly used when APs are already online on the AC and carry WLAN services.
* Scheduled upgrade: mainly used when APs are already online on the AC and carry WLAN services. The scheduled upgrade is usually performed during off-peak hours.

#### CAPWAP Tunnel Maintenance



CAPWAP Tunnel 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.

#### 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.
* A regulatory domain profile provides configurations of the country code, calibration channel, and calibration bandwidth for an AP.
* 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. Correct country code configuration ensures that radio attributes of APs comply with local laws and regulations.

Configure a source interface or address(for establishing CAPWAP tunnels with APs):

* Specify a unique IP address, VLANIF interface, or Loopback interface on an AC. In this manner, APs connected to the AC can learn the specified IP address or the IP address of the specified interface to establish CAPWAP tunnels with the AC. This specified IP address or interface is called the source address or interface.
* Only after the unique source interface or address is specified on an AC, can APs establish CAPWAP tunnels with the AC.
* A VLANIF or Loopback interface can be used as the source interface, and their IP addresses can be configured as the source address.

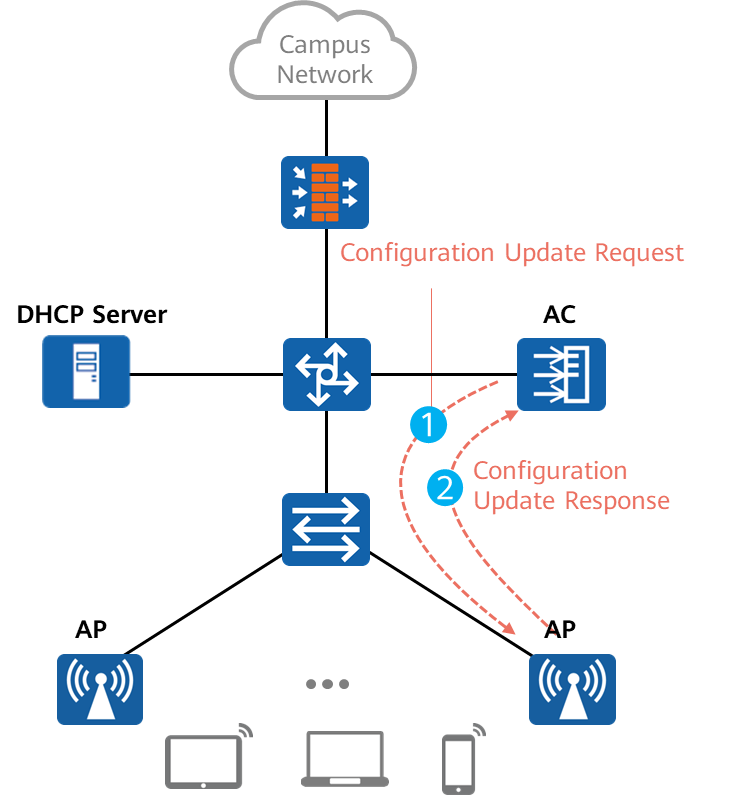
(Optional) Configure the automatic AP upgrade:

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



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.

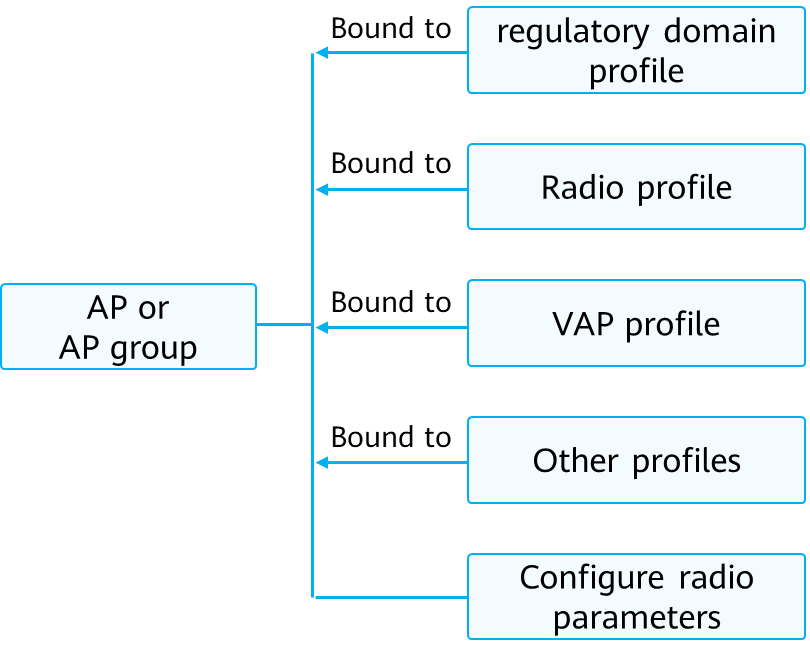
After an AP goes online, it sends a Configuration Status Request containing its running configuration to the AC. The AC then compares the AP's running configuration with the local AP configuration. If they are inconsistent, the AC sends a Configuration Status Response message to the AP.

Note: After an AP goes online, it obtains the existing configuration from the AC. The AC then manages the AP and delivers service configurations to the AP.

#### 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.

To simplify the configuration of a large number of APs, you can add them to an AP group and perform centralized configuration.However, APs may have different configurations. These configurations cannot be uniformly performed but can be directly performed on each AP.Each AP must and can only join one AP group when going online. If an AP obtains both AP group and specific configurations from an AC, the AP specific configurations are preferentially used.



WLAN Profiles

Various profiles can be bound to the AP group and AP: regulatory domain profile, radio profile, VAP profile, Location profile, AP system profile, WIDS profile, AP wired port profile, WDS profile, and Mesh profile. Some of the listed profiles can further reference other profiles.

Regulatory domain profile：

* A country code identifies the country to which AP radios belong. Different countries support different AP radio attributes, including the transmit power and supported channels. Correct country code configuration ensures that radio attributes of APs comply with laws and regulations of countries and regions to which the APs are delivered.
* A calibration channel set limits the dynamic AP channel adjustment range when the radio calibration function is configured. Radar channels and the channels that are not supported by STAs are avoided.

Radio profile

* You can adjust and optimize radio parameters to adapt to different network environments, enabling APs to provide required radio capabilities and improving signal quality of WLANs. After parameters in a radio profile are delivered to an AP, only the parameters supported by the AP can take effect.
* Parameters that can be configured include the radio type, radio rate, multicast rate of radio packets, and interval at which an AP sends Beacon frames.

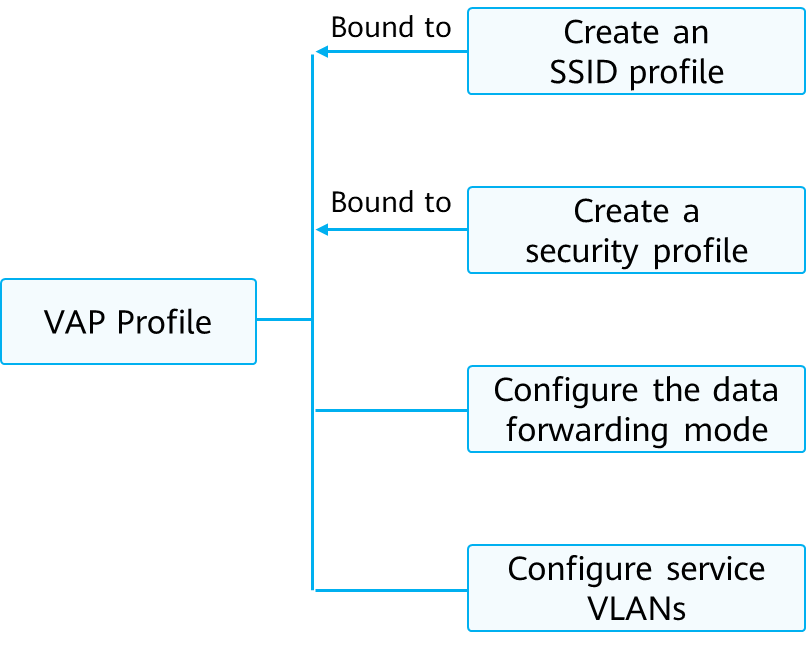
VAP profile

* After parameters in a VAP profile are configured, and the VAP profile is bound to an AP group or AP, virtual access points (VAPs) are created on APs. VAPs provide wireless access services for STAs. You can configure parameters in the VAP profile to enable APs to provide different wireless services.
* A VAP profile can also reference an SSID profile, a security profile, a traffic profile and etc.

Configure radio parameters:

* Configure different radio parameters for AP radios based on actual WLAN environments, so that the AP radios can work at the optimal performance.
* If working channels of adjacent APs have overlapping frequencies, signal interference occurs and affects AP working status. To prevent signal interference and enable APs to work at the optimal performance with higher WLAN quality, configure any two adjacent APs to work on non-overlapping channels.
* Configure the transmit power and antenna gain for radios according to actual network environments so that the radios provide sufficient signal strength, improving signal quality of WLANs.
* In actual application scenarios, two APs may be connected over dozens of meters to dozens of kilometers. Due to different AP distances, the time to wait for ACK packets from the peer AP varies. A proper timeout value can improve data transmission efficiency between APs.

#### VAP Profile



VAP Profile

An SSID profile is used to configure the SSID name and other access parameters of a WLAN. The following parameters are set in an SSID profile:

* SSID hiding: This functions enables an AP to hide the SSID of a WLAN. Only the users who know the SSID can connect to the WLAN, improving security.
* Maximum number of STAs on a VAP: More access users on a VAP indicate fewer network resources that are available to each user. To ensure Internet experience of users, you can configure a proper maximum number of access users on a VAP according to actual network situations.
* SSID hiding when the number of STAs reaches the maximum: When this function is enabled and the number of access users on a WLAN reaches the maximum, the SSID of the WLAN is hidden and new users cannot find the SSID.

Security profile: You can configure WLAN security policies to authenticate STAs and encrypt user packets, protecting the security of the WLAN and users.

* The supported WLAN security policies include open system authentication, WEP, WPA/WPA2-PSK, and WPA/WPA2-802.1X. You can configure one of them in a security profile.

Data forwarding mode:

* Control packets are forwarded through CAPWAP control tunnels. Data packets are forwarded in tunnel forwarding (centralized forwarding) or direct forwarding (local forwarding) mode. The data forwarding modes will be detailed later in the course.

Service VLAN:

* Since WLANs provide flexible access modes, STAs may connect to the same WLAN at the office entrance or stadium entrance, and then roam to different APs.
  1. If a single VLAN is configured as the service VLAN, IP address resources may become insufficient in areas where many STAs access the WLAN, and IP addresses in the other areas are wasted.
  2. After a VLAN pool is created, add multiple VLANs to the VLAN pool and configure the VLANs as service VLANs. In this way, an SSID can use multiple service VLANs to provide wireless access services. Newly connected STAs are dynamically assigned to VLANs in the VLAN pool, which reduces the number of STAs in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

### WLAN Working Process: Step 3

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
* user authentication

#### Scanning

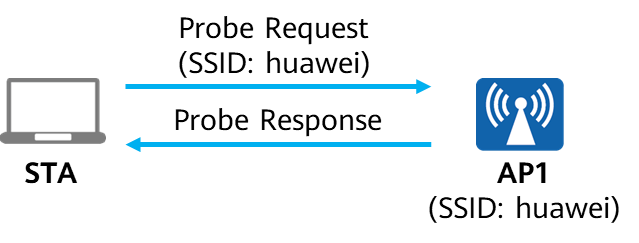
In active scanning, a STA periodically searches for nearby wireless networks.

The STA can send two types of Probe Request frames: probes containing an SSID and probes that do not contain an SSID.

Active scanning:

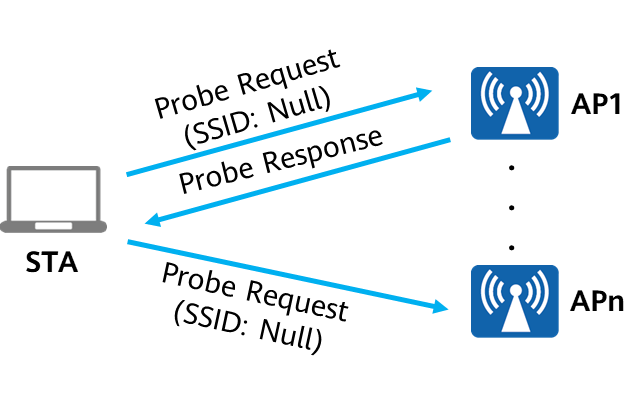
Probes containing an SSID: applies when a STA actively scans wireless networks to access a specified wireless network.

Probes that do not contain an SSID: applies when a STA actively scans wireless networks to determine whether wireless services are available.



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.



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.

Active scanning and passive scanning

* Active scanning
  1. Probes containing an SSID: applies when a STA actively scans wireless networks to access a specified wireless network.
  2. Probes that do not contain an SSID: applies when a STA actively scans wireless networks to determine whether wireless services are available.
* Passive scanning
  1. STAs can passively scan wireless networks.
  2. In passive scanning mode, a STA listens to Beacon frames (containing the SSID and supported rate) periodically sent by an AP to discover surrounding wireless networks. By default, an AP sends Beacon frames at an interval of 100 TUs (1 TU = 1024 us).

#### 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |

Common security policy

Three WLAN security policies are available: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2. Each security policy has a series of security mechanisms, including link authentication used to establish a wireless link, user authentication used when users attempt to connect to a wireless network, and data encryption used during data transmission.

WEP:

WEP, defined in IEEE 802.11, is used to protect data of authorized users from being intercepted during transmission on a WLAN. WEP uses the RC4 algorithm to encrypt data through a 64-bit, 128-bit, or 152-bit key. Each encryption key contains a 24-bit initialization vector (IV) generated by the system. Therefore, the length of the key configured on the WLAN server and client is 40 bits, 104 bits, or 128 bits. WEP uses a static encryption key. All STAs associating with the same SSID use the same key to connect to the WLAN.

WPA/WPA2:

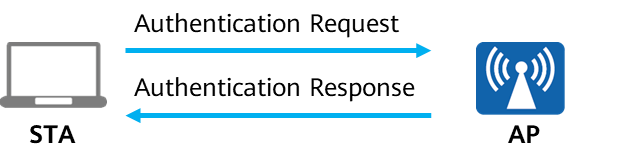
* WEP shared key authentication uses the Rivest Cipher 4 (RC4) symmetric stream cipher to encrypt data. Therefore, the same static key must be preconfigured on the server and clients. Both the encryption mechanism and algorithm, however, are prone to security threats. To address this challenge, the Wi-Fi Alliance developed WPA to overcome WEP defects. In addition to the RC4 algorithm, WPA defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm on the basis of WEP, uses the 802.1X identity authentication framework, and supports Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) and EAP-Transport Layer Security (EAP-TLS) authentication. Later, 802.11i defined WPA2. WPA2 uses a more secure encryption algorithm, that is, Counter Mode with CBC-MAC Protocol (CCMP).
* Both WPA and WPA2 can use 802.1X access authentication and the TKIP or CCMP encryption algorithm, giving better compatibility. WPA and WPA2 provide almost the same security level, with the only difference being the protocol packet format.
* The WPA/WPA2 security policy involves four phases: link authentication, access authentication, key negotiation, and data encryption.

#### Link Authentication

To ensure wireless link security, an AP needs to authenticate STAs that attempt to access the AP.

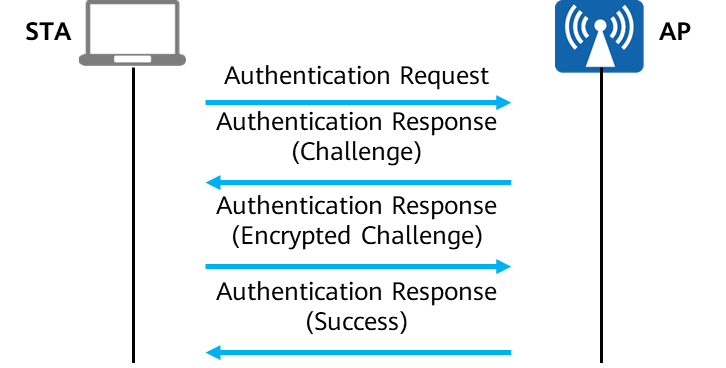
A WLAN needs to ensure validity and security of STA access. To achieve this, STAs need to be authenticated before accessing the WLAN. This process is known as link authentication, which is usually considered the beginning of STA access.

IEEE 802.11 defines two authentication modes: open system authentication and shared key 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.

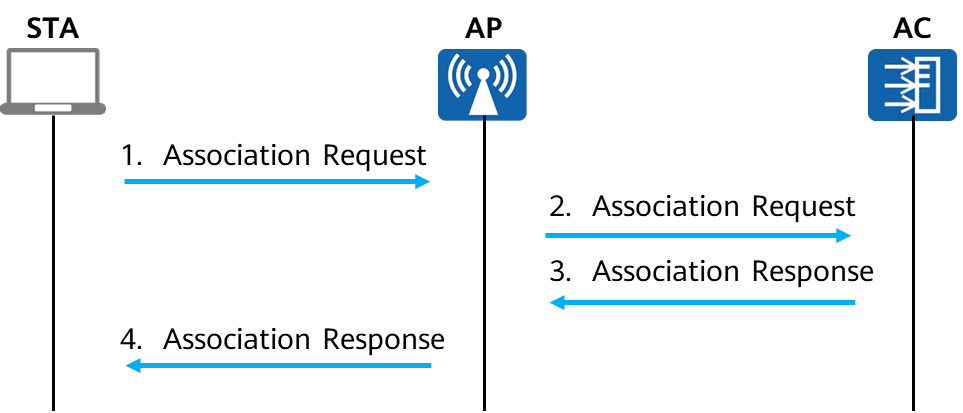
Shared key authentication:

* The same shared key is configured for STAs and APs in advance. The AP checks whether the STA has the same shared key during link authentication. If so, the STA is successfully authenticated. Otherwise, STA authentication fails.
* Authentication process:
  1. The STA sends an Authentication Request packet to the AP.
  2. The AP generates a challenge and sends it to the STA.
  3. The STA uses the preconfigured key to encrypt the challenge and sends the encrypted challenge to the AP.
  4. The AP uses the preconfigured key to decrypt the encrypted challenge and compares the decrypted challenge with the challenge sent to the STA. If the two challenges are the same, the STA is successfully 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.



Association

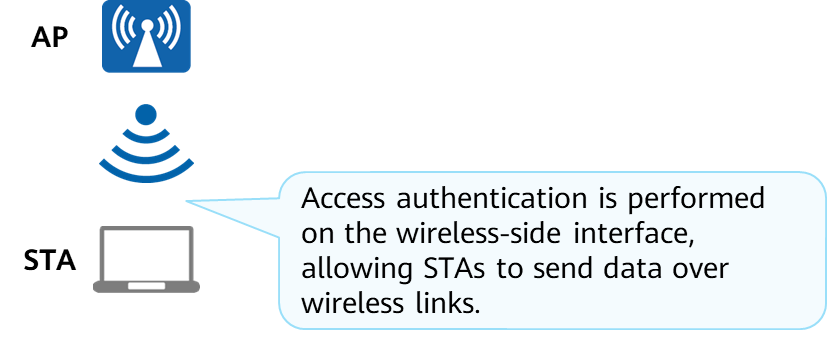
STA association in the Fit AP architecture consists of the following steps:

* The STA sends an Association Request packet to the AP. The Association Request packet carries the STA's parameters and the parameters selected by the STA according to the service configuration, including the transmission rate, channel, and QoS capabilities.
* After receiving the Association Request packet, the AP encapsulates the packet into a CAPWAP packet and sends the CAPWAP packet to the AC.
* The AC determines whether to permit the STA access according to the received Association Request packet and replies with a CAPWAP packet containing an Association Response.
* The AP decapsulates the CAPWAP packet to obtain the Association Response, and sends the Association Response to the STA.

#### 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.



Access Authentication

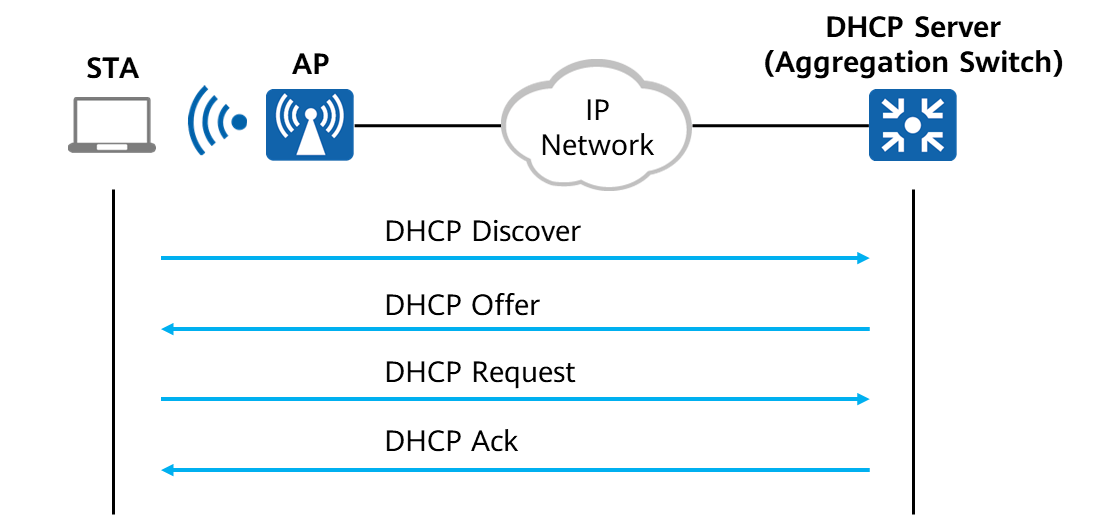
Data encryption:

In addition to user access authentication, data packets need to be encrypted to ensure data security, which is also implemented in the access authentication phase. After a data packet is encrypted, only the device that holds the key can decrypt the packet. Other devices cannot decrypt the packet even if they receive the packet because they do not have the corresponding key.

#### STA Address Allocation

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.



STA Address Allocation

#### User Authentication

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

With the application and development of enterprise networks, threats increasingly bring risks, such as viruses, Trojan horses, spyware, and malicious network attacks. On a traditional enterprise network, the intranet is considered secure and threats come from the extranet. However, research shows that 80% of cyber security vulnerabilities come from inside the network. The network security threats and viruses affect the network seriously, leading to system or network crashes. In addition, when intranet users browse websites on the external network, the spyware and Trojan horse software may be automatically installed on users' computers, which cannot be sensed by the users. The malicious software may spread on the intranet.

Therefore, as security challenges keep escalating, traditional security measures are far from enough. The security model needs to be changed from the passive mode to active mode. Thoroughly solving network security problems from the root (terminal) can improve the information security level of the entire enterprise.

Portal Authentication:

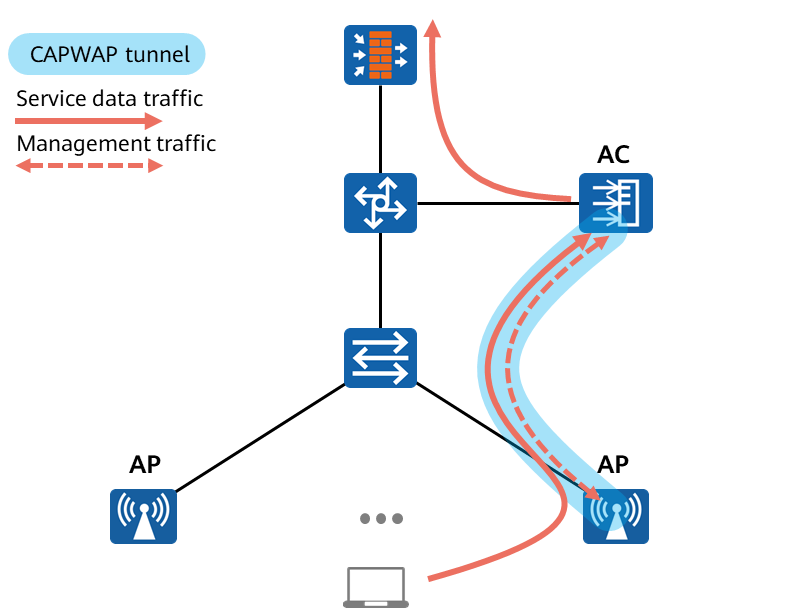
* Portal authentication is also known as web authentication. Portal authentication websites are referred to as web portals.
* To access the Internet, users must be authenticated on web portals. The users can access network resources only after successful authentication.

### WLAN Working Process: Step 4

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

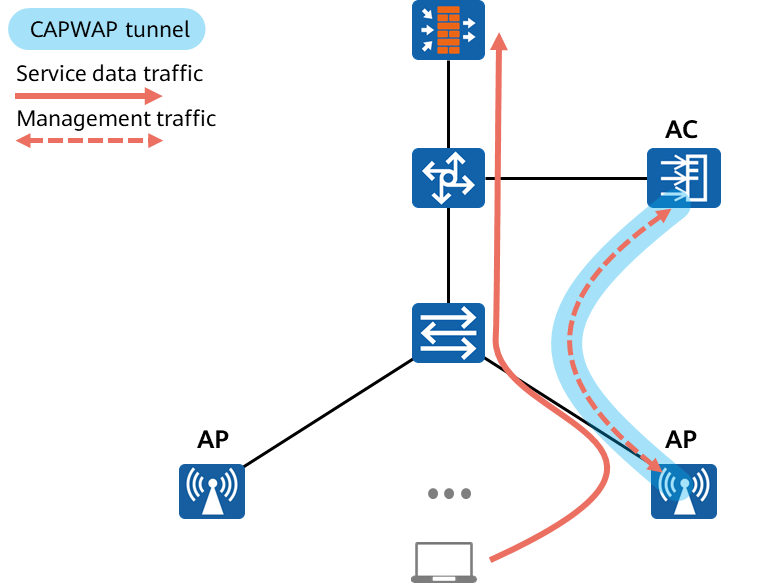


Tunnel Forwarding

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.

Advantages of tunnel mode: An AC forwards all data packets, ensuring security and facilitating centralized management and control.

Disadvantages of tunnel mode: Service data must be forwarded by an AC, which is inefficient and increases the load on the AC.



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.

Advantages of direct mode: Service data packets do not need to be forwarded by an AC, improving packet forwarding efficiency and reducing the burden on the AC.

Disadvantages of direct mode: Service data is difficult to manage and control in a centralized manner.

## WLAN Configuration Implementation

### Basic WLAN Configuration Commands: Configuring an AP to Go Online

* 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*

*code*: specifies the code of a user-defined option. The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 121 and 184.

**sub-option** *sub-code*: specifies the code of a user-defined sub-option. The value is an integer ranging from 1 to 254. For details about well-known options, see RFC 2132.

**ascii** | **hex** | **cipher**: specifies the user-defined option code as an ASCII character string, hexadecimal character string, or ciphertext character string.

**ip-address** *ip-address*: specifies the user-defined option code as an IP address.

* 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.

**name** *profile-name*: specifies the name of a regulatory domain profile. The value is a string of 1 to 35 case-insensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

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

Configure the country code.

**country-code**: specifies a country code. The value is a string of characters in enumerated type.

The AC supports multiple country codes, such as:

CN (default value): China

AU: Australia

CA: Canada

DE: Germany

FR: France

US: United States

...

[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.

**name** *group-name*: specifies the name of an AP group. The value is a string of 1 to 35 characters. It cannot contain question marks (?), slashes (/), or spaces, and cannot start or end with double quotation marks (").

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

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

* 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.

* 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.

**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* } ]

* 1. *ap-id*: specifies the ID of an AP. The value is an integer that ranges from 0 to 8191.
  2. *type-id:* specifies the ID of an AP type. The value is an integer that ranges from 0 to 255.
  3. *ap-type*: specifies the type of an AP. The value is a string of 1 to 31 characters.
  4. *ap-mac:* specifies the MAC address of an AP. The value is in H-H-H format. An H is a 4-digit hexadecimal number.
  5. *ap-sn:* specifies the SN of an AP. The value is a string of 1 to 31 characters, and can contain only letters and digits.

[AC-wlan-view] **ap-id** *0*

[AC-wlan-ap-0] **ap-group** *ap-group*

Add the AP to an AP group.

* Verify the configuration.

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

Check AP information.

### Basic WLAN Configuration Commands: Configuring Radios

* Enter the radio view.

[AC-wlan-view] **ap-id** *0*

[AC-wlan-ap-0] **radio** *radio-id*

[AC-wlan-radio-0]

radio-id: specifies the ID of a radio. The radio ID must exist.

* Configure the working bandwidth and channel for a radio.

[AC-wlan-radio-0/0] **channel** { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** | **160mhz** } *channel*

[AC-wlan-radio-0/0] **channel 80+80mhz** *channel1 channel2*

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

**channel { 20mhz | 40mhz-minus | 40mhz-plus | 80mhz | 160mhz }** *channel*

**channel 80+80mhz** *channel1 channel2*

**20mhz**: sets the working bandwidth of a radio to 20 MHz.

**40mhz-minus:** sets the working bandwidth of a radio to 40 MHz Minus.

**40mhz-plus:** sets the working bandwidth of a radio to 40 MHz Plus.

**80mhz:** sets the working bandwidth of a radio to 80 MHz.

**160mhz:** sets the working bandwidth of a radio to 160 MHz.

**80+80mhz:** sets the working bandwidth of a radio to 80+80 MHz.

*channel/channel1/channel2:* specifies the working channel for a radio. The channel is selected based on the country code and radio mode. The parameter is an enumeration value. The value range is determined according to the country code and radio mode.

* 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.

**antenna-gain**: specifies the antenna gain. The value is an integer that ranges from 0 to 30, in dB.

* 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.

**eirp**: specifies the transmit power. The value is an integer that ranges from 1 to 127, in dBm.

* 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.

**distance**: specifies the radio coverage distance. Each distance corresponds to a group of slottime, acktimeout, and ctstimeout values. You can configure the radio coverage distance based on the AP distance, so that APs adjust the values of slottime, acktimeout, and ctstimeout values accordingly. The value is an integer that 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.

[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.

**name** *profile-name*: specifies the name of a 2G radio profile. The value is a string of 1 to 35 case-insensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

By default, the system provides the 2G radio profile default.

* 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.

**profile-name**: specifies the name of a 2G radio profile. The 2G radio profile must exist.

**radio** *radio-id*: specifies the ID of a radio. The value is an integer that can be 0 or 2.

**radio all**: specifies all radios.

### Basic WLAN Configuration Commands: Configuring VAPs

* 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.

* 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.

* 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.

* 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.

* 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.

**ssid**: specifies an SSID. The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters.

To start an SSID with a space, you need to encompass the SSID with double quotation marks ("), for example, " hello". The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, \"hello. The backslash occupies one character.

[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* }

Display information about service VAPs.

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

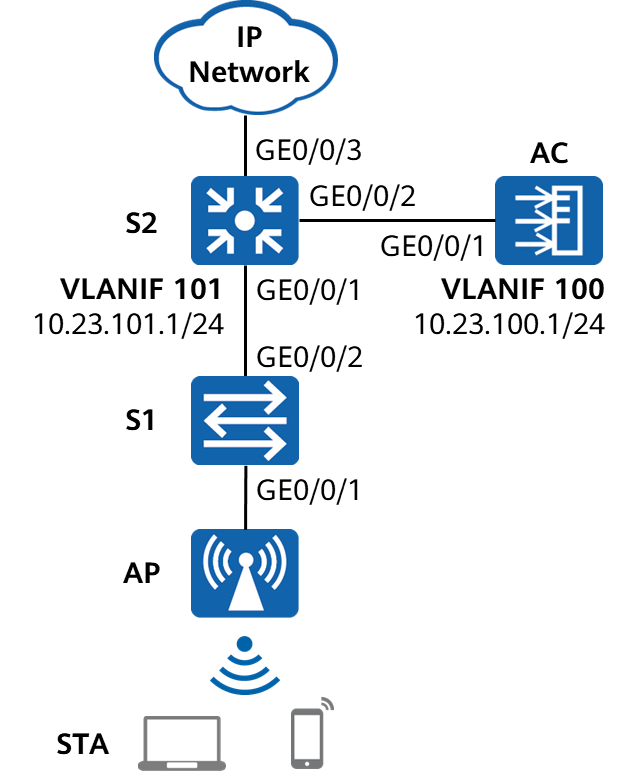


Diagram of example

|  |  |
| --- | --- |
| **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** |

Schedule of example

Service requirements:

An enterprise wants to enable users to access the Internet through a WLAN, meeting the basic mobile office requirements.

Networking requirements

* AC networking mode: Layer 2 networking in off-path mode
* DHCP deployment mode:
  + 1. The AC functions as a DHCP server to assign IP addresses to APs.
    2. The aggregation switch S2 functions as a DHCP server to assign IP addresses to STAs.
* Service data forwarding mode: tunnel forwarding

Configuration roadmap

* Configure network connectivity between the AC, APs, and other network devices.
* Configure the APs to go online.

1. Create an AP group and add APs that require the same configuration to the group for unified configuration.
2. Configure AC system parameters, including the country code and source interface used by the AC to communicate with the APs.
3. Configure the AP authentication mode and imports the APs in offline mode for them to go online.

* Configure WLAN service parameters for STAs to access the WLAN.

### Configuring Network Connectivity

Create VLANs and interfaces on S1, S2, and AC.

* S1 configuration:

[S1] vlan batch 100

[S1] interface gigabitethernet 0/0/1

[S1-GigabitEthernet0/0/1] port link-type trunk

[S1-GigabitEthernet0/0/1] port trunk pvid vlan 100

[S1-GigabitEthernet0/0/1] port trunk allow-pass vlan 100

[S1-GigabitEthernet0/0/1] quit

[S1] interface gigabitethernet 0/0/2

[S1-GigabitEthernet0/0/2] port link-type trunk

[S1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100

[S1-GigabitEthernet0/0/2] quit

* S2 configuration:

[S2] vlan batch 100 101

[S2] interface gigabitethernet 0/0/1

[S2-GigabitEthernet0/0/1] port link-type trunk

[S2-GigabitEthernet0/0/1] port trunk allow-pass vlan 100

[S2-GigabitEthernet0/0/1] quit

[S2] interface gigabitethernet 0/0/2

[S2-GigabitEthernet0/0/2] port link-type trunk

[S2-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 101

[S2-GigabitEthernet0/0/2] quit

[S2] interface gigabitethernet 0/0/3

[S2-GigabitEthernet0/0/3] port link-type trunk

[S2-GigabitEthernet0/0/3] port trunk allow-pass vlan 101

[S2-GigabitEthernet0/0/3] quit

* AC configuration:

[AC] vlan batch 100 101

[AC] interface gigabitethernet 0/0/1

[AC-GigabitEthernet0/0/1] port link-type trunk

[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101

[AC-GigabitEthernet0/0/1] quit

### Configuring APs to Go Online

* Create an AP group.

[AC] wlan

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

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

* 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

* Configure the AC's source interface.

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

* 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

Description of the **display ap** command output:

* ID: AP ID.
* MAC: AP MAC address.
* Name: AP name.
* Group: Name of the AP group to which an AP belongs.
* IP: IP address of an AP. In NAT scenarios, APs are on the private network and the AC on the public network. This value is an AP's private IP address. To check the public IP address of an AP, run the **display ap run-info** command.
* Type: AP type.
* State: AP state.
  1. normal: An AP has gone online on an AC and is working properly.
  2. commit-failed: WLAN service configurations fail to be delivered to an AP after it goes online on an AC.
  3. download: An AP is in upgrade state.
  4. fault: An AP fails to go online.
  5. idle: It is the initialization state of an AP before it establishes a link with the AC for the first time.
* STA: Number of STAs connected to an AP.
* Uptime: Online duration of an AP.
* ExtraInfo: Extra information. The value P indicates an AP has no sufficient power supply.

### Configuring WLAN Service Parameters

* 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

* 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

* 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

* 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

Description of the **display vap** command output:

* AP ID: AP ID.
* AP name: AP name.
* RfID: Radio ID.
* WID: VAP ID.
* SSID: SSID name.
* BSSID: MAC address of a VAP.
* Status: Current status of a VAP.
  1. ON: The VAP service is enabled.
  2. OFF: The VAP service is disabled.
* Auth type: VAP authentication mode.
* STA: Number of STAs connected to a VAP.

## Next-Generation WLAN Solutions

### 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

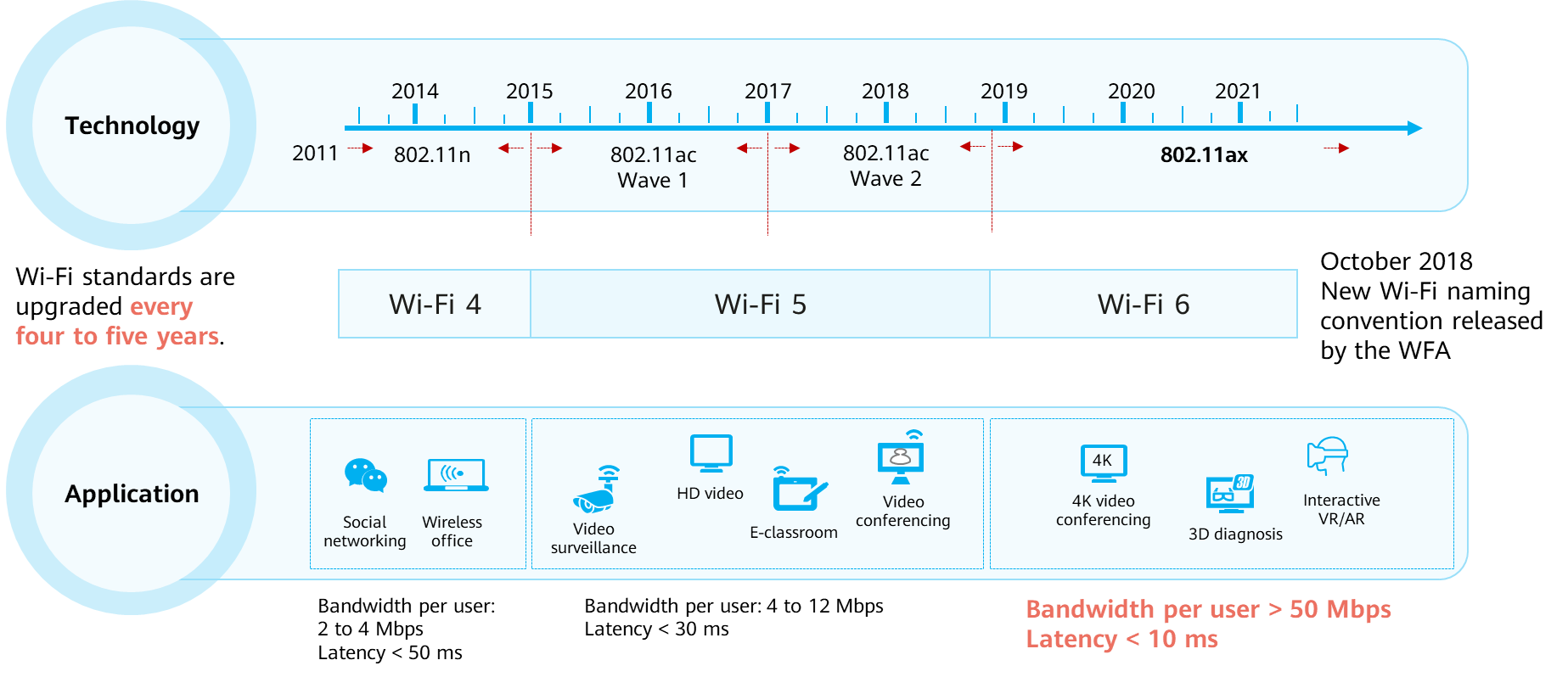
Easy deployment:

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

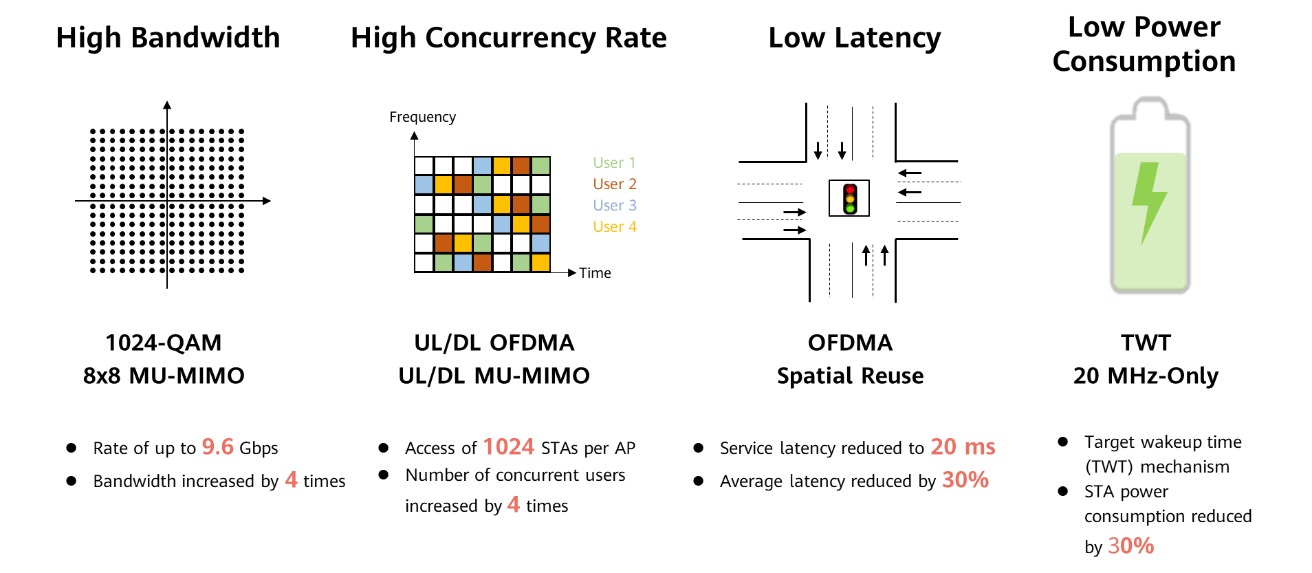


WI-FI 6

Wi-Fi 5 cannot meet the low service latency and high bandwidth requirements of 4K/8K video conferencing scenarios.

Powered by Huawei SmartRadio intelligent application acceleration, Wi-Fi 6 achieves a latency of as low as 10 ms.

### Wi-Fi 6 Vs. Wi-Fi 5



Wi-Fi 6 Vs. Wi-Fi 5

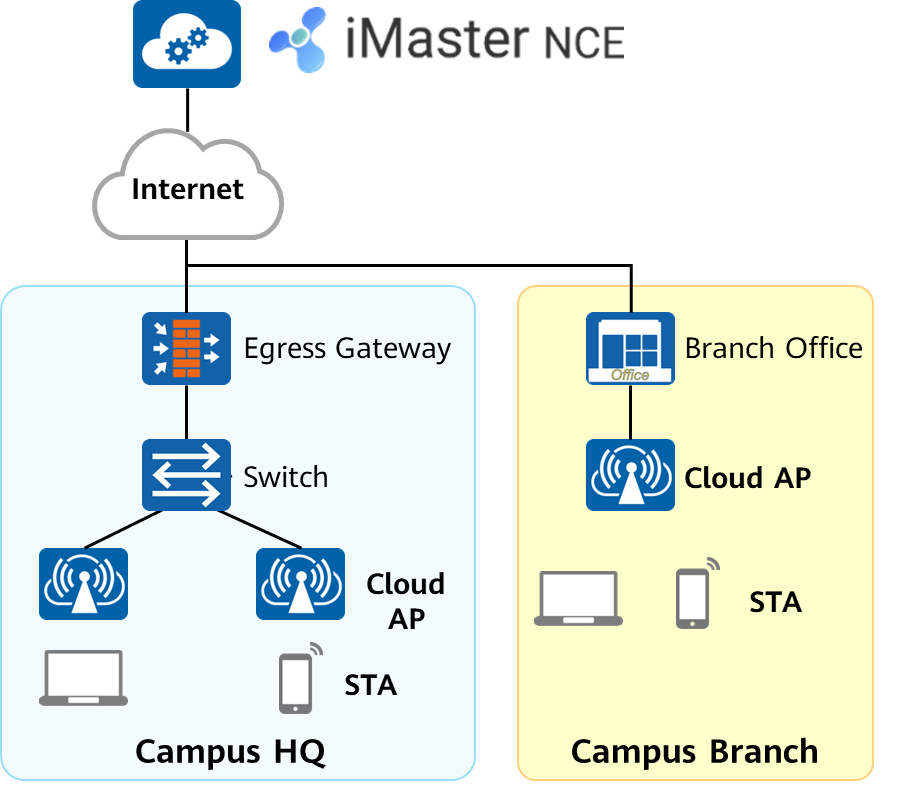
Currently, the theoretical rate of all Wi-Fi 5 products (Wave 2) is 2.5 Gbit/s, and that of Wi-Fi 6 products is 9.6 Gbit/s. Therefore, Wi-Fi 6 increases the rate by four folds compared with Wi-Fi 5.

Wi-Fi 6 increases the number of concurrent users by four folds compared with Wi-Fi 5. In the actual test, at a per user bandwidth of 2 Mbit/s, the concurrent number of users supported by Wi-Fi 5 is 100, and that supported by Wi-Fi 6 is 400.

The average latency supported by Wi-Fi 6 is about 20 ms (about 30 ms in Wi-Fi 5). Huawei SmartRadio intelligent application acceleration technology further reduces the service latency to as low as 10 ms.

TWT is not supported by Wi-Fi 5.

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



Next generation campus network(Small- and Medium-Sized)

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.

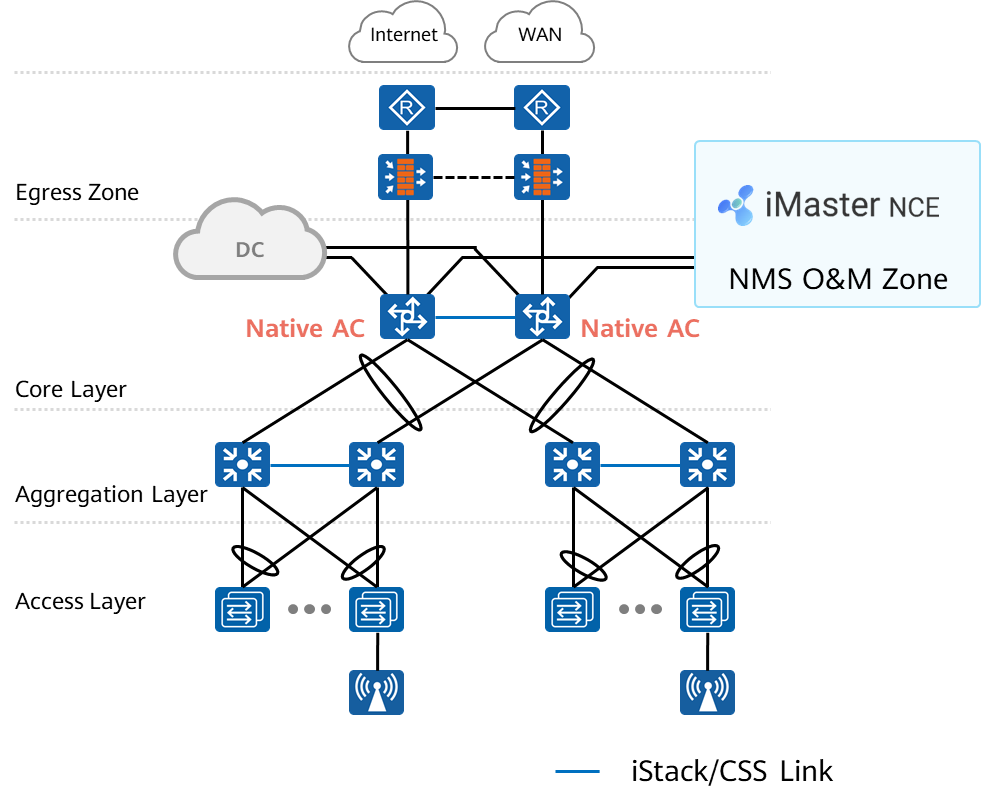
Disadvantages of traditional network solutions:

Traditional network solutions have many network deployment problems, such as high deployment costs and O&M difficulties. These problems are obvious in enterprises with many branches or geographically dispersed branches.

Cloud management architecture:

* The cloud management architecture can solve the problems faced by traditional network solutions. The cloud management platform can manage and maintain devices in a centralized manner at any place, greatly reducing network deployment and O&M costs.
* After a cloud AP is deployed, the network administrator does not need to go to the site for cloud AP software commissioning. After power-on, the cloud AP automatically connects to the specified cloud management platform to load system files such as the configuration file, software package, and patch file. In this manner, the cloud AP can go online with zero touch configuration. The network administrator can deliver configurations to the cloud APs through the cloud management platform at anytime and anywhere, facilitating batch service configurations.

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



Next generation campus network(Medium- and Large-Sized)

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

## 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.

## Quiz

1. (Multiple) Which of the following methods are supported by Fit APs to discover an AC? ( )
2. Static discovery
3. Dynamic discovery through DHCP
4. Dynamic discovery through FTP
5. Dynamic discovery through DNS
6. (Single) What is the roaming scenario when a user roams between different subnets of the same AC? ( )
7. Intra-AC Layer 2 roaming
8. Intra-AC Layer 3 roaming
9. Inter-AC Layer 2 roaming
10. Inter-AC Layer 3 roaming
11. (Single) Which of the following VLANs is configured in a VAP profile to transmit user Internet access data? ( )
12. Management VLAN
13. Service VLAN
14. User VLAN
15. Guest VLAN
16. (Multiple) When deploying APs on multiple floors of a building, you need to pay attention to the following factors: ( )
17. Wall material
18. Other interference signals
19. To ensure good appearance, the AP should be hidden in the ceiling.
20. Unified channel planning
21. (True or False) To facilitate management, STAs connected to the WLAN can only automatically obtain IP addresses using DHCP. ( )
22. True
23. False
24. (True or False) WLAN architectures include controller-based Fit AP architecture and traditional independent Fat AP architecture. ( )
25. True
26. False
27. What are the advantages and disadvantages of in-path and off-path networking modes?