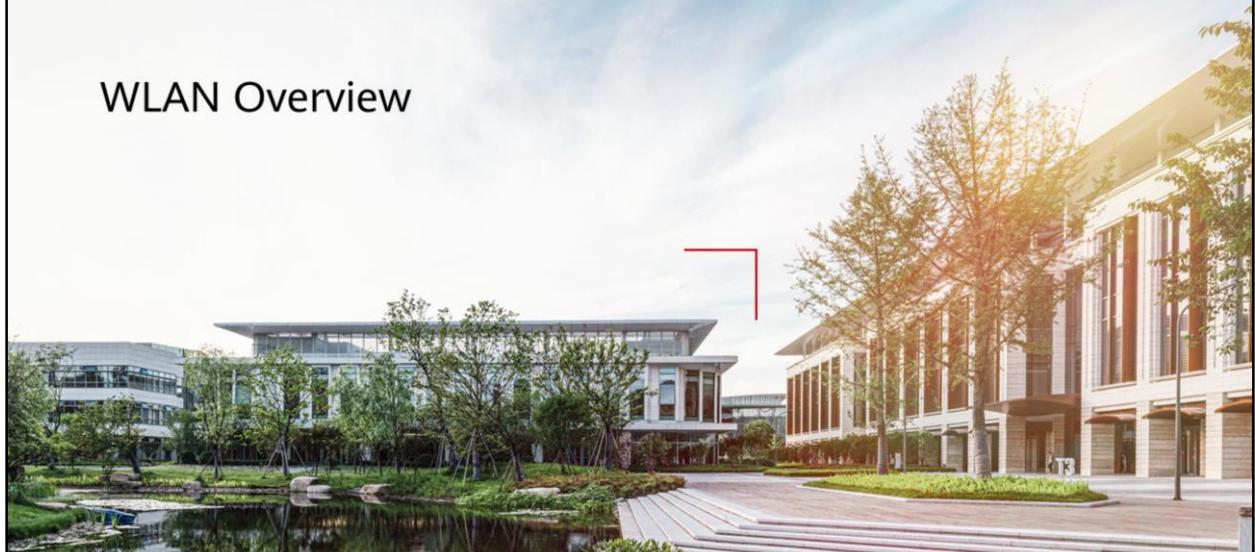


WLAN Overview



Foreword

- Wired LANs use wired cables or optical fibers as transmission media, which are expensive and lack mobility. As further emphasis is placed on network portability and mobility, traditional wired LANs cannot meet users' requirements. This leads to the development of wireless LANs (WLAN).
- WLAN is now the most cost-efficient and convenient network access mode.
- This course describes the basic concepts, development history, and standards organizations of WLAN. It also illustrates the changes and challenges facing WLAN, as well as the development trend of WLAN technologies.

Objectives

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

- Describe the basic concepts and development history of WLAN.
- Describe the functions of various WLAN standards organizations.
- Compare WLAN and Wi-Fi.
- Describe typical application scenarios of WLAN technologies.
- Illustrate the challenges and development trend of WLAN.

Contents

- 1. Enterprise WLAN Overview**
2. Challenges Faced by Enterprise WLAN
3. Next-Generation Enterprise WLAN Solution

What Is WLAN?

- A Wireless Local Area Network (WLAN) is constructed using wireless technologies.
- Wireless technologies mentioned here include not only Wi-Fi, but also infrared, Bluetooth, and ZigBee. WLAN technology allows you to easily access a wireless network and move around within the coverage of the wireless network.
- Wireless networks can fall into WPAN, WLAN, WMAN, and WWAN based on the application scope.

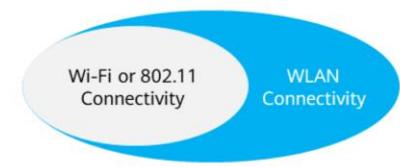


- Wireless Personal Area Networks (WPANs) provide wireless connections in personal areas, which are generally point-to-point connections and small-scale network connections.
 - Features: easy-to-use, low-cost, and portable
 - Main technologies: Bluetooth, ZigBee, and Near Field Communication (NFC), working at the 2.4 GHz frequency band
 - ZigBee applies to low-speed and low-power wireless networks, such as sensor networks and wireless meter reading networks, as well as to smart toys, smart homes, and smart agriculture.
 - NFC is a short-distance high-frequency wireless communication technology. Devices that use the NFC technology (such as smartphones) can exchange data when they are close to each other.
- Wireless Local Area Networks (WLANs) use 2.4 GHz and 5 GHz frequency bands.
 - High energy consumption
 - Support for multiple users; flexible design
 - Main technologies: 802.11n/ac/ax
- Wireless Metropolitan Area Networks (WMANs) are mainly used for backbone network coverage.
 - Frequencies must be applied before the WMAN is used. Public frequencies are

acceptable but vulnerable to interference.

- Main technologies: WiMax (802.16)

WLAN vs. Wi-Fi

| WLAN | Wi-Fi |
|--|---|
|  <p>WLAN is a combination of computer networks and wireless communication technologies. It is an extension of wired networks. Wireless connections facilitate network construction and allow users to move around without interrupting communication.</p> <p>The difference between Wi-Fi and WLAN is that IEEE 802.11 is a WLAN standard while Wi-Fi is an implementation of IEEE 802.11 standard.</p> |  <p>Wi-Fi is a trademark of the Wi-Fi Alliance. It is a WLAN technology based on the IEEE 802.11 standard.</p> |

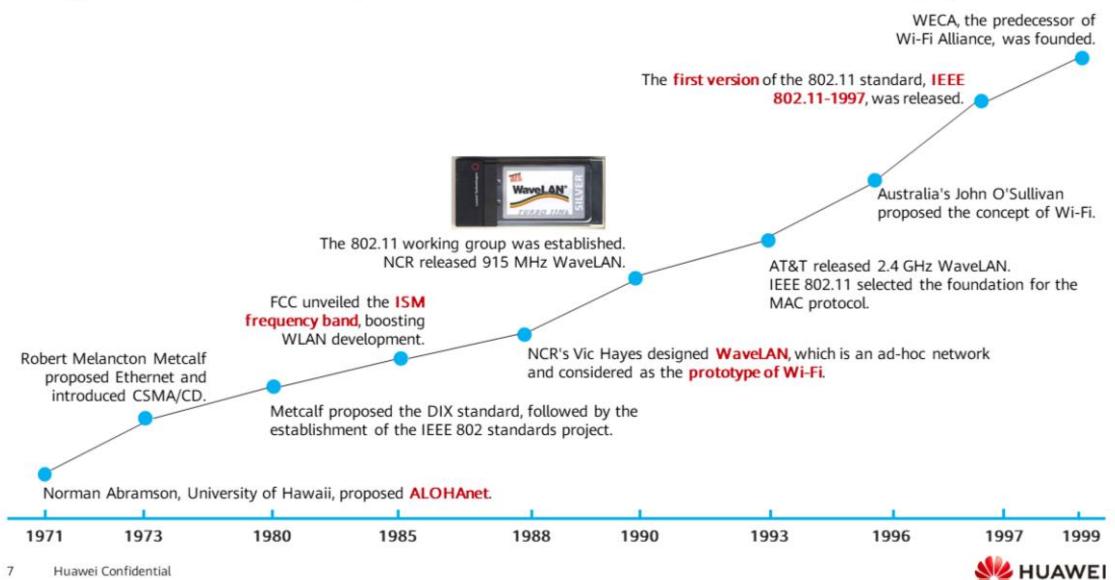
6

Huawei Confidential



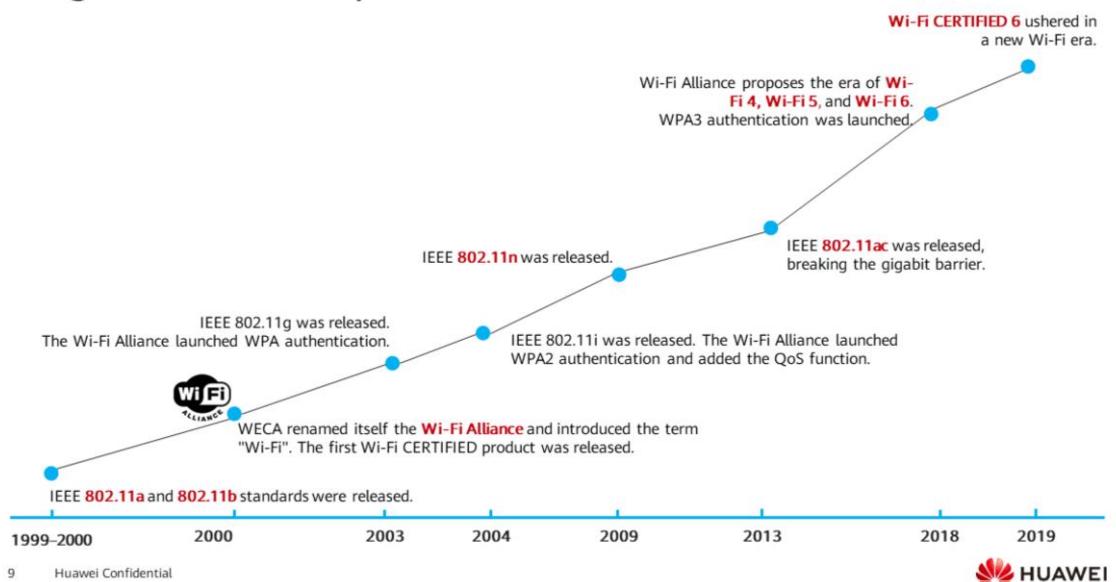
- The term Wi-Fi suggests Wireless Fidelity, resembling the long-established audio-equipment classification term Hi-Fi (used since 1950) or high fidelity (in use since the 1930s). Even the Wi-Fi Alliance itself has often used the phrase Wireless Fidelity in its press releases and documents; the term also appears in a white paper on Wi-Fi from ITAA. In fact, the word Wi-Fi is meaningless and not written in its entirety. If you ask a common user what an 802.11 wireless network is, they may be confused, as most people are used to calling it Wi-Fi. Wi-Fi is a market term, and people around the world use "Wi-Fi" as a synonym for 802.11 wireless network.
- In 1999, several visionary companies formed the Wireless Ethernet Compatibility Alliance (WECA), a global nonprofit association that aims to deliver the best user experience with a new wireless network technology, regardless of brand. In 2000, the WECA adopted the term "Wi-Fi" as its proprietary name for its technical work and announced its official name: Wi-Fi Alliance.
- Wi-Fi products are rigorously tested by independent Authorized Test Laboratories of the Wi-Fi Alliance. When a product successfully passes testing, the manufacturer or vendor is granted the right to use the Wi-Fi logo, Wi-Fi CERTIFIED logo, and related trademarks. The Wi-Fi Alliance uses the term "Wi-Fi CERTIFIED" to refer to these certified products. Certification means that a product has been tested in numerous configurations with a diverse sampling of other devices to validate interoperability with other Wi-Fi CERTIFIED equipment operating in the same frequency band.

Origin and Development of Wireless Networks (1)



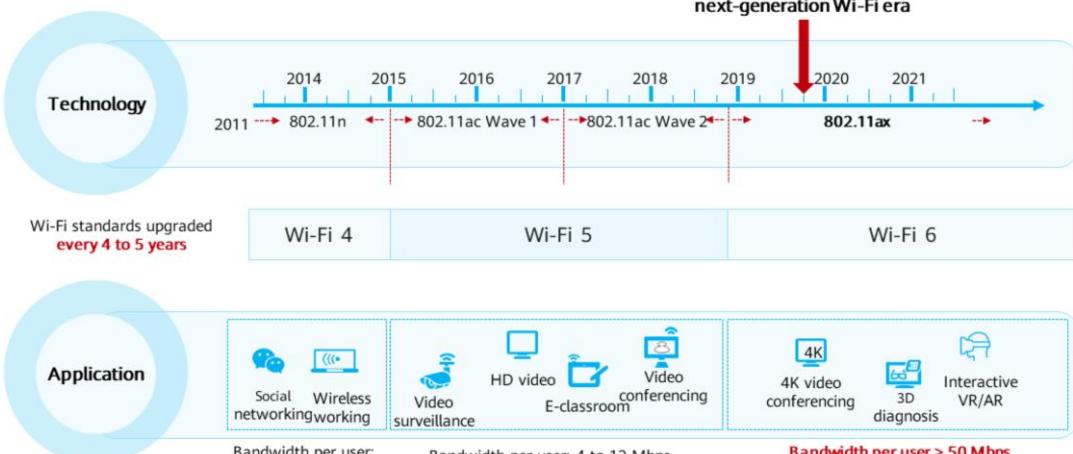
- Wireless networks adopt wireless network technologies defined by IEEE. When IEEE officially defined the 802.11 standard in 1999, it selected and determined that the wireless network technology invented by CSIRO is the best one in the world. Therefore, the wireless network technology standard of CSIRO became the core technical standard of Wi-Fi in 2010.
- The initial use of wireless networks can be traced back to World War II, when the U.S. Army used radio signals for data transmission. They developed a radio transmission technology, used together with a fairly high-intensity encryption technology, which was widely used by the U.S. and Allied forces. They may not have thought that this radio transmission technology would change our lives today.
- Many scholars took inspiration from this, and in 1971, researchers at the University of Hawaii created the first radio communications network based on encapsulation technology. This network, known as AlohaNet, is a fairly early WLAN. It consists of seven computers that span four Hawaiian islands in a two-way star topology, with the central computer on Oahu. Since then, wireless networks have been born.
- In 1990, the IEEE officially initiated the IEEE 802.11 project, and wireless network technologies gradually became mature. Since the birth of the IEEE 802.11 (Wi-Fi) standard, there have been 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11h, 802.11i, 802.11j, 802.11n, 802.11ac, and 802.11ax. 802.11ax (Wi-Fi 6) has been designed and launched to deliver high-speed, high-quality WLAN services for users.
- In 1993, AT&T released the 2.4 GHz WaveLAN, which provides a rate of 2 Mbps, and completed the first large-scale installation of WaveLAN at Carnegie Mellon University. In the same year, IEEE 802.11 selected the basis of the MAC protocol from the NCR, Symbol Technologies, and Xircom proposals.

Origin and Development of Wireless Networks (2)



- Wi-Fi is based on the IEEE 802.11 standard. In 2018, the Wi-Fi Alliance launched the "Generational Wi-Fi" marketing program. Based on major Wi-Fi technology (PHY) versions, the Wi-Fi Alliance introduced consumer-friendly Wi-Fi generation names (formatted as "Wi-Fi" followed by an integer) and encouraged people to use these Wi-Fi generation names in industry terminology. Generation names do not affect the previous certification program names. For previous certification programs (such as Wi-Fi CERTIFIED ac or earlier programs), the original certification program names continue to be used. Wi-Fi Alliance has not assigned new names to Wi-Fi generations prior to Wi-Fi 4.

Technology and Application Development Ushers in the Wi-Fi 6 Era



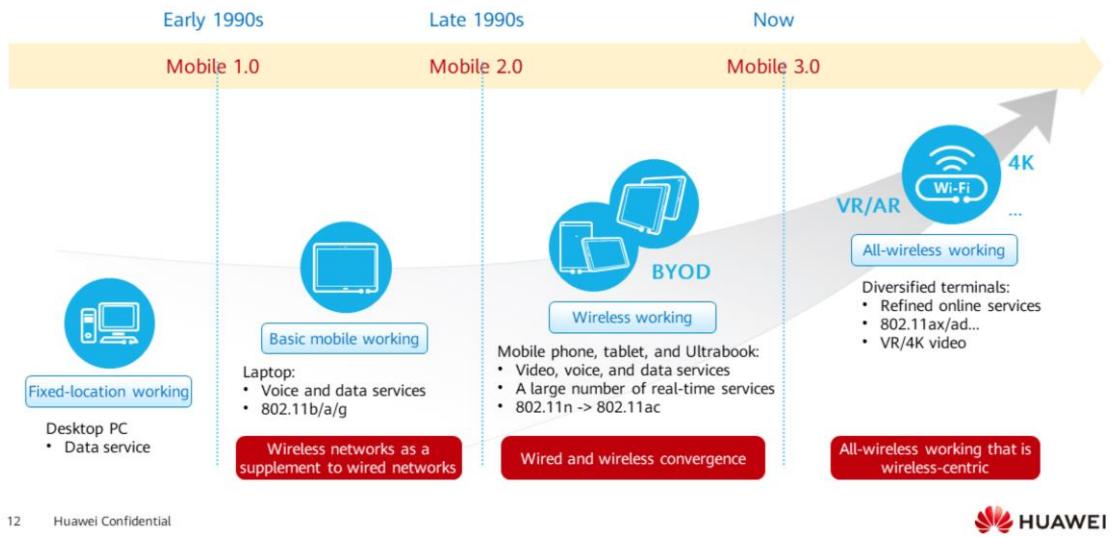
- Wi-Fi 5 cannot meet the requirements of low service latency and high bandwidth in 4K/8K video conferencing scenarios.
- Wi-Fi 6 works with Huawei SmartRadio technology to reduce the latency to 10 ms.

IEEE 802.11 Standards and Wi-Fi Generations

| Wi-Fi Generation | 802.11 Standard | Released In | Working Band | Theoretical Rate |
|------------------|-----------------|-------------|------------------|------------------|
| - | 802.11 | 1997 | 2.4 GHz | 2 Mbps |
| - | 802.11b | 1999 | 2.4 GHz | 11 Mbps |
| - | 802.11a | 1999 | 5 GHz | 54 Mbps |
| | 802.11g | 2003 | 2.4 GHz | 54 Mbps |
| Wi-Fi 4 | 802.11n | 2009 | 2.4 GHz or 5 GHz | 600 Mbps |
| Wi-Fi 5 | 802.11ac Wave 1 | 2013 | 5 GHz | 3.47 Gbps |
| | 802.11ac Wave 2 | 2015 | 5 GHz | 6.9 Gbps |
| Wi-Fi 6 | 802.11ax | 2018/19 | 2.4 GHz or 5 GHz | 9.6 Gbps |

- The original version of IEEE 802.11 was released in 1997 and defined the MAC and PHY layers of WLAN traffic.
- Since then, more and more 802.11-based supplementary standards have been defined. The most well-known standards that affect Wi-Fi evolution include 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

Development Trend of Wi-Fi in Enterprise Working Scenarios



- Phase 1: In the era of basic mobile working, wireless networks were a supplement to wired networks.
 - The application of WaveLAN technology is considered as the earliest form of enterprise WLAN. The Wi-Fi technology at an early stage was mainly used on IoT devices such as wireless radios. However, with the introduction of 802.11a/b/g standards, the advantages of wireless connectivity become more obvious. Enterprises and consumers began to realize the potential of Wi-Fi, and wireless hotspots emerged in coffee shops, airports, and hotels.
 - Wi-Fi was also born during this period. It is a trademark of the Wi-Fi Alliance and was created to drive the formulation of the 802.11b standard and compatibility certification of Wi-Fi products worldwide. With the evolution of standards and the popularity of standards-compliant products, people often equate Wi-Fi with the 802.11 standard.
 - 802.11 is only one of many WLAN technologies and has become a mainstream technology widely adopted in the industry. Therefore, when people talk about WLAN, they usually refer to WLAN that uses Wi-Fi technology.
 - This was the first phase of WLAN application, focusing mainly on implementing wireless access. Its key value is to break away from the constraints of wired networks so that devices can move within a certain range, that is, using wireless networks to extend wired networks. However, in this phase, there were no specific requirements on WLAN's security, capacity, and roaming performance. And an access point, or AP, was used independently for networking coverage. Such an AP

is called a Fat AP.

Contents

1. Enterprise WLAN Overview
- 2. Challenges Faced by Enterprise WLAN**
3. Next-Generation Enterprise WLAN Solution

Challenge 1: Diversified Wi-Fi Deployment Scenarios

| Differentiated Indoor Coverage Scenarios | High-density Stadium Coverage | Wi-Fi & IoT Convergence | Outdoor Coverage | Backhaul and Coverage In Rail Transportation |
|---|--|--|---|--|
| <ul style="list-style-type: none">Scenarios such as offices, shopping malls, and supermarkets vary greatly, and one single solution cannot adapt to such scenarios. | <ul style="list-style-type: none">Up to 80,000 users20,000 concurrent usersDifficult planning and installation | <ul style="list-style-type: none">Independent deployment of IoT networks increases costs.Wi-Fi and IoT networks are managed separately, complicating maintenance. | <ul style="list-style-type: none">High reliability and stability are required in high-temperature and rainy outdoor environments. | <ul style="list-style-type: none">120 km/h fast handover in rail transportationHigh-density coverage in carriages |



Challenge 2: Wi-Fi Technology Bottlenecks Degrade User Experience

- Good signal quality does not mean that all STAs can access the WLAN.



Some STAs fail to access the WLAN because the number of STAs connected to the WLAN is too large.

- Access success does not necessarily mean good user experience.



Rich media content is developing rapidly, and severe wireless network interference exists, increasing service delay.

- Good experience does not mean consistent experience.



Campus 1



Campus 2



Branch 1

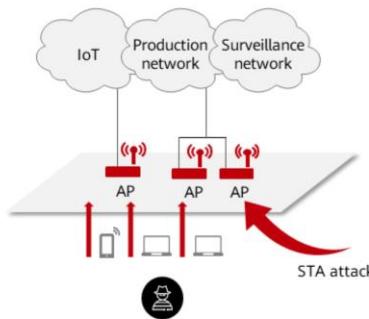


Users cannot obtain consistent service quality assurance.

Challenge 3: The Security of Wi-Fi Services Is Questioned

The wireless channel becomes an important way for hackers and illegals to attack and destroy networks in the mobile era.

Losses and damages caused by attacks on IoT, production, and other services will be catastrophic.



Challenge 4: Planning, Deployment, and Maintenance Become Complex Due to the Increase of Wi-Fi Nodes

1

Doubled planning difficulty

Difficult to evaluate signal strength and radio interference



- Device deployment?
- Interference shielding?
- Channel allocation?
- ...
- Wired connection?
- Bandwidth allocation?
- ...

2

Complex Wi-Fi deployment

SSID, security, authentication, traffic, application...

- Sharp increase in Wi-Fi devices
- More parameters
- Independent wired and wireless networks
- ...

3

Device monitoring failing to guide service optimization

User- and service-oriented KPI monitoring provides guidance for network optimization.

- Signal coverage
- Radio interference
- User bandwidth
- Application throughput
- Enable 5G-prior?
- Adjust the bandwidth policy?
- Adjust the threshold?
- Adjust the application policy?



4

Difficult to locate Wi-Fi faults

Imagine your home's wireless network goes down...

- STA settings
- Radio interference
- Incorrect policy
- Authentication failure
- ...

- Planning

- Experience is required, and many factors need to be considered, such as channel planning based on the field strength, interference, user quantity, wall structure, mounting mode (wall-mounted or ceiling-mounted), etc.
- It is difficult to verify the effect after manual planning, for example, whether the planned signals can completely cover desired areas.

- Deployment

- The efficiency in deploying a large number of devices is low.
- There are too many commands, and configuration items and procedures are prone to errors.

- Monitoring

- There are many network KPIs, such as the CPU usage, memory usage, bandwidth usage, number of access users, access rate, signal strength, and signal-to-noise ratio (SNR). If you only view KPI data, network optimization cannot be performed.

- Fault diagnosis

- Using traditional ways to troubleshoot a large number of fault points is inefficient. We need to find out how to quickly locate and rectify faults.

Contents

1. Enterprise WLAN Overview
2. Challenges Faced by Enterprise WLAN
- 3. Next-Generation Enterprise WLAN Solution**

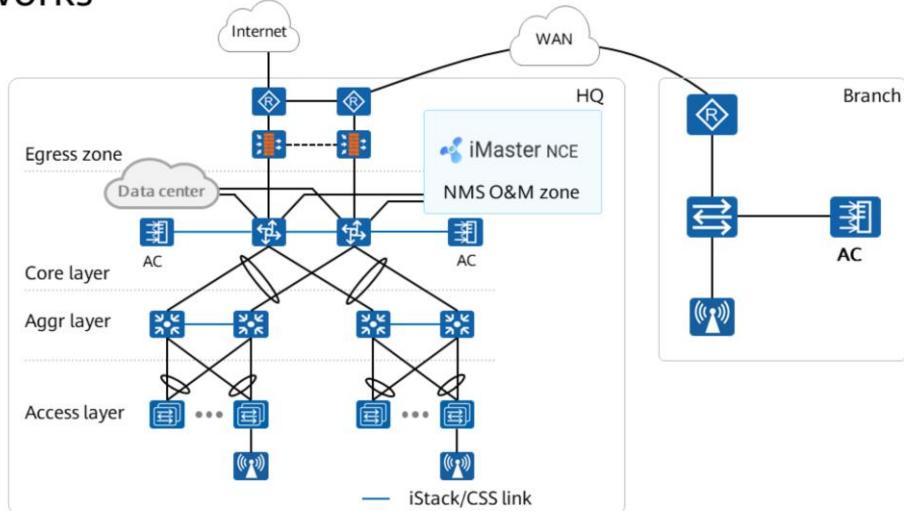
Next-Generation Enterprise WLAN Solution

| Support for 802.11ax | | | |
|--|--|---|---|
| Wireless air interface technology | Security technology | Network planning, deployment, and maintenance | Wi-Fi & IoT convergence |
| <ul style="list-style-type: none">• Wireless coverage: radio calibration.• Anti-interference: CCA, RTS-CTS, advanced antenna technologies.• User QoS: air interface priority scheduling, airtime scheduling.• Mobile experience: fast roaming, smart roaming. | <ul style="list-style-type: none">• Air interface attack defense• Data encryption• Diversified wireless authentication modes | <ul style="list-style-type: none">• All-scenario WLAN planning solution• Multiple tools for network planning and maintenance | <ul style="list-style-type: none">• IoT AP integrated with Bluetooth technology• IoT AP integrated with RFID technology• IoT AP integrated with ZigBee technology |

Features of Huawei WLAN Solution

| | |
|-----------------------------|---|
| All-scenario support | <ul style="list-style-type: none">Scenario-specific solutions for complex and diversified application scenariosComplete WLAN deployment and management schemes for campus and branch networks |
| High bandwidth | <ul style="list-style-type: none">802.11ac Wave 2 support: dual-5G radio coverage; maximum wireless access bandwidth of 6.9 GbpsHuawei takes the lead in formulating the next-generation 802.11ax standard (Wi-Fi 6), with 9.6 Gbps rate per 5 GHz radio.Wireless roaming and multiple wireless QoS protocols such as WMM to ensure service quality |
| High security | <ul style="list-style-type: none">Mainstream authentication/encryption modes, such as WPA, WPA2, WPA3, and WAPIWireless intrusion detectionPortal and 802.1X authentication, protecting intranet security |
| Easy deployment | <ul style="list-style-type: none">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 simplify installation and enable fast deployment.APs can smoothly switch between the cloud and local management modes. |

WLAN Networking Solution for Large-Scale Campus Networks



22 Huawei Confidential

HUAWEI

- If a wireless network needs to be deployed independently on a campus network where a wired network has been deployed or the wireless network scale is large, it is recommended that an independent AC be deployed.
- On a large campus network, ACs are typically connected to aggregation or core switches in off-path mode.
- Tunnel forwarding is recommended in this scenario to reduce changes to the existing wired network and facilitate centralized management and control on the AC. To improve AC reliability, VRRP hot standby is usually deployed in the independent AC solution.

Quiz

1. (Multiple-Answer Question) Based on the application scope, wireless networks can fall into:
 - A. WPAN
 - B. WLAN
 - C. WMAN
 - D. WWAN
2. (Multiple-Answer Question) Which of the following are characteristics of Huawei WLAN solution?
 - A. All-scenario support
 - B. High bandwidth
 - C. High security
 - D. Easy deployment

- ABCD
- ABCD

Summary

- Driven by rapid development of standards and accompanied by an explosive growth of diversified scenarios, enterprise WLANs have evolved from wired networks to all-wireless office networks. Requirements for services carried on such networks go beyond just Internet access. Enterprise WLANs have become the infrastructure that supports digital transformation across various industries while improving production and work efficiency. The challenges faced by enterprise WLANs are even more daunting.
- After learning about the challenges facing WLANs and related solutions, you can work out effective measures to plan, design, and deploy WLANs that meet your needs.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors
that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



Enterprise WLAN Basics



Foreword

- The wireless local area network (WLAN), as a wireless communication technology, transmits information in space by using electromagnetic waves, like radio stations.
- 802.11 was originally a WLAN communication standard defined by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. The IEEE then made amendments to the standard, forming the 802.11 family, including 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i, 802.11n, 802.11ac, and 802.11ax.
- This course describes the concepts of wireless communication, key WLAN technologies, 802.11 protocols, and Wi-Fi 6 technologies.

Objectives

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

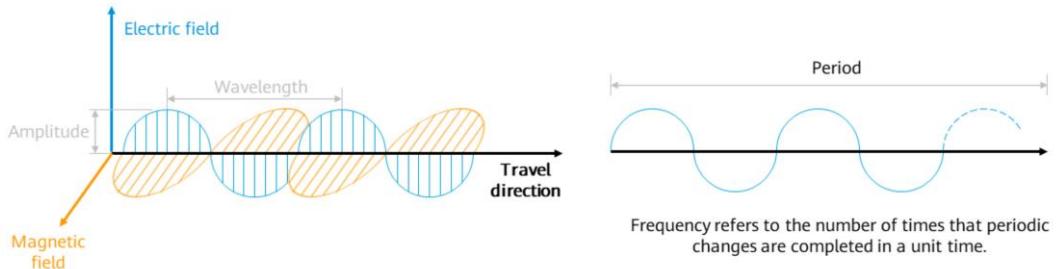
- Describe basic concepts of wireless communication.
- Distinguish 802.11 protocols and describe Wi-Fi generations.
- Describe the highlights of Wi-Fi 6.
- Describe key WLAN technologies.

Contents

- 1. Basic Concepts of Wireless Communication**
2. Introduction to 802.11 Standards
3. Key WLAN Technologies

Radio Wave

- Radio waves are a type of electromagnetic waves.
- Electromagnetic waves (namely, electromagnetic radiation) are synchronized oscillations of electric and magnetic fields, which are perpendicular to each other. Electromagnetic waves travel through space at the speed of light to transmit energy in a direction perpendicular to the electric and magnetic fields.

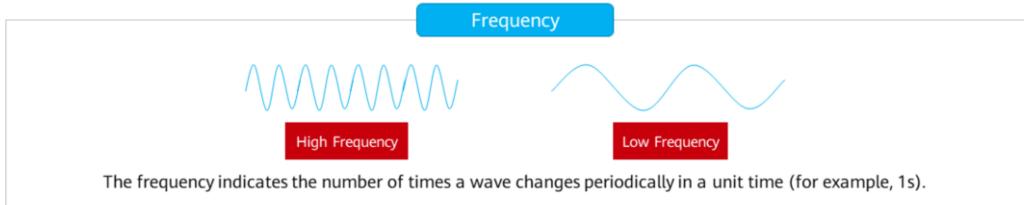


31 Huawei Confidential

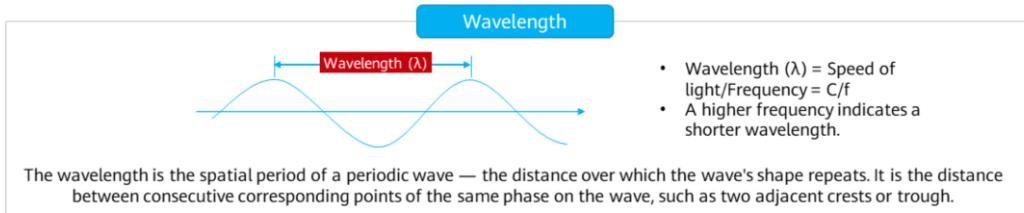
 HUAWEI

- Electromagnetic radiation consists of electromagnetic waves, which are synchronized oscillations of electric and magnetic fields perpendicular to each other. Electromagnetic waves travel through space to transmit energy in a direction perpendicular to the electric and magnetic fields.
- Radio waves are electromagnetic waves emitted in the free space (including air and vacuum), with frequencies lower than 300 GHz. (The lowest frequencies are different. The commonly used lowest frequencies are 3 kHz to 300 GHz, 9 kHz to 300 GHz, and 10 kHz to 300 GHz.)
- The current change in a conductor generates radio waves. Therefore, information can be carried by radio waves through modulation. When an electromagnetic wave reaches the receiver, the electromagnetic field change caused by the electromagnetic wave generates current. Information can be extracted from current through demodulation. Information is thus transmitted.

Radio Frequency and Wavelength



The frequency indicates the number of times a wave changes periodically in a unit time (for example, 1s).

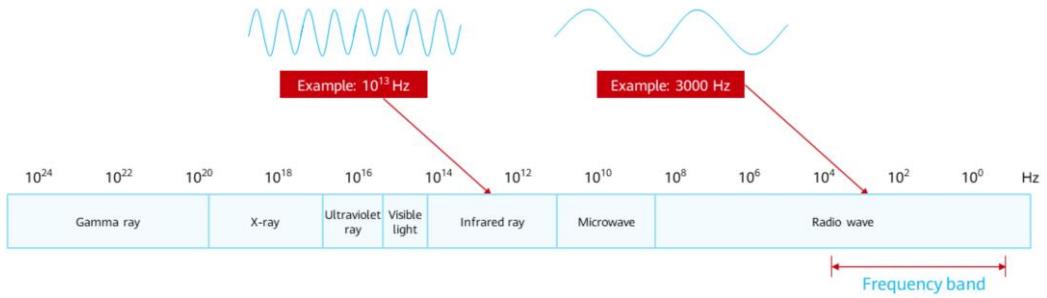


- Wavelength (λ) = Speed of light/Frequency = C/f
- A higher frequency indicates a shorter wavelength.

The wavelength is the spatial period of a periodic wave — the distance over which the wave's shape repeats. It is the distance between consecutive corresponding points of the same phase on the wave, such as two adjacent crests or troughs.

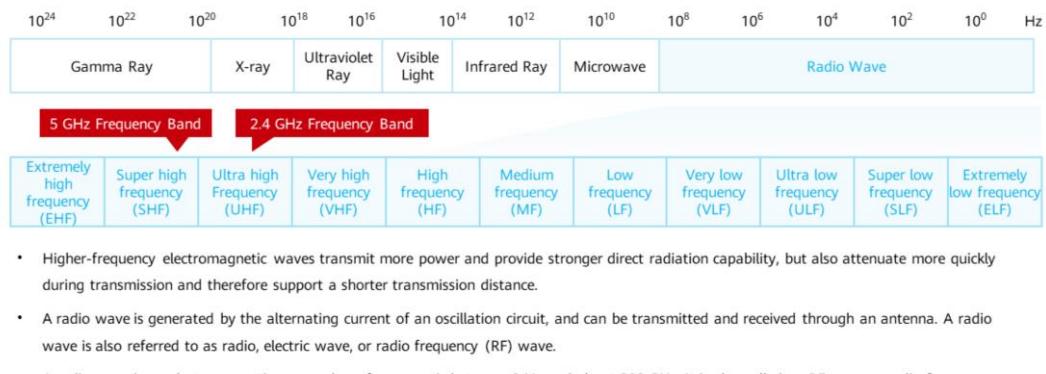
- The frequency is an important physical index of waves. The frequency of a wave is the oscillation frequency of the wave, which is expressed in Hz. If a wave oscillates once per second, the frequency is 1 Hz.
- A wave consists of consecutive crests and troughs. The distance between adjacent crests or troughs is the wavelength. Waves vary in size from very long radio waves (as long as a football field) to very short gamma-rays (shorter than the radius of an atom). A higher frequency indicates a shorter wavelength.
- The frequency of radio waves ranges from 3 kHz to 300 GHz, and the wavelength ranges from 0.1 mm to 10 km.

Frequency and Frequency Band



- The frequency distribution is the spectrum. The figure above shows the electromagnetic wave spectrum, which is arranged in descending order of frequency from left to right.
- The frequency range of a radio wave is referred to as a frequency band.
- WLANs use radio waves.

Electromagnetic Wave Spectrum and Radio Wave



34 Huawei Confidential

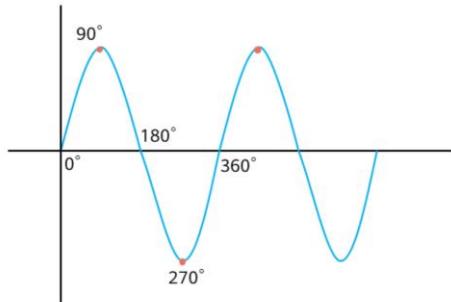
HUAWEI

- WLANs use the 2.4 GHz frequency band (2.4–2.4835 GHz) and 5 GHz frequency band (5.15–5.35 GHz and 5.725–5.85 GHz).
- Designed for Industrial, Scientific, and Medical (ISM), the 2.4 GHz and 5 GHz frequency bands can be used without licenses or fees as long as the transmit power requirement (generally less than 1 W) is met and no interference is caused to other frequency bands. The free frequency band resources reduce WLAN deployment costs but cause co-channel interference when multiple wireless communication technologies work on the same frequency band. The frequency bands to be used by WLANs must comply with local laws and regulations.
- ELF (3 Hz to 30 Hz): Submarine communication or direct conversion into sound
- SLF (30 Hz to 300 Hz): Direct conversion into sound or AC power transmission system (50 Hz to 60 Hz)
- ULF (300 Hz to 3 kHz): Mine communication or direct conversion into sound
- VLF (3 kHz to 30 kHz): Direct conversion into sound, ultrasound, and geophysics research
- LF (30 kHz to 300 kHz): International broadcasting
- MF (300 kHz to 3 MHz): Amplitude Modulation (AM) broadcasting, maritime, and aeronautical communication
- HF (3 MHz to 30 MHz): Short wave and civil radio stations
- VHF (30 MHz to 300 MHz): Frequency Modulation (FM) radio, TV broadcast, and aeronautical communication
- UHF (300 MHz to 3 GHz): TV broadcasting, wireless telephone communication, wireless network, and microwave oven
- SHF (3 GHz to 30 GHz): Wireless network, radar, and satellite receiving
- EHF (30 GHz to 300 GHz): Radio astronomy, remote sensing, and human body scanner

- 300 GHz or higher: Infrared ray, visible light, ultraviolet ray, and other rays

Phase of Radio Waves

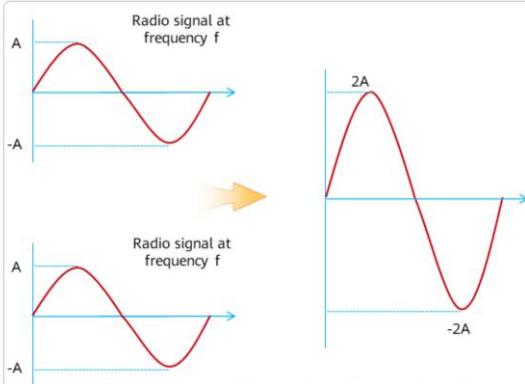
- The radio phase is the distance between the point of origin of any given wave and its first zero crossing. The phase is expressed in degrees or radians.
- Each cycle of a wave spans 360 degrees.
 - $2\pi = 360^\circ$
 - $57.3^\circ = 1 \text{ radian}$



- Phase is a relative term that describes the relationship between two co-channel waves. To measure the wave phase, the wavelength of a wave is divided into 360 parts and each part is 1° . 0° is used as the propagation start time of a wave. If one wave starts to propagate at 0° and the other wave starts to propagate at 90° , the two waves are 90° out-of-phase. If electromagnetic waves with the same frequency start to propagate at different time, the wave propagation is greatly affected.

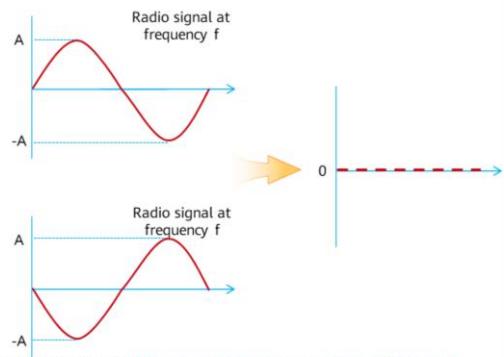
Impact of Phase on Signals

Signal enhancement



If two radio signals **at the same frequency** have the **same phase** when they arrive at the receiver, the two signals are superimposed and the signal strength is enhanced.

Signal weakening



If two radio signals **at the same frequency** have a **phase difference of 180°** when they arrive at the receiver, the two signals attenuate and the signal strength is weakened.

Wireless Communication System



- In a wireless communication system, information may be an image, a text, a sound, or the like.
- The transmitter 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.
- The transmitter and receiver are connected by using interfaces and channels. For wired communication, interfaces and cables on devices are visible. For wireless communication, interfaces are invisible and are connected to invisible space, which is referred to as air interfaces.

Code



Source coding

- Source coding is a process of converting raw information into digital signals by using a coding scheme.
- The information is compressed to the maximum extent without distortion.
- Different types of information require different coding schemes. For example, H.264 is intended for coding videos.

Channel coding

- Channel coding is a technology for correcting and detecting information errors to improve channel transmission reliability.
- Channel coding is introduced to restore information to the maximum extent at the receiver, thereby reducing the bit error rate.
- Channel coding adds redundant information to the raw information and therefore increases the information length.
- The ratio of the number of pre-coding bits (that is, raw information) to the number of post-coding bits is referred to as the coding efficiency, also called the coding rate.
- **Channel coding decreases the transmission rate of valid information but increases the transmission success rate of valid information.** Therefore, the best performance and effectiveness can be achieved by selecting a proper coding scheme for communication protocols.

- **Source coding**

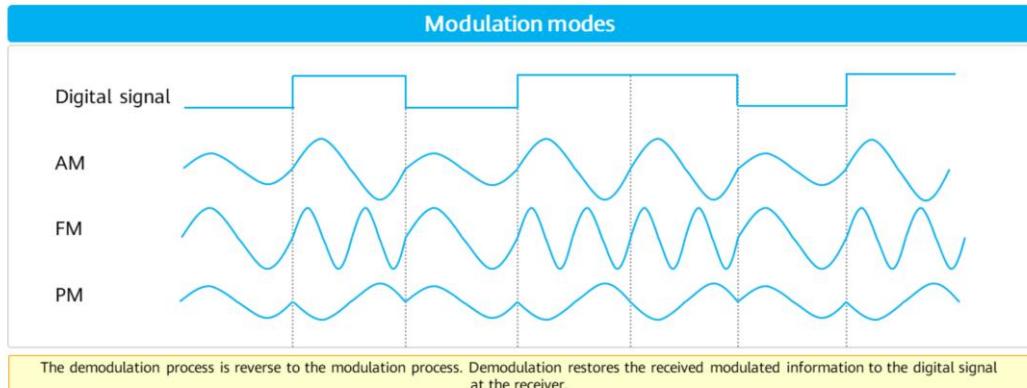
- Source coding is a process of converting raw information into digital signals by using a coding scheme. Source coding can reduce redundant information in the raw information, by compressing the information to the maximum extent without distortion.

- **Channel coding**

- 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 receiver may be erroneous. Channel coding is introduced to restore information to the maximum extent at the receiver, thereby reducing the bit error rate. WLANs use Binary Convolutional Code (BCC) and Low Density Parity Check (LDPC).
 - Channel coding adds redundant information to the raw information and therefore increases the information length. The ratio of the number of pre-coding bits (that is, raw information) to the number of post-coding bits is referred to as the coding efficiency, also called the coding rate. Channel coding decreases the transmission rate of valid information but increases the transmission success rate of valid information. Therefore, the best performance and effectiveness can be achieved by selecting a proper coding scheme for communication protocols.

Modulation and Demodulation

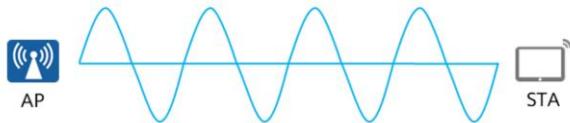
- Modulation: converts various digital baseband signals into digital modulation signals that are suitable for channel transmission. Modulation falls into Amplitude Modulation (AM), Frequency Modulation (FM), and Phase Modulation (PM).
- Demodulation: converts received digital frequency band signals to digital baseband signals.



- Modulation is classified the following types based on controlled signal parameters:
 - AM: The amplitude of high-frequency carrier signals changes with the instantaneous change of modulation signals. That is, the amplitude of a high-frequency signal is changed by using a modulation signal, so that information of the modulation signal is included in the high-frequency signal, the high-frequency signal is transmitted by using an antenna, and then the modulation signal is also transmitted. The receiver then can demodulate the modulation signal, that is, parse the amplitude of the high-frequency signal to obtain the modulation signal.
 - FM: It changes the carrier frequency according to modulation signals. The change of the modulation wave frequency is determined by the size of a modulation signal, and the change period is determined by the frequency of the modulation signal. The amplitude of the modulation wave remains unchanged. The waveform of the FM wave is like a spring that is compressed unevenly.
 - PM: PM is a modulation mode in which the deviation value of the carrier phase relative to the reference phase varies proportionally with the instantaneous value of the modulation signal. That is, the initial phase of a carrier varies with the baseband digital signal. For example, the digital signal 1 corresponds to the phase 180° , and the digital signal 0 corresponds to the phase 0° .

Carrier

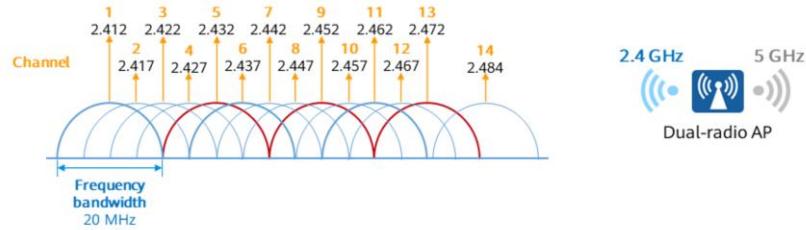
- A carrier is a radio wave of a specific frequency (in Hz). It is an electromagnetic wave whose frequency, amplitude, or phase is modulated for the purpose of conveying voice, music, image, or other signals.
- Carriers are the basis of wireless communication. The following figure shows a basic carrier that is generated at the transmitter and does not carry any information. The basic carrier is also used as an invariable signal at the receiver.



The Bit is the smallest unit of data. The transmitter sends 0 and 1 in a certain way to transmit data between two places. AC or DC signals do not have the capability of transmitting data. However, if signals fluctuate or change slightly, the transmitter and receiver can parse the signals to successfully transmit and receive data. The converted signal may be distinguished between 0 and 1, and is generally referred to as a carrier signal. The process of adjusting a signal to produce a carrier signal is referred to as modulation.

- A carrier is a waveform that is modulated with an information bearing signal for the purpose of conveying information. It is typically a sine wave. Generally, the frequency of a sine carrier is required to be far higher than the bandwidth of a modulation signal; otherwise, aliasing may occur, causing distortion of the transmitted signal.
- Generally, data to be sent has a low frequency. If the data is transmitted at the original frequency, it is difficult for the data to be received or synchronized. With carrier wave transmission, data signals can be loaded onto carrier wave signals. The receiver receives data signals at the carrier wave frequency. Meaningful and meaningless signal waves have different amplitudes, so that the needed data signals can be extracted through demodulation.
- Three properties (amplitude, frequency, and phase) of an electromagnetic wave can be modulated to generate a carrier signal.

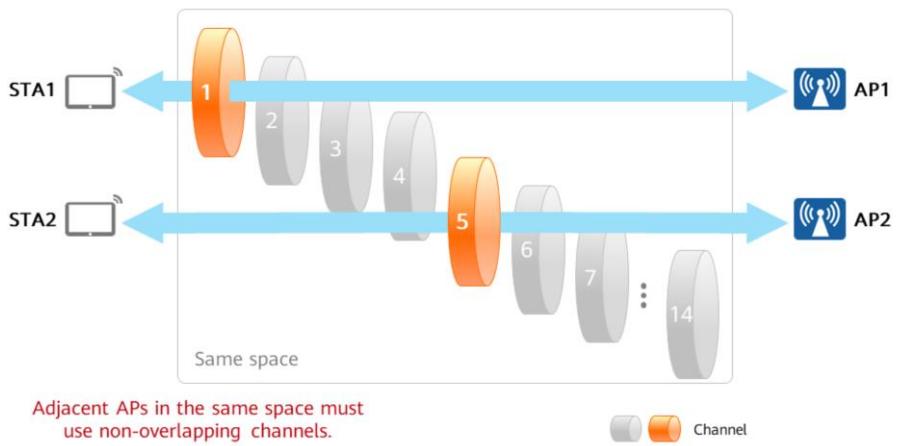
Channel



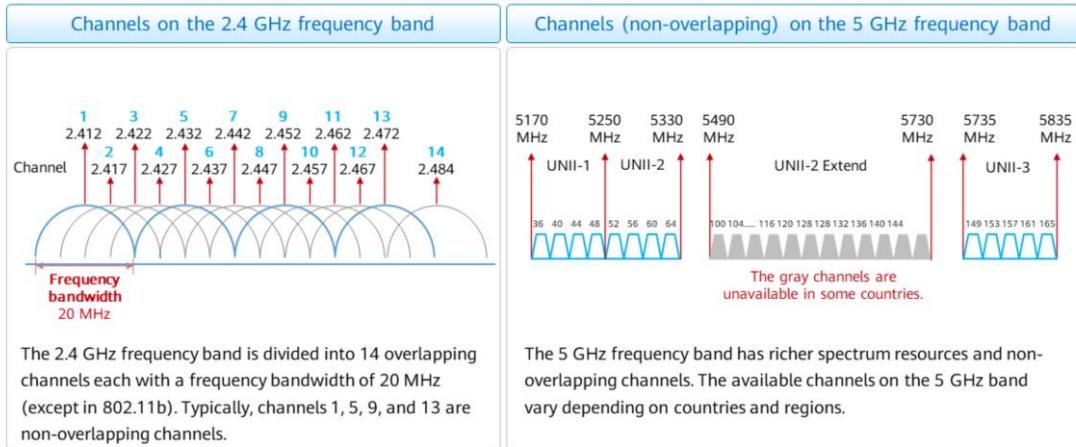
- **Channel:** A channel is used to transmit information, and a radio channel refers to a channel used by radio waves to transmit information in space. Given that radio waves are ubiquitous, random use of spectrum resources will cause endless interference issues. Therefore, in addition to defining the available frequency bands, wireless communication protocols must also accurately divide the frequency ranges. Each frequency range is a channel.
- **Overlapping channels:** Overlapping channels, such as channels 1 and 2, interfere with each other.
- **Non-overlapping channels:** Non-overlapping channels do not interfere with each other. Traditionally, only channels 1, 6, and 11 are non-overlapping channels on the 2.4 GHz frequency band. Since 802.11b (bandwidth: 22 MHz) has faded out of WLANs. Channels 1, 5, 9, and 13 are non-overlapping channels when the compatibility issue is not considered.

- The channel frequency bandwidth in 802.11b is 22 MHz. Currently, the single-channel frequency bandwidth in 802.11n, 802.11ac, and 802.11ax is 20 MHz.

Vividly Understanding Channels



2.4 GHz and 5 GHz Channels



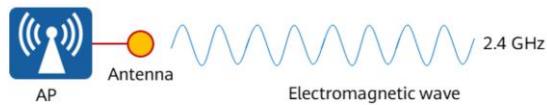
43 Huawei Confidential

 HUAWEI

- The frequency of a channel is represented by its center frequency.
- The center frequency of channels 1 to 13 is calculated as follows: $2412 + (n - 1) \times 5 \text{ MHz}$. The center frequency of channel 14 is defined as 2.484 GHz. Currently, channel 14 can be used only in a few countries, such as Japan.
- UNII: Unlicensed National Information Infrastructure
- The 5 GHz frequency band of Wi-Fi performs better than the 2.4 GHz frequency band in terms of frequency, data rate, and anti-interference performance. However, as the 5 GHz frequency band has higher frequencies and therefore has a shorter wavelength than the 2.4 GHz frequency band, it delivers poor signal penetration capabilities and shorter transmission distances. The available channels on the 5 GHz frequency band vary in different countries and regions. Its wide frequency bandwidth and reduced interference make it suitable for high-speed transmission.

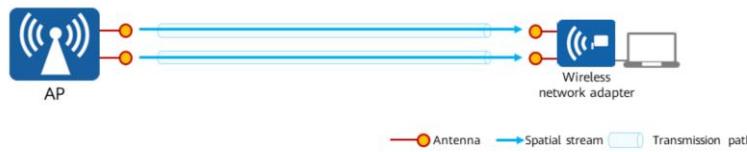
Radio, Frequency Band, Antenna

- WLANs use radio waves for data transmission. A radio wave is generated by the alternating current of an oscillation circuit, and can be transmitted and received through an antenna. A radio wave is also referred to as a radio wave, an electric wave, or a radio frequency (RF) wave.
- The frequency range of a radio wave is referred to as a frequency band.
- An antenna is a converter that converts guided waves transmitted on a transmission line into electromagnetic waves transmitted in space or vice versa. It is used with a radio device to transmit or receive electromagnetic waves.



Spatial Stream

- A radio system sends multiple radio signals at the same time. Each set of signals is called a spatial stream.
- A spatial stream is sent from the antenna of the transmitter. Each spatial stream follows an independent path to the receiver. A wireless system can transmit and receive spatial streams, and can distinguish signals destined for or from different spatial directions.
- In most cases, a spatial stream can be established between a transmit (TX) antenna and a receive (RX) antenna. For example, if an AP has four antennas and a STA has four antennas, four spatial streams can be established between the AP and STA.
- However, 802.11ac and 802.11ax defines that one radio supports a maximum of eight spatial streams. That is, even if an AP and a STA each has 12 antennas, only eight spatial streams can be established between them.



45 Huawei Confidential

 HUAWEI

- In 802.11n, the maximum transmission rate changes with the number of spatial streams. For example, an independent spatial stream supports a maximum rate of 150 Mbps, and two independent spatial streams support 300 Mbps. An 802.11n device supports up to 4x4 MIMO, that is, a maximum of four spatial streams, with a rate of up to 600 Mbps. The number of spatial streams determines the maximum physical transmission rate.
- In the MIMO system, the number of spatial streams is typically less than or equal to the number of antennas. If the number of RX antennas is different from that of TX antennas, the number of spatial streams is smaller than or equal to the minimum number of antennas on the transmitter or receiver. For example, a 4x4 MIMO system can transmit four or fewer spatial streams, whereas a 3x2 MIMO system can transmit two or fewer spatial streams.

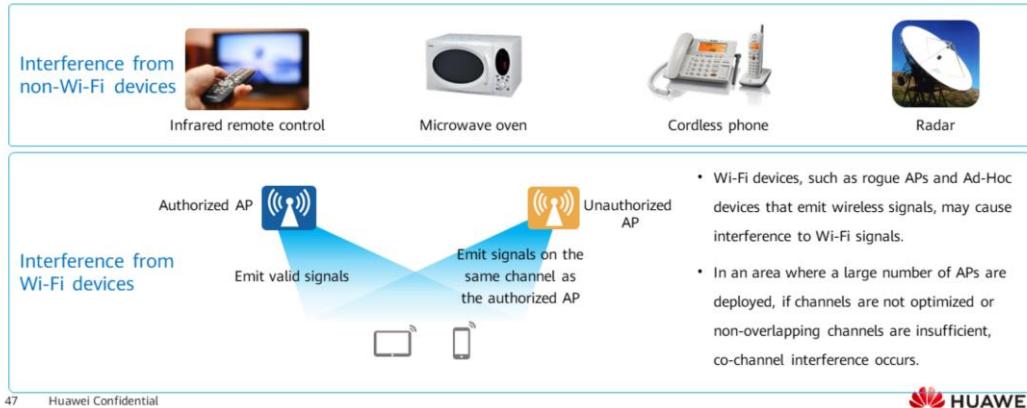
Single-Radio, Dual-Radio, and Three-Radio APs

| Single-radio AP | Dual-radio AP | Three-radio AP |
|--|--|---|
|  |  |  |
| <p>Single-radio APs work on either the 2.4 GHz or 5 GHz frequency band, and apply to the scenario where STAs work on the same frequency band.</p> | <p>Dual-radio APs work on both the 2.4 GHz and 5 GHz frequency bands, and apply to most mainstream WLAN scenarios.</p> | <p>Three-radio APs have two radios working on the 5 GHz frequency band and one on the 2.4 GHz frequency band. They apply to e-classrooms, high-density scenarios, as well as shopping malls and supermarkets.</p> |
| <p>One radio module can use multiple antennas to exchange data between an AP and a STA through multiple spatial streams, improving the data transmission rate.</p> | | |

- Compared with a single-radio AP, a dual-radio AP allows access of more STAs while ensuring STA performance. For example, in a bandwidth-demanding scenario, a single radio module can connect to 20 to 25 STAs. However, if an AP can work on both the 2.4 GHz and 5 GHz frequency bands, it can connect to 40 to 50 STAs.
- In this way, the access capacity is doubled in the same physical space. Therefore, dual-radio APs are applicable to high-density scenarios, such as libraries, conference rooms, academic lecture halls, and student dormitories.
- A three-radio AP provides one more radio than a dual-radio AP. This radio can be used for service coverage to improve the user access capability or used for spectrum monitoring, security scanning, and wireless location. It supports link aggregation of two Ethernet interfaces, ensuring link reliability and improving the service load balancing capability. Using three-radio APs effectively solves problems in high-density scenarios, such as difficult STA access, data congestion, and poor roaming performance.

Interference

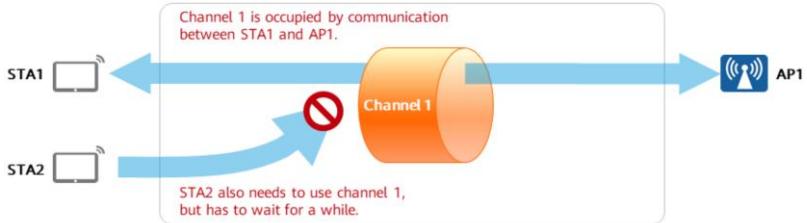
- In the communications field, a signal represents a message. For example, electrical signals with different amplitudes, frequencies, or phase may represent different messages.
- Interference is the damage to the reception of useful signals.



- Interference from non-Wi-Fi devices: Many household appliances, such as microwave ovens, Bluetooth headsets, and infrared remote controls, work on the 2.4 GHz frequency band. Consequently, a large number of 2.4 GHz channels are occupied, reducing the utilization of Wi-Fi transmission channels.

Interference and Channel Utilization

- Channel utilization is also called channel efficiency.
 - For the data transmitter, the channel utilization is the ratio of the time of a radio channel that is used for effective packet transmission over the total channel time.
 - Channel utilization = Duration in which a channel is busy/Total channel time
- WLAN interference aggravates collision and backoff. When multiple devices transmit data simultaneously, an air interface collision occurs. As a result, the receiver cannot parse packets normally. The transmitter retransmits packets after the backoff time, which prolongs the idle waiting time and reduces the channel utilization.



Theoretical Rate and Implementation Rate

- The theoretical rate refers to the maximum data transmission rate that a standard can achieve. For example, 802.11ac Wave 2 can achieve a theoretical data rate of 6.9 Gbps.
- The implementation rate refers to the maximum data rate that a product developed by a vendor in compliance with a standard can reach.

| Standard | | Released in | 2.4 GHz | 5 GHz | Theoretical Rate | Huawei's Implementation Rate |
|----------|-----------------|-------------|---------|-------|---------------------------------------|---------------------------------------|
| Wi-Fi 4 | 802.11n | 2009 | √ | √ | 2.4 GHz: 450 Mbps 5 GHz: 600 Mbps | 2.4 GHz: 450 Mbps 5 GHz: 600 Mbps |
| Wi-Fi 5 | 802.11ac Wave 1 | 2013 | - | √ | 3.74 Gbps | 1.3 Gbps |
| | 802.11ac Wave 2 | 2015 | - | √ | 6.9 Gbps | 1.73 Gbps |
| Wi-Fi 6 | 802.11ax | 2019 | √ | √ | 2.4 GHz: 1.15 Gbps 5 GHz: 9.6 Gbps | 2.4 GHz: 1.15 Gbps 5 GHz: 9.6 Gbps |

- The actual wireless access rate is significantly different from the implementation rate due to the following reasons:
 - Distance: The distance to an AP and physical obstacles (such as walls, signal barriers, or reflection materials) affects signal transmission and reduces the transmission rate.
 - Interference: Devices on other wireless networks working at the same frequency in the same area affect network performance.
 - Bandwidth sharing: The available bandwidth is shared by all users on the same wireless network.

Contents

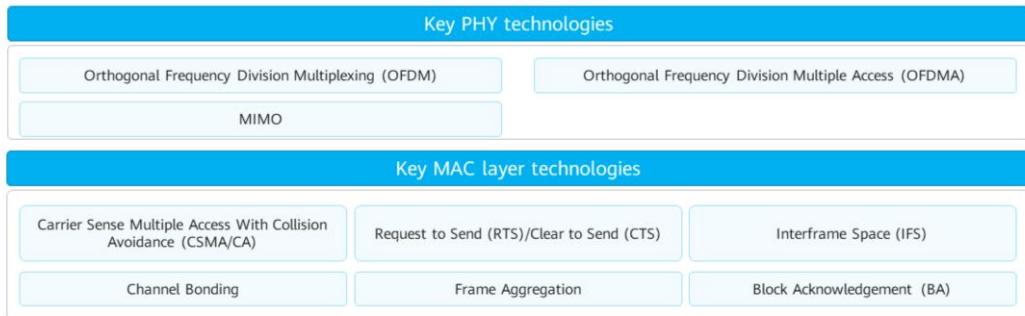
1. Basic Concepts of Wireless Communication
- 2. Key WLAN Technologies**
3. Introduction to 802.11 Standards

IEEE 802 and Equivalent TCP/IP Model

- WLAN technology is implemented based on IEEE 802.11 standards.
 - 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.
 - PHY layer: transmits bit streams over the air interface, for example, specifying the frequency band.



Overview of Key WLAN Technologies



802.11 PHY Technologies

- 802.11 uses three PHY technologies:
 - Frequency hopping (FH or FHSS)
 - Direct sequence (DS or DSSS)
 - Orthogonal frequency division multiplexing (OFDM)

- Frequency hopping (FH or FHSS)
 - FHSS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.
- Direct sequence (DS or DSSS)
 - DSSS uses mathematics functions to spread power to wider frequency band.
- Orthogonal Frequency Division Multiplexing (OFDM)
 - OFDM divides available channels into sub-channels and decodes some of the signals on each sub-channel.
 - The OFDM technology is used in 802.11n to 802.11ax. Therefore, this document describes only the OFDM technology in detail.

Subcarrier

- A channel is a radio wave of a specific frequency. Each user uses a frequency to transmit and receive information.
- A subcarrier is a sub-channel in multi-carrier communication.
- Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier modulation technology. Multiple subcarriers within the same single channel are modulated independently and transmitted in parallel, improving the channel's spectrum utilization.

Input data: 1 0 0 1 0 1 0 0 1 0 1 0 0 1 0 1 0 1...

Subcarrier 1: 1 1 0 0 0 1 1 0 0 1 0 1...

Subcarrier 2: 0 0 0 1 1 0 0 0 1 0 0 0...

Subcarrier 3: 0 1 1 0 0 1 1 1 0 1 1 0...



When OFDM is not enabled, a single channel allows only one single subcarrier at a time.



When OFDM is enabled, a single channel is divided into multiple sub-channels and multiple subcarriers can be transmitted in parallel.

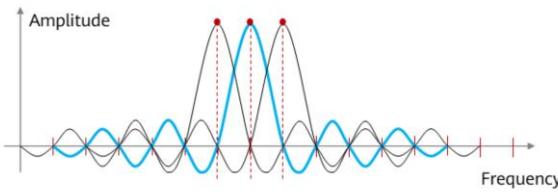


- In OFDM, subcarriers are orthogonal and their spectrums are overlapped. Therefore, due to high spectrum utilization, OFDM is widely applied, especially in preventing multipath fading. It is also easily implemented.
- As shown in the figure above, a channel is considered as a lane. When OFDM is not enabled, a single channel allows only one single subcarrier at a time, which is similar to that only one vehicle can pass at a time, resulting in low efficiency. When OFDM is enabled, a channel is divided into several sub-channels, so that multiple subcarriers can be transmitted at the same time, thereby greatly improving channel utilization.

OFDM

OFDM

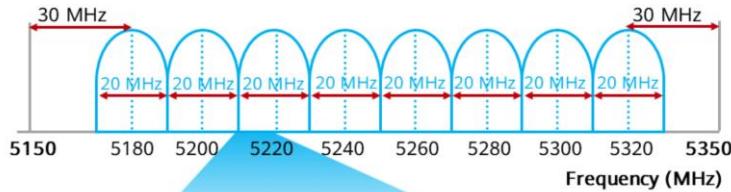
- OFDM is a multi-carrier modulation technology. By dividing a channel into multiple orthogonal sub-channels, it converts high-speed serial digital signals into low-speed parallel data streams and modulates them onto the sub-channels for transmission. Carriers corresponding to orthogonal sub-channels are usually referred to as subcarriers.
- OFDM enables orthogonal subcarriers. When one subcarrier reaches its wave peak and another is at the zero-crossing point, they do not interfere with each other.



- **Sub-carriers** in an OFDM system overlap but do not interfere with each other because they are orthogonal to each other.
- In the figure on the left, a signal is transmitted via three subcarriers. The individual wave peak of each subcarrier is used for data coding, as indicated by the red points. When the subcarrier marked in blue reaches its wave peak and lines up with zero amplitudes of the other two subcarriers, they are orthogonal to each other.

- OFDM divides a wide channel into multiple sub-channels, each of which is used for data transmission.
- Subcarriers in an OFDM system overlap but do not interfere with each other because they are orthogonal to each other. In mathematics, "orthogonal" is used to describe independent projects.
- OFDM operates properly because the waveform of a subcarrier is not affected by other subcarriers.

OFDM 5 GHz Channel Example



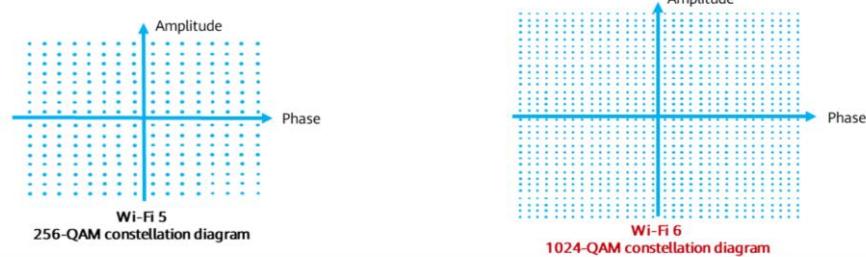
Each subcarrier occupies frequency bandwidth of 312.5 kHz.



48 sub-channels are used for data transmission, and 4 sub-channels are used for phase reference.

OFDM Sub-Channel Modulation Technology

- Available OFDM modulation schemes:
 - Binary phase shift keying (BPSK)
 - Quadrature phase shift keying (QPSK)
 - **Quadrature amplitude modulation (QAM)**
- QAM uses carrier amplitude and phase to transmit information.

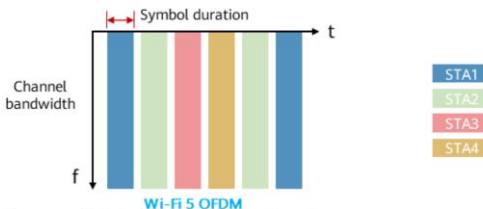


1024-QAM increases the rate of each spatial stream by 25% compared with 256-QAM.

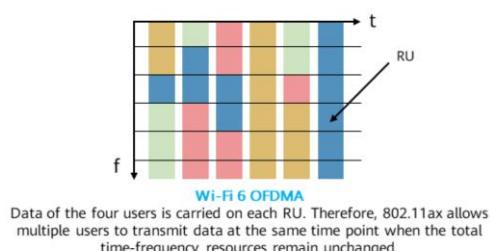
- To improve the throughput, 802.11ac introduces 256-QAM — a higher-order modulation scheme with higher modulation efficiency. 256-QAM supports the coding rates of 3/4 and 5/6 and increases the number of MCS types to 10. In terms of MCS representation, 802.11ac eliminates MCS coding for each MIMO combination, reducing the number of MCS types from dozens to 10. A higher MCS index indicates higher throughput due to the difference in the number of bits represented by each subcarrier in different MCS types. Each subcarrier (represented by a point in the constellation diagram) can carry data of 2 bits in BPSK, 4 bits in 16-QAM, 6 bits in 64-QAM, and 8 bits in 256-QAM.
- To improve the throughput, 802.11ax introduces 1024-QAM — a higher-order modulation scheme with higher modulation efficiency. 1024-QAM supports the coding rates of 3/4 and 5/6 and increases the number of MCS types to 12. A higher MCS index indicates higher throughput due to the difference in the number of bits represented by each subcarrier in different MCS types. Each subcarrier can carry data of 2 bits in BPSK, 4 bits in 16-QAM, 6 bits in 64-QAM, 8 bits in 256-QAM, and 10 bits in 1024-QAM. The figures above show the constellation diagrams of 256-QAM and 1024-QAM. A higher-order modulation scheme provides higher modulation efficiency. However, efficiency improvement in different modulation schemes is not linear and gradually becomes not obvious for higher-order modulation schemes.

OFDMA (1/3)

- OFDMA is used to distinguish users by frequency. Compared with the traditional FDMA, OFDMA significantly improves the spectrum utilization. OFDMA enables simultaneous data transmission of multiple users, which increases the air interface efficiency, greatly reduces the application latency, and lowers the conflict backoff probability.
- Resource unit (RU):
 - 802.11ax divides existing 20 MHz, 40 MHz, 80 MHz, and 160 MHz bandwidths into several RUs.
 - 802.11ax defines seven types of RUs: 26-tone, 52-tone, 106-tone, 242-tone, 484-tone, 996-tone, and 2x996-tone RUs. A user can transmit data on multiple RUs at a time. For example, the 80 MHz bandwidth can be divided into a maximum of 37 RUs, which can be used by 37 users concurrently.



58 Huawei Confidential

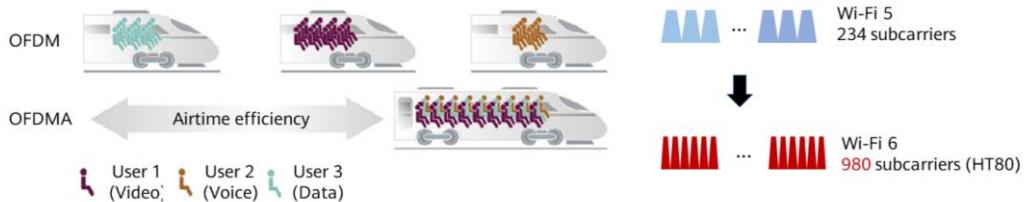


HUAWEI

- OFDM:
 - Users are differentiated by time segment. In each time segment, one user occupies all subcarriers.
- OFDMA:
 - An AP determines how to allocate channel resources based on communication requirements of multiple users, and always allocates all available RUs in the downlink direction. The AP may allocate the entire channel to one user at a time or partition the channel to serve multiple users concurrently.
 - In OFDMA mode, channel resources can be allocated more delicately, allowing finer-grained QoS.
- RU:
 - 802.11ax defines the RUs of different tones, including 26, 52, 106, 242, 484, 996, and 2x996 tones. RUs with different tones are applicable when different channel bandwidths are available: 484-tone RUs available only at 40 MHz, 80 MHz, or 160 MHz; 996-tone RUs available only at 80 MHz or 160 MHz; and 2x996-tone RUs available only at 160 MHz.
- OFDMA working mode (as shown in the right figure): Users are differentiated by time-frequency RUs. The resources of a channel are divided into small fixed time-frequency blocks, which are known as RUs. In this mode, user data is carried on each RU. Therefore, multiple users may simultaneously send data in each time segment when the total time-frequency resources remain unchanged.

OFDMA (2/3)

- OFDMA divides a radio channel into a plurality of sub-channels (subcarriers) in a frequency domain, and allocates resources in each radio channel into multiple RUs.
- User data is carried on RUs instead of occupying the entire channel. In this way, multiple users can simultaneously transmit data in each time segment without queuing or contention, thereby reducing the queuing time and improving data transmission efficiency. Therefore, OFDMA is ideal for multi-user scenarios where a large number of small data packets are transmitted, for example, IoT or voice scenarios.



- Compared with OFDM, OFDMA has the following advantages:
 - Finer resource allocation: The transmit power can be allocated based on the channel quality, especially when the channel status of some nodes is not good. This helps to allocate channel time-frequency resources in a more delicate manner.
 - Better QoS: According to earlier 802.11 standards, one user occupies the entire channel to transmit data. If a QoS node wants to send a data packet, it must wait until the current sender releases the complete channel. This causes a long latency. With OFDMA, however, one sender occupies only a part of the channel, which reduces the access latency for QoS nodes.
- Note: 26-tone RUs are similar to radar signals, and may be detected by radars by mistake.
- The Wi-Fi 6 standard uses OFDMA to improve the spectrum utilization. For example, 80 MHz bandwidth can be divided into a maximum of 37 RUs, which can serve 37 users concurrently.
- Wi-Fi 6 reduces the subcarrier spacing to 78.125 kHz from 312.5 kHz in Wi-Fi 5. This means that Wi-Fi 6 achieves a four-fold increase in the number of subcarriers that in Wi-Fi 5 with the same channel bandwidth.

OFDMA (3/3)

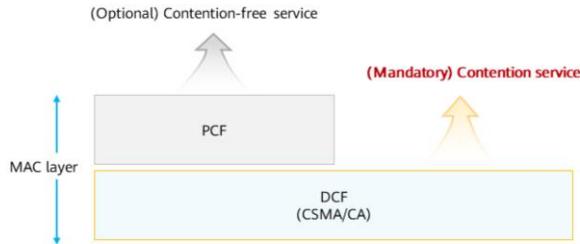
- OFDMA divides the entire channel's resources into multiple subcarriers, which are then divided into several groups based on RU type. Each user may occupy one or more groups of RUs to meet various bandwidth requirements. The following table lists the maximum number of RUs under different channel bandwidths.

| RU Type | CBW20 | CBW40 | CBW80 | CBW160 and CBW80+80 |
|---------------|--------------|--------------|--------------|---------------------|
| 26-tone RU | 9 | 18 | 37 | 74 |
| 52-tone RU | 4 | 8 | 16 | 32 |
| 106-tone RU | 2 | 4 | 8 | 16 |
| 242-tone RU | 1-SU/MU-MIMO | 2 | 4 | 8 |
| 484-tone RU | N/A | 1-SU/MU-MIMO | 2 | 4 |
| 996-tone RU | N/A | N/A | 1-SU/MU-MIMO | 2 |
| 2x996-tone RU | N/A | N/A | N/A | 1-SU/MU-MIMO |

- In Wi-Fi 6, the minimum RU size and minimum subcarrier bandwidth are 2 MHz and 78.125 kHz, respectively. Therefore, the minimum RU type is 26-tone RU. By analogy, there are 52-tone, 106-tone, 242-tone, 484-tone, and 996-tone RUs.
- An RU includes data subcarriers and pilot subcarriers. Data subcarriers are used to carry data, and pilot subcarriers are used for channel estimation.

802.11 MAC Layer

- A WLAN channel is shared by all STAs, and only one STA is allowed to transmit data at a time. Therefore, a channel allocation mechanism is required to coordinate when each STA transmits and receives data. 802.11 proposes the following two coordination modes at the MAC layer:
 - Distributed coordination function (DCF): uses the CSMA/CA mechanism to enable each STA to contend for a channel for data transmission.
 - Point coordination function (PCF): leverages the centralized access control algorithm to enable STAs to transmit data frames in turn (in a way similar to the round-robin mode), thereby preventing collisions.



DCF is mandatory and PCF is optional. DCF, with the core being CSMA/CA, is commonly used in the industry.

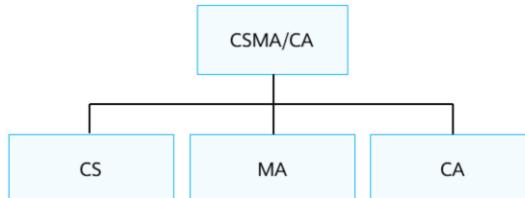
- Simply speaking, with CSMA/CA, a STA listens on the channel before sending data. If the channel is busy, a collision exists and the STA waits for a period of time before sending data. If the channel is not busy, the STA can directly send data.

What Is CSMA/CA?

CSMA/CA

802.11 protocols use the carrier sense multiple access with collision avoidance (CSMA/CA) mechanism to prevent collision detection from wasting transmission resources.

- CS: Before transmitting data, a STA checks whether the channel is idle to reduce chances of collision.
- MA: Data sent by a STA can be received by multiple STAs.
- CA: It is designed to minimize the probability of collision.

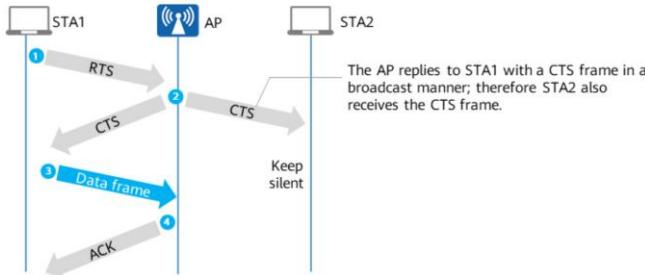


- The basis for CSMA/CA is carrier sense. 802.11 proposes two carrier sense methods based on medium characteristics of WLANs: physical and virtual carrier sense. These two carrier sense methods may be performed at the same time. As long as either of the two methods shows that the media is in use, the media is considered busy.
 - Physical carrier sense: works at the PHY layer and depends on the medium in use and modulation scheme. This method detects the signal energy from the received radio frequency or antenna signals and estimates the busy or idle status of channels based on the signal quality.
 - Virtual carrier sense: works at the MAC layer. With this method, the transmit STA notifies other STAs of the duration it needs to occupy the channel so that the other STAs stop sending data during this period.
- "Virtual" herein means that other STAs do not send data because they receive notifications from the transmit STA but do not actually detect the physical channel. Notifications sent from the transmit STA are implemented by filling the Duration field of the MAC frame header with the time (in μ s) during which the STA will occupy the channel after the current frame transmission is completed, including the time required by the receive STA (destination) to send an ACK frame. When a STA other than the transmit (source) and receive (destination) STAs detects the Duration field in the header of a MAC frame that is being transmitted on a channel, the STA adjusts its own NAV.
- Collision detection cannot be used on WLANs. As long as data is transmitted, the transmission of the entire frame must be completed. If a collision occurs during the transmission on a WLAN, resources of the entire channel are wasted in this period of time.

Therefore, collisions should be minimized on WLANs.

RTS/CTS

- The request to send (RTS)/clear to send (CTS) protocol is used by 802.11 standards to reduce collisions caused by hidden node problems.
 - An RTS frame is used to reserve the right to use a link. STAs that receive the RTS frame keep silent.
 - A CTS frame is used by an AP to respond to an RTS frame. Other STAs that receive the CTS frame keep silent.
- The core of RTS/CTS is to allow the transmitter to reserve channels and avoid collision of subsequent large data frames through small reserved packets (RTS/CTS frames).



IFS

Interframe space (IFS)

- To avoid collisions, 802.11 protocols stipulate that all STAs wait for a very short time before sending a next frame. During this period, the STAs still listen to the channel state. This period is known as IFS.
- The IFS depends on the frame type. A shorter IFS is imposed on higher-priority frames, which can be sent preferentially.
- When the medium becomes busy transmitting higher-priority frames, transmission of lower-priority frames has to be delayed. This reduces the chance of collision.

Short IFS (SIFS): short wait time of 16 µs (802.11ax) and high priority

- Separates frames in each exchange. A STA should be able to switch from the transmit mode to the receive mode within this period. SIFS frames, including ACK, CTS, and control frames, have the highest priority and require immediate response.

Distributed coordination function IFS (DIFS): long wait time and low priority

- Transmits data frames and management frames in DCF mode.
- A DIFS is the shortest time for a medium to remain idle in competitive services. If the medium is continuously idle for a time longer than the DIFS, a STA can access the medium immediately.

- SIFS

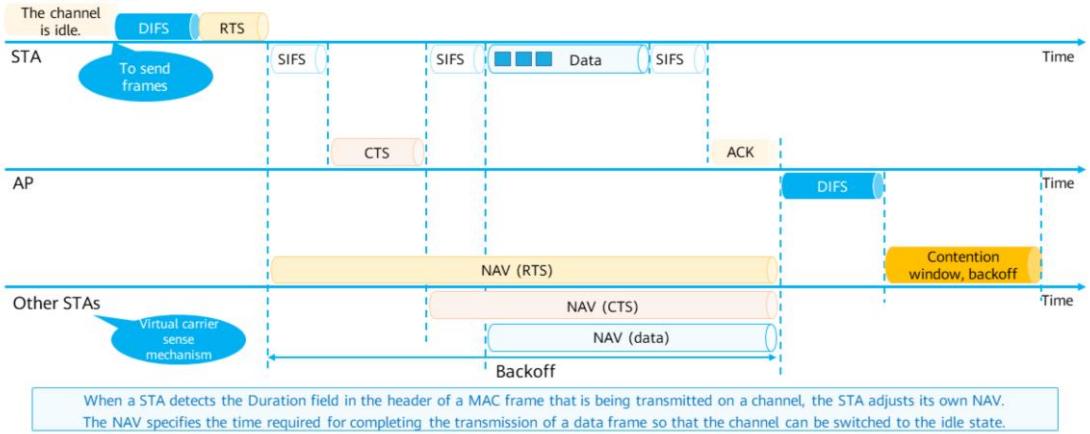
- Features the shortest wait time and highest priority.
- Separates frames in each exchange.
- Allows a STA to switch from the transmit mode to the receive mode within this period.
- SIFS applies to transmission of the following frames: ACK frames, CTS frames, fragmented MAC frames, Probe Response frames, and frames sent from an AP to a STA in PCF mode.

- DIFS

- Features the longest wait time and lowest priority.
- Transmits data frames and management frames in DCF mode.
- A DIFS is the shortest time for a medium to remain idle in competitive services. If the medium is continuously idle for a time longer than the DIFS, a STA can access the medium immediately.

Key Technologies of CSMA/CA

- 802.11 defines physical carrier sense on the air interface. A STA starts to send the first MAC frame after a DIFS only if it finds the channel idle.

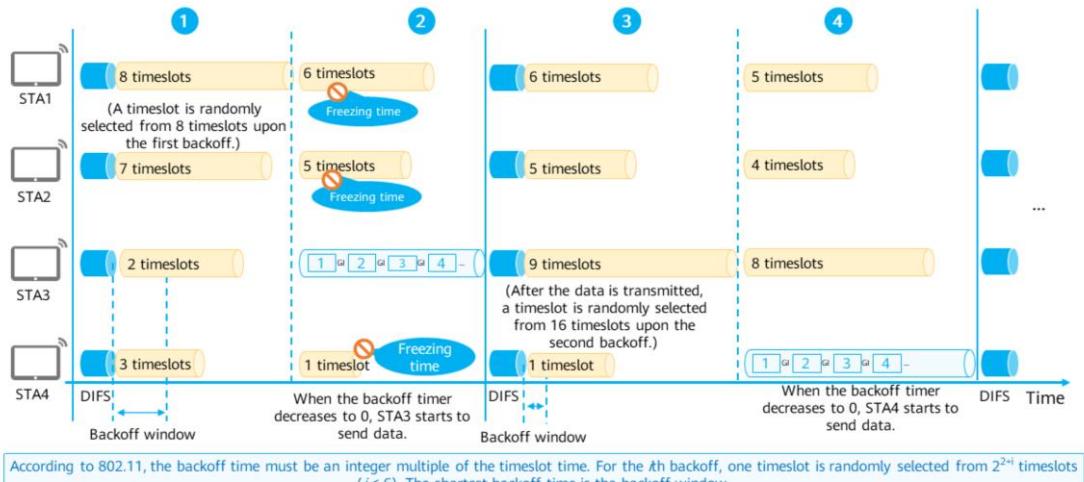


66 Huawei Confidential

HUAWEI

- A STA needs to wait for another DIFS until the channel is idle because another STA may have a high-priority frame to be sent. Higher-priority frames will be sent preferentially.
- If there is no higher priority frame, the STA is ready to send data.
- Before sending data, the STA sends RTS and CTS frames to avoid packet collision. This is the virtual carrier sense mechanism, which enables a STA to notify all STAs of the channel occupation duration (including the time required for the AP to send an ACK frame). In this manner, all the other STAs stop sending data in this period of time, thereby greatly reducing the chance of collision.
 - With the virtual carrier sense mechanism, other STAs do not send data because they receive notifications from the transmit STA (source) but do not actually detect the physical channel. This achieves the same effect as that of channel detection by other STAs. Notifications sent from the transmit STA are implemented by filling the Duration field of the MAC frame header with the time (in μ s) during which the STA will occupy the channel after the current frame transmission is completed, including the time required by the receive STA (destination) to send an ACK frame.
- When a STA detects the Duration field in the header of a MAC frame that is being transmitted on a channel, the STA adjusts its own NAV. The NAV specifies the time required for completing the transmission of a data frame so that the channel can be switched to the idle state. Therefore, the STA determines that a channel is busy based on physical carrier sense or virtual carrier sense at the MAC layer.

Random Backoff Mechanism of 802.11



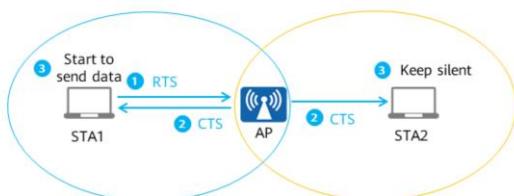
69 Huawei Confidential

HUAWEI

- 802.11 standards use the binary exponential backoff algorithm, but the specific implementation is slightly different. For the i th backoff, one timeslot is randomly selected from 2^{2i+1} timeslots. That is, upon the first backoff, one timeslot is randomly selected from 8 timeslots (not two timeslots); and upon the second backoff, one timeslot is randomly selected from 16 timeslots (not four timeslots). When the timeslot number reaches 255 (corresponding to the sixth backoff), the number does not increase anymore.
- When a STA that wants to send data selects a timeslot in the contention window using the backoff algorithm, a backoff timer starts to count down from the selected timeslot. When the backoff timer counts down to 0, the STA starts to send data. Alternatively, if the channel is sensed busy before the backoff timer counts down to 0, the backoff timer is frozen and waits for the channel to become idle again. After the DIFS elapses, the backoff timer continues to count down (starting from the remaining time). This provision allows the STA that continues to start the backoff timer to access the channel earlier.
- In the figure above, the backoff timer of STA3 counts down to zero first. Therefore, STA3 immediately sends the entire data frame. Note that the channel becomes idle immediately after STA3 sends data. The backoff timer of STA3 keeps counting down. When STA3 is sending data, other STAs sense the channel busy, freeze their backoff timers, and wait for the channel to become idle.
- After STA3 finishes sending data, other STAs wait for a DIFS and their backoff timers start to count down from their respective remaining times. Now, the backoff timer of STA4 reaches zero first, and STA4 is granted the transmission right. When STA4 sends data, other STAs freeze their backoff timers until the remaining time expires, and then send data. Freezing the remaining time of the backoff timer aims to make channel resources fairer to all STAs.

RTS/CTS: Hidden Node

- A hidden node problem occurs when a STA can communicate with an AP but cannot directly communicate with other STAs associated with the AP.



STA1 and STA2 are hidden nodes to each other.

- 1 STA1 sends an RTS frame to reserve access to the channel.
- 2 After receiving the RTS frame, the AP broadcasts a CTS frame as a response.
- 3 After receiving the CTS frame from the AP, STA1 is ready to send data.
- 4 STA2 receives the CTS frame sent by the AP and learns that the current channel is busy. Therefore, STA2 keeps silent and cannot send data.

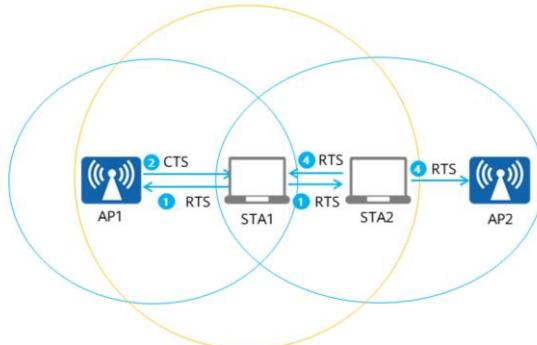
As the distance between STA1 and STA2 is too long, STA1 and STA2 cannot detect each other.

- To resolve the hidden node problem on a WLAN, the IEEE 802.11 protocol allows a STA to reserve access to a channel by using the RTS/CTS mechanism.
- With the RTS/CTS mechanism, a STA does not send data immediately after a DIFS. Instead, the STA sends an RTS frame to apply for channel occupation. Other STAs that receive the RTS frame respond with a CTS frame after an SIFS, informing the transmit STA that they are ready to receive data. After successful RTS/CTS signal exchange (that is, the handshake process is completed), the transmit STA starts to transmit data. In this manner, when multiple STAs that are invisible to each other simultaneously attempt to send signals to the same destination STA, only the STA that receives the CTS frame returned by the destination STA can successfully send data, thereby avoiding collisions. In this case, a collision (if any) may occur only when the RTS frame is transmitted. For the STAs that did not receive the CTS frame from the destination STA, a contention mechanism provided by the DCF is available to allocate random backoff timer values to them. These STAs then will wait for a DIFS until the medium becomes idle again and contend by sending RTS frames. This process continues until the STAs succeed in sending data.
- The RTS/CTS mechanism improves transmission efficiency as follows:
 - Mitigates the hidden node problem because long data frames can be sent only after channel resources are successfully reserved.
 - Involves only a short RTS or CTS frame collision (if any) duration because these two frames are relatively small in size. Once the RTS and CTS frames are correctly transmitted, subsequent data frames and ACK frames can be sent without any

collision.

RTS/CTS: Exposed Node

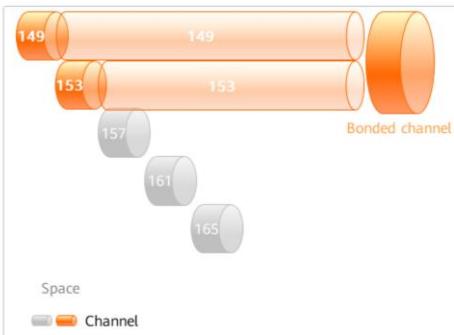
- An exposed node problem occurs when a STA can communicate with other STAs associated with an AP but cannot directly communicate with the AP.



STA1 and STA2 are exposed nodes to each other.

- 1 STA1 broadcasts an RTS frame to reserve access to the channel.
- 2 After receiving the RTS frame, the AP broadcasts a CTS frame as a response.
- 3 STA2 receives the RTS frame from STA1 but not the CTS frame from AP1.
- 4 STA2 broadcasts an RTS frame to reserve access to the channel.

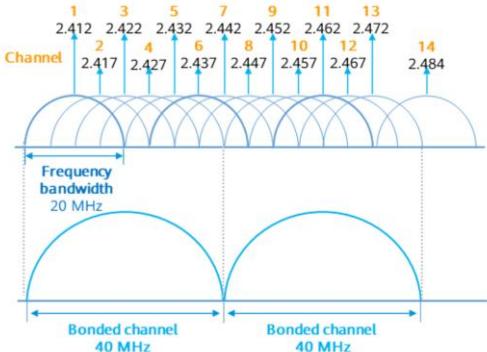
Channel Bonding



- By binding two or more adjacent non-overlapping channels together into one channel, the transmission rate can be doubled.
- For wireless technologies, increasing the channel width can directly increase the throughput. This is similar to a road. If the road is widened, the traffic capacity of the road is improved.
- In 802.11 standards, the air interface works at 20 MHz bandwidth. By bonding two adjacent 20 MHz channels into a 40 MHz channel, the transmission rate is doubled. In 802.11ac and later standards, eight channels can be bonded into a 160 MHz channel, and the transmission rate exceeds 1000 Mbps.

- In practice, a bonded channel contains one primary channel and one auxiliary channel. Hence, either a 40 MHz channel or a single 20 MHz channel can be used for transmitting and receiving data.
- A small part of bandwidth is reserved between two 20 MHz channels to avoid mutual interference. When channel bonding technology is used to achieve 40 MHz bandwidth, the reserved bandwidth may also be used for communication, thereby further improving throughput.
- Theoretically, a 40 MHz bonded channel can increase the spectrum utilization and double the throughput compared with 20 MHz channels. However, the 2.4 GHz frequency band has limited spectrum resources, and has only four non-overlapping channels that can form at most two 40 MHz bonded channels that do not interfere with each other on the band. Therefore, channel bonding on the 2.4 GHz frequency band is not practical on the live network. Currently, channel bonding is mainly performed on the 5 GHz frequency band.

2.4 GHz Channel Bonding

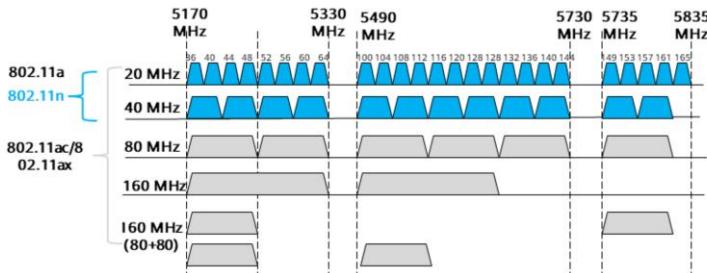


- Channel bonding can bond two adjacent non-overlapping 20 MHz channels into a 40 MHz channel, multiplying the data transmission rate. For example, channel 1 and channel 5 can be bonded, and channel 9 and channel 13 can be bonded.
- One of the two 20 MHz channels is the primary channel, and the other the auxiliary channel. The primary channel is used to transmit **beacon packets and some data packets**, and the auxiliary channel is used to transmit other packets.

The 2.4 GHz frequency band supports channel bonding to achieve a maximum of 40 MHz bandwidth.

- Theoretically, a 40 MHz bonded channel can increase the spectrum utilization and double the throughput compared with 20 MHz channels. However, the 2.4 GHz frequency band does not support two 40 MHz bonded channels that do not interfere with each other due to limited spectrum resources on the band. Only channels 1, 5, 9, and 13 can be bonded to form two non-overlapping channels.
- A small part of bandwidth is reserved between two 20 MHz channels to avoid mutual interference. When channel bonding technology is used to achieve 40 MHz bandwidth, the reserved bandwidth may also be used for communication, thereby further improving throughput.
- If two adjacent 20 MHz channels are bonded and the center frequency of the auxiliary 20 MHz channel is lower than that of the primary channel, the bonded channel is named xxxplus. Otherwise, the bonded channel is named xxxminus.
 - For example, on the 2.4 GHz frequency band, if channel 1 is used as the primary channel in channel bonding, the bonded channel is known as channel 1plus, indicating channel 1 is the primary channel, channel 5 is the auxiliary channel, and the frequency bandwidth of the bonded channel is 40 MHz.
 - If channel 5 is used as the primary channel, the bonded channel is known as channel 5minus, indicating that channel 5 is the primary channel, channel 1 is the auxiliary channel, and the frequency bandwidth of the bonded channel is 40 MHz.

5 GHz Channel Bonding

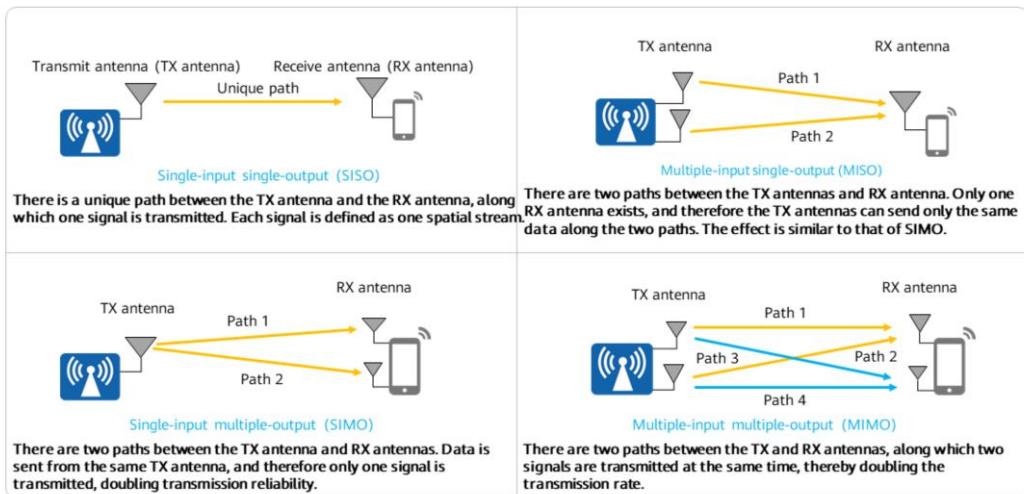


- Two adjacent 20 MHz channels can be bonded into a 40 MHz channel. One of the two 20 MHz channels is the primary channel, and the other the auxiliary channel.
 - For example, on channel 149, the 40 MHz bandwidth is configured by bonding with another channel. That is, the 40 MHz bandwidth is provided by bonding channels 149 and 153. Channel 149+ indicates that the 40 MHz channel is available by bonding the 20 MHz channel with the center frequency 149 and the 20 MHz channel with the center frequency 153.
- Two neighboring 40 MHz channels are bonded into an 80 MHz channel, and two neighboring 80 MHz channels are bonded into a 160 MHz channel.
- The primary channel is used for transmission of the management and control packets. A bonded channel is idle only when its primary channel is idle.

If two adjacent 20 MHz channels are bonded and the center frequency of the auxiliary 20 MHz channel is lower than that of the primary channel, the bonded channel is named xxplus. Otherwise, the bonded channel is named xxminus.

- The 5 GHz frequency band has abundant spectrum resources. The FCC allocates 23 non-overlapping 20 MHz channels. In China, there are five non-overlapping 20 MHz channels, which are enough to be bonded into 40 MHz channels.
- Therefore, it is not recommended that 802.11n uses 40 MHz bandwidth on the 2.4 GHz frequency band. That is, 802.11g and 802.11n usually have 20 MHz frequency bandwidths deployed to obtain more channel resources, supporting cellular coverage.
- Two adjacent 20 MHz channels can be bonded into a 40 MHz channel. One of the two 20 MHz channels is the primary channel, and the other the auxiliary channel.
- Two adjacent 40 MHz channels can be bonded into an 80 MHz channel. In an 80 MHz channel, one 20 MHz channel must be selected as the primary channel. The other 20 MHz channel in the 40 MHz channel containing the primary channel is known as the auxiliary 20 MHz channel. The 40 MHz channel that does not contain the primary channel is known as the auxiliary 40 MHz channel.
- Two adjacent 80 MHz channels can be bonded into a 160 MHz channel. In a 160 MHz channel, one 20 MHz channel must be selected as the primary channel. The other 20 MHz channels in the 80 MHz channel containing the primary channel are known as auxiliary 20 MHz channels. The 40 MHz channels that do not contain the primary channel are known as auxiliary 40 MHz channels. The 80 MHz channel that does not contain the primary channel is known as the auxiliary 80 MHz channel. On the 5 GHz frequency band, a maximum of two 160 MHz channels can be formed.
- An 80+80 MHz channel is formed by bonding two non-adjacent 80 MHz channels. Division of the primary and auxiliary channels is similar to that for a 160 MHz channel. Compared with the 160 MHz channel solution, the 80+80 MHz channel solution can divide more than three non-overlapping channels on the 5 GHz frequency band and therefore is suitable for cellular channel planning, meeting wireless network deployment requirements.

SISO, MISO, SIMO, and MIMO



75 Huawei Confidential

 HUAWEI

- **SISO**

- Apparently, SISO transmission is unreliable and rate limited because there is only one path between the TX antenna and RX antenna. To address this issue, we add more antennas on the receiver (STA) so that two or more signals can be received concurrently, achieving single-input multiple-output (SIMO).

- **SIMO**

- There are multiple paths between the TX antenna and RX antennas. Data is sent from the same TX antenna, and therefore only one signal is transmitted, doubling reliability. This mode is also known as receive diversity.

- **MISO**

- There are multiple paths between TX antennas and the RX antenna. Only one RX antenna exists, and therefore the TX antennas can send only the same data along the two paths. The effect is similar to that of SIMO. This mode is also known as transmit diversity.

- **MIMO**

- MIMO technology allows multiple antennas to send and receive spatial streams (multiple signals) simultaneously and to differentiate the signals sent to or received from different spaces. By leveraging technologies such as spatial reuse (SR) and space diversity (SD), MIMO improves the system capacity, coverage, and SNR without increasing the occupied bandwidth.

MU-MIMO

Multi-user MIMO (MU-MIMO)

- An AP leverages space domain resources of antennas to communicate with multiple STAs at the same time.
- The CSMA-CA mechanism used by the WLAN allows only one channel to be occupied by only one STA at a time. During this period, other STAs cannot communicate with the AP. To optimized channel resource utilization, MU-MIMO emerges. With this function enabled, STAs supporting MU-MIMO can form an MU group to simultaneously receive downlink data from the same air interface channel, improving channel efficiency and overall downlink throughput.

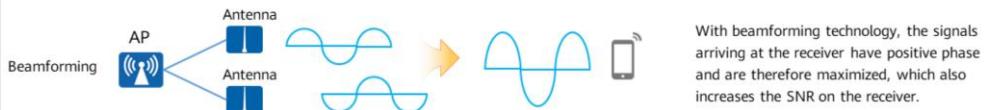
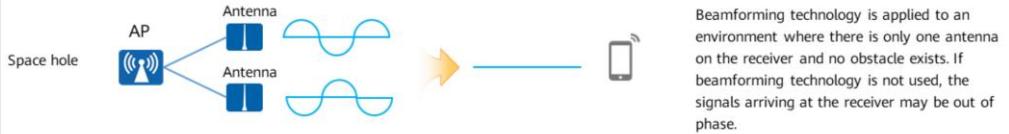


- A router that supports MU-MIMO technology can transmit data simultaneously with a plurality of STAs, which changes the serial transmission mode to parallel and shortens the waiting time before STAs obtain data from the router wirelessly. Additionally, the bandwidth resources obtained by each STA are not compromised. Therefore, this technology maximizes the resource utilization and thereby increases the access capacity of the router and the Internet access speed of STAs.

MIMO: Beamforming

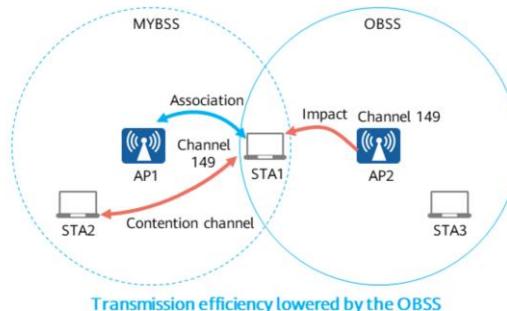
Beamforming

- When the transmitter has multiple TX antennas, the signals transmitted from each antenna are adjusted to improve the signal strength on the receiver.



OBSS

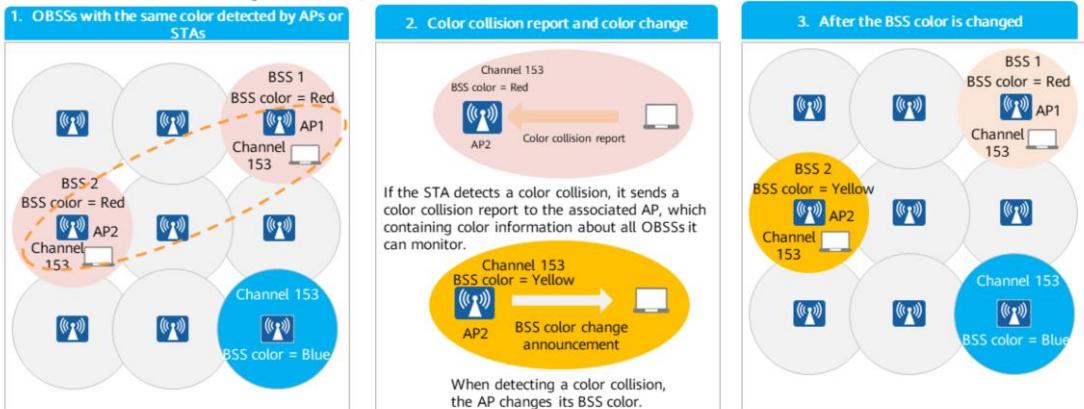
- The basic unit of a WLAN is a basic service set (BSS), which consists of one fixed AP and multiple STAs.
- When STA1 is associated with AP1, the BSS of AP1 is MYBSS for STA1. In addition, STA1 is located in an overlapping basic service set (OBSS). This means that STA1 can also receive packets from AP2. In this case, the BSS of AP2 is OBSS for STA1. To STA1, frames from MYBSS are intra-BSS frames, and those from OBSS are inter-BSS frames. Communication in the OBSS causes backoff of STA1, consequently decreasing transmission efficiency.



- Before SR was introduced, WLAN systems used the CSMA/CA mechanism. The CSMA/CA mechanism allows only one link to transmit data at a time within the signal coverage of a STA. This can be done only after the STA obtains the channel access right through contention. The CSMA/CA mechanism enables all WLAN participants in a collision domain to fairly share channels. However, when the number of WLAN participants greatly increases, especially when there are a large number of APs with OBSSs on the network, transmission efficiency decreases.
- 802.11 uses CSMA/CA at the MAC layer. It uses the half-duplex communication mechanism, in which only one radio device can transmit data on the network at a time. If an 802.11 STA detects a transmission signal (by checking the PHY header) from any other 802.11 STA, the 802.11 STA delays its transmission. When APs and STAs are deployed to work on the same channel and contend for signal transmission, they are located in the same OBSS, which suffers from co-channel interference.
- 802.11ax devices distinguish BSSs by adding the BSS color field to the PHY header of a packet. During contention, a node allocates a contention behavior at the MAC layer based on the detected BSS color field value in the PHY header. If the BSS color field values are the same, the nodes are in the same BSS, indicating intra-BSS contention. If the BSS color field values are different, the nodes are in an OBSS, indicating inter-BSS contention.

802.11ax BSS Coloring

- BSS coloring is a method for improving the spatial reuse (SR) efficiency and reducing the contention overhead at the MAC layer caused by overlapping basic service sets (OBSSs). BSS coloring aims to improve the SR efficiency while preventing inter-BSS interference affecting the PHY layer transmission rate between nodes (that is, reducing the MCS value).



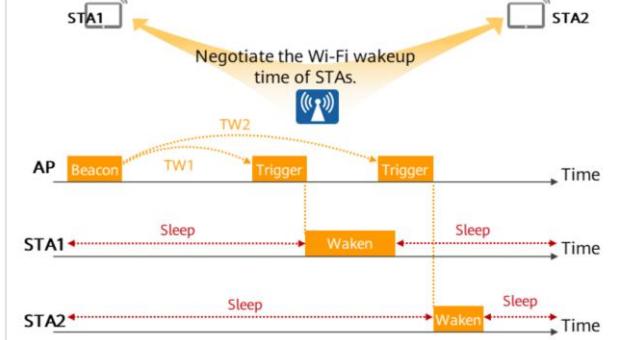
79 Huawei Confidential

HUAWEI

- Based on the BSS coloring mechanism, wireless traffic is marked at the beginning of transmission, which helps surrounding devices determine whether to allow wireless medium to be used at the same time. Even if the level of the detection signal from the neighboring network exceeds the traditional signal detection threshold, the wireless medium can be considered idle and new transmission is allowed as long as the transmit power of the new transmission is lowered appropriately. The BSS coloring mechanism aims to enable devices to distinguish between the transmissions on the local and neighboring networks. The self-adaptive power and sensitivity thresholds allow dynamic adjustment of the transmit power and signal detection threshold to increase SR efficiency and minimize co-channel interference.
- If an 802.11ax AP detects an OBSS with the same color, the AP can change its own BSS color to reduce co-channel interference. If two APs have the same BSS color, a BSS color collision occurs. As shown in the figure above, if an 802.11ax AP detects different BSS color field values from other APs or the AP itself, a BSS color collision is detected.
- If a STA detects a BSS color collision, it sends a color collision report to the associated AP. The report contains BSS coloring information about all OBSSs it has detected.
- The AP informs all nodes within the same BSS of the BSS color change through a Beacon frame that carries the new BSS color in the New BSS Color sub-field. The BSS color change may also be notified through a Probe Response and a Reassociation Response frame.
- When detecting a BSS color collision, an AP can change its own BSS color. The 802.11ax draft amendment does not define the BSS coloring standard or a method for selecting a new BSS color. WLAN vendors can customize BSS color selection protocols, such as the Aerohive Channel Selection Protocol (ACSP).

TWT

The battery life of STAs is primarily affected by **high-power-consumption applications**.

| Why TWT? | TWT implementation |
|---|--|
|  |  |

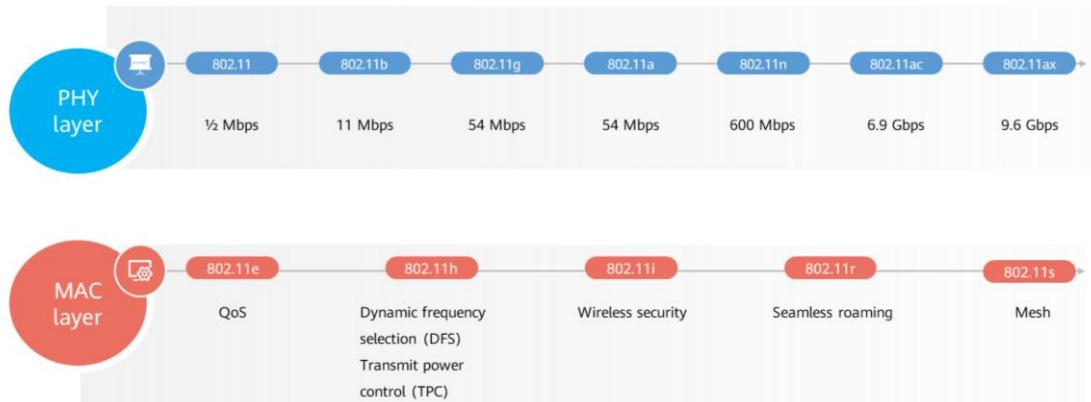
80 Huawei Confidential 

- Each generation of new Wi-Fi standards can extend the battery life of STAs by supporting faster and longer transmission to lower their power consumption. Wi-Fi 6 introduces target wakeup time (TWT), which allows an AP to inform a STA when to sleep and provide a scheduling table defining when the STA is awake. Even though a STA sleeps for a short period of time each time, multiple sleeps significantly prolong the battery life of the STA.
- TWT was first proposed in the 802.11ah standard. This mechanism is designed to save energy for IoT devices, especially for devices with low traffic volume such as smart electricity meters. It allows IoT devices to stay in the sleep state as long as possible, reducing power consumption. After a TWT agreement is established, a STA wakes up after a longer period of time, without the need of receiving a Beacon frame. The 802.11ax standard improves on TWT by defining rules for STA behaviors and implementing channel access control on the premise of meeting energy saving requirements. TWT is classified into unicast TWT and broadcast TWT.

Contents

1. Basic Concepts of Wireless Communication
2. Key WLAN Technologies
- 3. Introduction to 802.11 Standards**

IEEE 802.11 Family



82 Huawei Confidential

 HUAWEI

- The IEEE 802.11 Working Group defines the standards related to:
 - 802.11 PHY layer
 - 802.11 MAC layer
- 802.11 PHY standards define the frequencies, MCSs, and maximum rates of wireless standards.
 - IEEE 802.11: In 1990, the IEEE Standards Association (IEEE-SA) set up the IEEE 802.11 Working Group, which defined 802.11 standards. The 802.11 standard specifies the set of MAC layer and PHY protocols for implementing WLAN communication. It defines signal characteristics and MCSs in data transmission at the PHY. According to the 802.11 standard, WLANs work at frequencies from 2.4 GHz to 2.4835 GHz and the maximum data rate is 2 Mbps.
 - IEEE 802.11a: Published in 1999, 802.11a defines the frequency of WLANs, which is between 5.15 GHz and 5.825 GHz. The maximum data rate is 54 Mbps.
 - IEEE 802.11b: IEEE 802.1b was approved in September 1999. According to 802.1b, WLANs work at 2.4 GHz to 2.4835 GHz. The maximum data rate is 11 Mbps.
 - IEEE 802.11g: IEEE 802.11g improves the data rate from 11 Mbps (802.11b) to 54 Mbps. 802.11g APs support access of 802.11b and 802.11g STAs.

IEEE 802.11 Standards and Wi-Fi Generations

| Standard | | Released In | Frequency Band | PHY Technologies | Modulation Scheme | Number of Spatial Streams | Channel Bandwidth (MHz) | Theoretical Rate |
|----------|-----------------|-------------|----------------|-----------------------------|-------------------|---------------------------|-------------------------|---------------------------------------|
| - | 802.11 | 1997 | 2.4 GHz | IR, FHSS, DSSS | - | - | 20 | 2 Mbps |
| - | 802.11b | 1999 | 2.4 GHz | DSSS/CCK | - | - | 22 | 11 Mbps |
| - | 802.11a | 1999 | 5 GHz | OFDM | - | - | 20 | 54 Mbps |
| - | 802.11g | 2003 | 2.4 GHz | OFDM | 64-QAM | - | 20 | 54 Mbps |
| Wi-Fi 4 | 802.11n | 2009 | 2.4 GHz, 5 GHz | OFDM DSSS/CCK | 64-QAM | 4 | 20, 40 | 2.4 GHz: 450 Mbps 5 GHz: 600 Mbps |
| Wi-Fi 5 | 802.11ac Wave 1 | 2013 | 5 GHz | OFDM SU-MIMO | 64-QAM | 4+4 | 20, 40 | 3.74 Gbps |
| | 802.11ac Wave 2 | 2015 | 5 GHz | OFDM DL MU-MIMO | 256-QAM | 8 | 20, 40, 80, 160, 80+80 | 6.9 Gbps |
| Wi-Fi 6 | 802.11ax | 2019 | 2.4 GHz, 5 GHz | OFDMA DL MU-MIMO UL MU-MIMO | 1024-QAM | 4+8 | 20, 40, 80, 160, 80+80 | 2.4 GHz: 1.15 Gbps 5 GHz: 9.6 Gbps |

802.11a/b/g

- 802.11a (5 GHz)
 - OFDM
 - Data rates: 6, 9, 12, 18, 24, 36, 48, 54, in Mbps
 - Working on the license-free 5 GHz frequency band; 23 non-overlapping channels available
- 802.11b (2.4 GHz)
 - Direct sequence spread spectrum (DSSS)
 - Data rates: 1, 2, 5.5, 11, in Mbps
 - Channel bandwidth: 22 MHz
- 802.11g (2.4 GHz)
 - OFDM
 - Data rates: 6, 9, 12, 18, 24, 36, 48, 54, in Mbps, and rates in 802.11b
 - Compatible with 802.11b STAs

802.11n

The IEEE 802.11 Working Group established a high throughput (HT) research group in 2002 on the next-generation standard, and officially released IEEE 802.11n that is based on **MIMO-OFDM** in 2009. 802.11n improves network throughput over the two previous standards — 802.11a and 802.11g — with a significant increase in the maximum data rate.



Huawei 802.11n-compliant AP
(with external antennas)

| Frequency Band | 802.11 Standards and Maximum Theoretical Rates | |
|----------------|--|--------------------------|
| 2.4 GHz | 802.11g: 54 Mbps | 802.11n: 450 Mbps |
| 5 GHz | 802.11a: 54 Mbps | 802.11n: 600 Mbps |

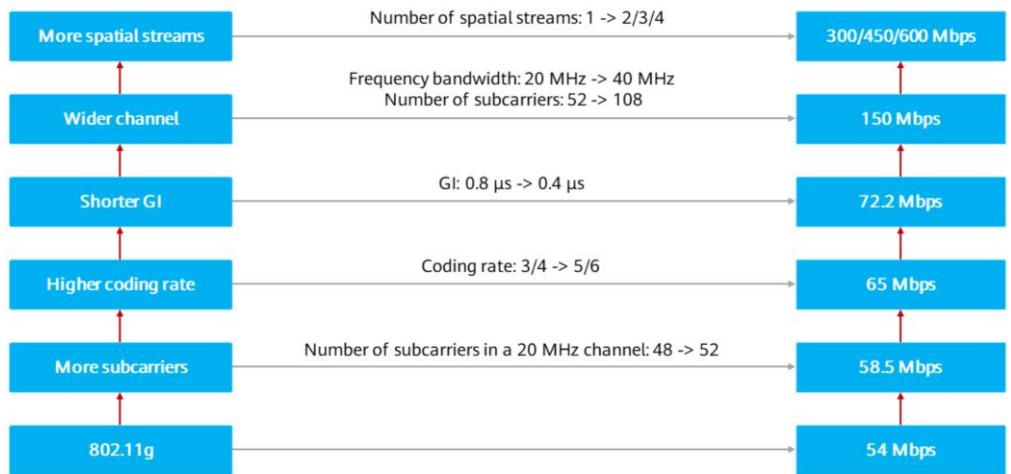
802.11n introduces many new technologies, which bring brand-new user experience, greatly promote the development of the WLAN industry, and make Wi-Fi popular. Up to now, a large number of 802.11n STAs are still used on the live network.

Brand-new technologies



- Different from 802.11a/b/g, 802.11n works in dual-band mode (2.4 GHz and 5 GHz frequency bands). Therefore, 802.11n is compatible with 802.11a/b/g.
- To improve the QoS of real-time services, 802.11n defines single-user beamforming technology to improve the signal receiving quality. It also incorporates the 802.11e (QoS) standard amendment, requiring 802.11n devices to support 802.11e features. In addition, 802.11n uses antenna and wireless transmission technologies, which greatly increase the transmission distance of WLANs to several kilometers while guaranteeing the data rate of 100 Mbps.
- 802.11n combines PHY and MAC layer technologies to improve the WLAN throughput. The main PHY technologies include MIMO, MIMO-OFDM, 40 MHz channel bonding, and short GI, which help to increase the PHY throughput to 600 Mbps. However, if only the PHY rate is improved but the MAC layer functions such as air interface access are not optimized, the PHY efficiency optimization cannot be achieved in 802.11n. This is similar to a wide road. Traffic jams and low efficiency are still problems if traffic scheduling and management are not optimized. To resolve such problem, 802.11n uses technologies such as block acknowledgment and frame aggregation, which greatly improve the MAC layer efficiency.
- Forward Error Correction (FEC): According to the basic principles of wireless communication, to make information suitable for transmission over unreliable media such as wireless channels, the transmitter encodes information to be sent and adds on redundant information to improve the system's error correction capability and allow the receiver to restore the original information. The QAM-64 encoding mechanism used by 802.11n can increase the coding rate of an FEC code (proportion of useful data) from 3/4 (in 802.11g) to 5/6. Therefore, with MIMO-OFDM, the physical rate of a spatial stream can be improved from 58.5 Mbps in 802.11g to 65 Mbps (that is, 58.5 Mbps times 5/6 divided by 3/4).

802.11n Key Technologies



- 802.11n supports a maximum rate of 600 Mbps thanks to the following:
 - Supports a maximum of four spatial streams.
 - Supports channel bonding. In 5 GHz scenarios, each channel supports a maximum of 108 subcarriers.
 - Uses short GI technology, reducing the GI from 0.8 μ s to 0.4 μ s.
 - Improves the coding rate from 3/4 to 5/6.
 - Delivers a data rate of up to 300 Mbps with the 20 MHz channel bandwidth and 600 Mbps with the 40 MHz channel bandwidth.

802.11ac

The IEEE 802.11 Working Group officially released the 802.11ac standard in 2014, which is also known as the Very High Throughput (VHT) standard. This standard signifies that the data rate of WLANs reaches the gigabit level. Note that 802.11ac supports **only the 5 GHz frequency band**.

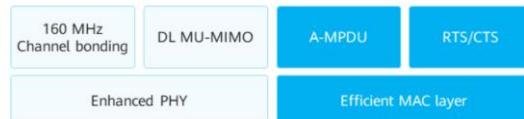


Huawei 802.11ac-compliant AP

| Frequency Band | 802.11 Standards and Maximum Theoretical Rates | |
|----------------|--|----------------------------------|
| 2.4 GHz | 802.11n: 450 Mbps | 802.11ac: Not supported |
| 5 GHz | 802.11n: 600 Mbps | 802.11ac Wave 2: 6.9 Gbps |

High throughput has always been the goal of Wi-Fi standards. To achieve higher bandwidth, 802.11ac has made new breakthroughs based on the original technologies. Compared with 802.11n, 802.11ac increases the maximum number of supported spatial streams from four to eight, and increases the channel bandwidth from 40 MHz to 160 MHz. In addition, 802.11ac introduces MU-MIMO technology to support downlink concurrent multi-user transmission.

Brand-new technologies



- 802.11ac has made many technological innovations, and it takes a long time to market these innovations into Wi-Fi products. Therefore, the Wi-Fi Alliance separated the introduction of 802.11ac products into two phases: Wave 1 and Wave 2. In this way, 802.11ac products can be quickly launched to the market to meet the rapidly increasing traffic requirements. Meanwhile, 802.11ac is evolvable to maintain the competitiveness of Wi-Fi.
- 802.11ac also enables seamless roaming of enterprise or home users, while supporting security, management, and diagnosis applications of Wi-Fi products during roaming.
- 802.11ac uses new technologies while extending original technologies to improve the maximum throughput and the number of access users. The technologies include more spatial streams, 256-QAM, and MU-MIMO.
- It defines downlink MU-MIMO (DL MU-MIMO) technology to support concurrent downlink multi-user transmission.
- 802.11ac extends A-MPDU technology.
 - 802.11n and later 802.11 standards introduce frame aggregation technology at the MAC layer to aggregate MSDUs or MPDUs before encapsulating them into PHY packets. In this way, multiple MSDUs or MPDUs share one PHY header, improving encapsulation efficiency, saving air interface resources, and reducing the number of times for preempting air interface resources.
 - Upon an error in the transmission of an A-MSDU, the entire A-MSDU needs to be retransmitted. In contrast, each MPDU in an A-MPDU has their own MAC headers. Upon an error in the transmission of an A-MPDU, only the MPDU with the error needs to be retransmitted.
 - 802.11ac data frames must be sent in A-MPDU mode. That is, A-MPDU cannot be disabled.

802.11ax

IEEE 802.11ax, marketed as Wi-Fi 6 by the Wi-Fi Alliance, is also known as the High-Efficiency Wireless (HEW) standard. 802.11ax supports both the 2.4 GHz and 5 GHz frequency bands, and is backward compatible with 802.11a/b/g/n/ac.

| Frequency Band | 802.11 Standards and Maximum Theoretical Rates | |
|----------------|--|----------------------------|
| 2.4 GHz | 802.11n: 450 Mbps | 802.11ax: 1.15 Gbps |
| 5 GHz | 802.11ac Wave 2: 6.9 Gbps | 802.11ax: 9.6 Gbps |



Huawei 802.11ax-compliant AP

To achieve higher bandwidth, 802.11ax adopts most technologies of 802.11ac and redefines Orthogonal frequency division multiple access (OFDMA) technology. It supports a narrower subcarrier spacing, and uses the 1024-QAM modulation and coding scheme (MCS). In addition, 802.11ax introduces UL MU-MIMO technology, which enables the theoretical rate of Wi-Fi 6 APs to exceed 10 Gbps and improves the throughput and quality of service (QoS) in high-density scenarios.



93 Huawei Confidential

HUAWEI

- The Wi-Fi Alliance launched the "Wi-Fi CERTIFIED 6" certification program on September 16, 2019, and announced IEEE 802.11ax that operates on the 6 GHz frequency band as Wi-Fi 6E on January 3, 2020.
- You may be very familiar with the concept of MU-MIMO. DL MU-MIMO introduced in 802.11ac may bring the following problems:
 - Many STAs use single antennas, and dual-antenna STAs need to switch to the single-stream DL MU-MIMO mode to prevent interference. The gain of an AP with four antennas is moderate compared with that of a single-antenna STA.
 - Even if an AP has eight antennas, it can exchange data with a maximum of only four STAs.
 - Channel probe responses from STAs are sent continuously, resulting in a high overhead.
 - Without UL MU enhancement, TCP/IP performance with TCP ACK in the uplink direction is weakened.
 - UL MU-MIMO was originally considered in 802.11ac, but was not introduced due to implementation issues.
- 802.11ax enhances the MU-MIMO function by supporting UL MU-MIMO:
 - Probe frames and data frames can be exchanged with multiple STAs to reduce the overhead and the uplink response time.
 - 8x8 DL/UL MU-MIMO is supported. The MU-MIMO throughput can be doubled or

quadrupled in single-user communication even if an AP works in single-stream mode.

Theoretical Data Rate of Wi-Fi 6: 10.75 Gbps

Device rate = Number of spatial streams × Number of code bits per subcarrier × Coding rate × Number of valid subcarriers
Symbol + GI

$$\text{Rate at 2.4 GHz} = \frac{4 \times 10 \text{ bits} \times 5/6 \times 468}{(12.8 + 0.8) \times 10^{-6} \text{ s}} = 1147 \times 10^6 \text{ bps} = 1147 \text{ Mbps}$$

$$\text{Rate at 5 GHz} = \frac{8 \times 10 \text{ bits} \times 5/6 \times 1960}{(12.8 + 0.8) \times 10^{-6} \text{ s}} = 9607 \times 10^6 \text{ bps} = 9607 \text{ Mbps}$$

Symbol and GI

| | 802.11ac and Earlier | 802.11ax |
|------------------------------|----------------------|------------|
| Fast Fourier transform (FFT) | 64-point | 256-point |
| Subcarrier spacing | 312.5 kHz | 78.125 kHz |
| Symbol duration | 3.2 us | 12.8 us |
| Short GI | 0.4 us | / |
| GI | 0.8 us | 0.8 us |
| 2 x GI | / | 1.6 us |
| 4 x GI | / | 3.2 us |

Why cannot 802.11ax use short GI technology?

Link setup rate over the air interface

1. 802.11ax
2. 8x8 MIMO
3. GI
4. 1024-QAM
5. Coding rate of channels: 5/6
6. 160 MHz, 1960 valid subcarriers (5 GHz)
7. 40 MHz, 468 valid subcarriers (2.4 GHz)

Number of valid subcarriers

| | 802.11ac and Earlier | 802.11ax |
|-----------------------------|----------------------|------------|
| FFT | 64-point | 256-point |
| Subcarrier spacing | 312.5 kHz | 78.125 kHz |
| Number of valid subcarriers | | |
| 20 MHz | 52 | 234 |
| 40 MHz | 108 | 468 |
| 80 MHz | 234 | 980 |
| 160 MHz | 468 | 1960 |

Up to 40 MHz at 2.4 GHz

Up to 160 MHz at 5 GHz



- Spatial stream

- Each of Huawei Wi-Fi 6 APs has four 2.4 GHz antennas and supports four spatial streams on the 2.4 GHz frequency band. Due to protocol restrictions, the 5 GHz frequency band can support a maximum eight spatial streams. Therefore, Huawei Wi-Fi 6 APs support a maximum of eight spatial streams on the 5 GHz frequency band.

- Coding scheme or number of code bits per subcarrier

- The coding scheme, also called the modulation scheme, converts signals generated by a signal source into a form suitable for wireless transmission (that is, number of bits that can be carried in one symbol).
- There are three basic modulation schemes: amplitude-shift keying (ASK), frequency-shift keying (FSK), and phase-shift keying (PSK). Other modulation schemes are all improvements or mixtures of these three schemes. For example, quadrature amplitude modulation (QAM) used by Wi-Fi is considered as a mixture of amplitude modulation and phase modulation.
- For example, 802.11ax uses 1024-QAM, which means that the size of data carried by each subcarrier is 10 bits (that is, $\log_2 1024$). 802.11ac uses 256-QAM, defining that the size of data carried by each subcarrier is 8 bits ($\log_2 256$). To put it simply, Wi-Fi 6 (802.11ax) uses 1024-QAM and each subcarrier transmits data of 10 bits ($2^{10} = 1024$), whereas Wi-Fi 5 (802.11ac) uses 256-QAM and each subcarrier transmits data of 8 bits ($2^8 = 256$).

Quiz

1. What technologies are used at the 802.11 PHY layer?
2. What is MIMO technology?

- 1. OFDM, OFDMA, MU-MIMO, QAM, Channel Bonding, BSS Coloring...
- 2. Frame Aggregation, Block Acknowledgement (BA), A-MPDU, RTS/CTS

Summary

- This course focuses on the basics and technologies of WLAN, introduces 802.11 standards, and details 802.11 PHY and MAC layer technologies.
- Upon completion of this course, you will have a basic understanding of WLAN, especially the advantages of Wi-Fi 6.

Recommendations

- What Is 802.11ax (Wi-Fi 6):
https://support.huawei.com/enterprise/en/doc/EDOC1100102755/d5da9bbc?idPath=24030814|21782164|21782201|22318528#EN-US_TOPIC_0189760680
- Huawei Wi-Fi 6 (802.11ax) Technology White Paper:
<https://e.huawei.com/en/material/networking/wlan/f3ae84efd98d440eb457b4caf405b509>

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future, market opportunities, product offerings and/or future performance, portfolio, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



WLAN Fundamentals



Foreword

- Traditionally, two WLAN architectures are available: Fat AP and AC + Fit AP. A Fat AP integrates WLAN management functions including user authentication, data encryption, and roaming, but brings a heavy deployment workload for a large WLAN. With the growth in wireless terminals, the AC + Fit AP architecture is widely applied, which is easy to control and expand. Communication between the AC and Fit APs is implemented using Control and Provisioning of Wireless Access Points (CAPWAP).
- In this course, we will get a glimpse into the origin and implementation of CAPWAP, key 802.11 frames, and STA roaming mechanism.

Objectives

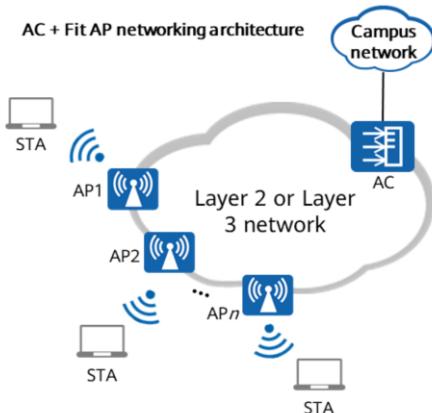
Upon completion of this course, you will be able to:

- Describe the origin and implementation of CAPWAP.
- Understand the CAPWAP tunnel establishment process.
- Describe how an AP joins an AC and how STAs go online.
- Master the working mechanism of STA roaming.

Contents

- 1. CAPWAP Tunnel**
2. Key 802.11 Frames
3. STA Going-Online Process
4. WLAN Roaming

CAPWAP Background



Challenges of traditional Fat AP networking

- An enterprise needs to deploy a large number of APs, which poses higher requirements on centralized O&M, control, and security.
- Traditional Fat AP networking encounters the following challenges:
 - Autonomous management, bringing security risks
 - No fine-grained user management and control
 - Difficult large-scale deployment, applicable only to SOHO small-scale networking

Solution

- The AC + Fit AP networking architecture applies to medium- and large-scale networks and has the following advantages over the Fat AP architecture:
 - Centralized, visualized management and control, reducing O&M costs
 - Fine-grained policy management for users
 - Authentication and accounting to safeguard enterprise data security at different layers
 - Value-added service capability, enriching services
- Under this background, **CAPWAP** — Control and Provisioning of Wireless Access Points, is developed for communication between the AC and APs.

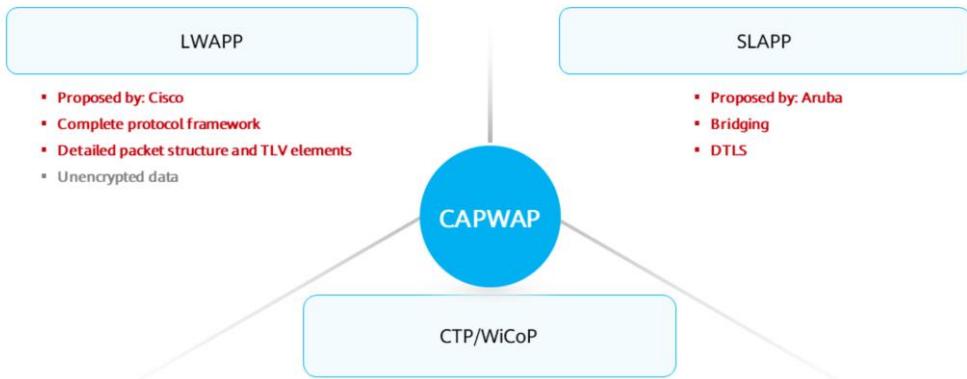


Origin of CAPWAP

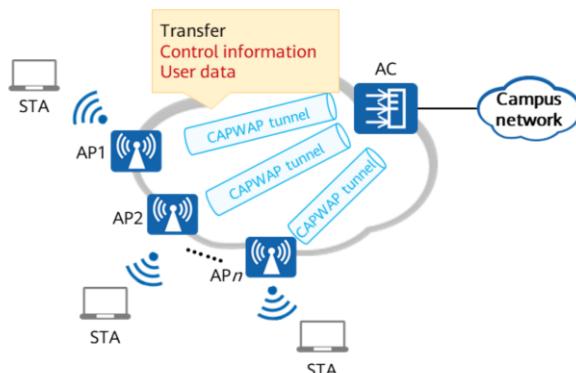
| Protocol | LWAPP | SLAPP | CTP | WiCoP |
|-----------------|--|--|---|---|
| Standard | RFC 5412 | RFC 5413 | draft-singh-capwap-ctp | RFC 5414 |
| Full name | Lightweight Access Point Protocol | Secure Light Access Point Protocol | CAPWAP Tunneling Protocol | Wireless LAN Control Protocol |
| Proposed by | Cisco - Airspace | Aruba | Siemens - Chantry | Panasonic |
| Characteristics | LWAPP gives a comprehensive description of detection, security and system management methods. Supports local MAC address and split MAC address. ACs and APs are connected at Layer 2 or Layer 3. At Layer 2, LWAPP packets are transmitted in Ethernet frames. At Layer 3, LWAPP packets are transmitted using user datagram protocol (UDP). | SLAPP supports two local MAC modes: bridging and tunnel, and allows for direct, Layer 2, and Layer 3 connection modes. It uses mature technologies and standards to build communication tunnels, and leverages GRE technology to set up data channels. | CTP uses extended SNMP to configure and manage WTPs. CTP control packets are used to control STA connection status, and WTP configuration and status. | WiCoP defines the AC discovery mechanism, including negotiation based on performance of the AC and STAs. This protocol also defines QoS parameters. |
| Encryption | Signaling: AES-CCM Data: not encrypted | Signaling: Datagram Transport Layer Security (DTLS) Data: DTLS | CTP defines authentication and a series of encryption rules based on AES-CCM, but the rules still need optimization. | WiCoP recommends IPsec and EAP security standards but does not specify implementation methods. |

- In the AC + Fit AP architecture, APs cannot work independently of the AC. Therefore, communication protocols are required for the interconnection between the AC and APs. The first tunnel communication protocol between APs and ACs, that is, LWAPP, was developed by Cisco. Then, the Internet Engineering Task Force (IETF) set up a CAPWAP working group in 2005 to tackle the problem that APs and ACs of different vendors cannot communicate, and to research large-scale WLAN solutions and standardized tunnel protocols for APs and ACs.
- The CAPWAP working group referred to the four different protocols above. LWAPP has a complete protocol architecture and defines detailed packet structure and multiple control messages. However, the effectiveness of the newly created security mechanism is yet to be proven. The highlight of SLAPP is the DTLS technology, which is highly applauded in the industry. CTP and WiCoP can satisfy the demands of a centralized WLAN architecture. However, they have some drawbacks, especially in terms of security.
- The CAPWAP working group compared and evaluated the four protocols, and finally developed the CAPWAP protocol, which is based on the LWAPP protocol and incorporates DTLS technology and features of the other three protocols.

CAPWAP Background



CAPWAP Overview



109 Huawei Confidential

CAPWAP tunnel

- CAPWAP defines how to manage and configure APs. That is, the AC manages and controls APs in a centralized manner through the CAPWAP tunnel.

Functions

- Allows APs to automatically discover an AC.
- Maintains the connectivity between the AC and APs.
- Allows the AC to manage APs and deliver service configurations to them.
- Allows APs to exchange data sent by STAs with the AC through CAPWAP tunnels in tunnel forwarding mode.

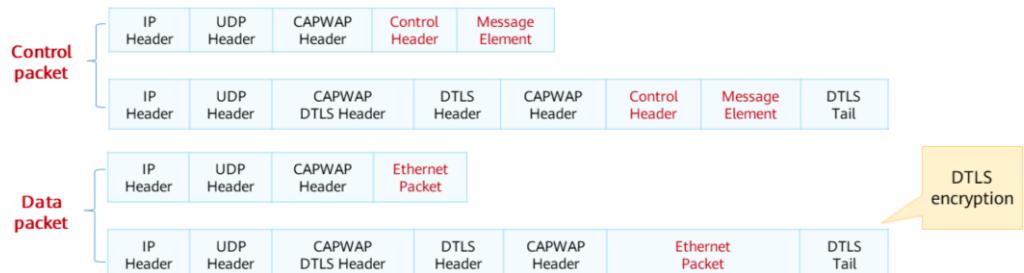


- Large-scale networking requires centralized management of multiple APs. However, the traditional WLAN architecture can no longer meet the requirements of large-scale networking. Therefore, the IETF set up a CAPWAP working group and developed the CAPWAP protocol.
- CAPWAP is an application-layer protocol based on UDP transmission.
 - CAPWAP functions in the transmission of two types of packets:
 - Data packets, which are encapsulated and forwarded through the CAPWAP data tunnel.
 - Control packets, which are exchanged for AP management through the CAPWAP control tunnel.
 - CAPWAP data and control packets are transmitted on different UDP ports:
 - The control packets are transmitted on UDP port of 5246.
 - The data packets are transmitted on UDP port of 5247.
- Note: The Internet Engineering Task Force (IETF)

CAPWAP Packet Format

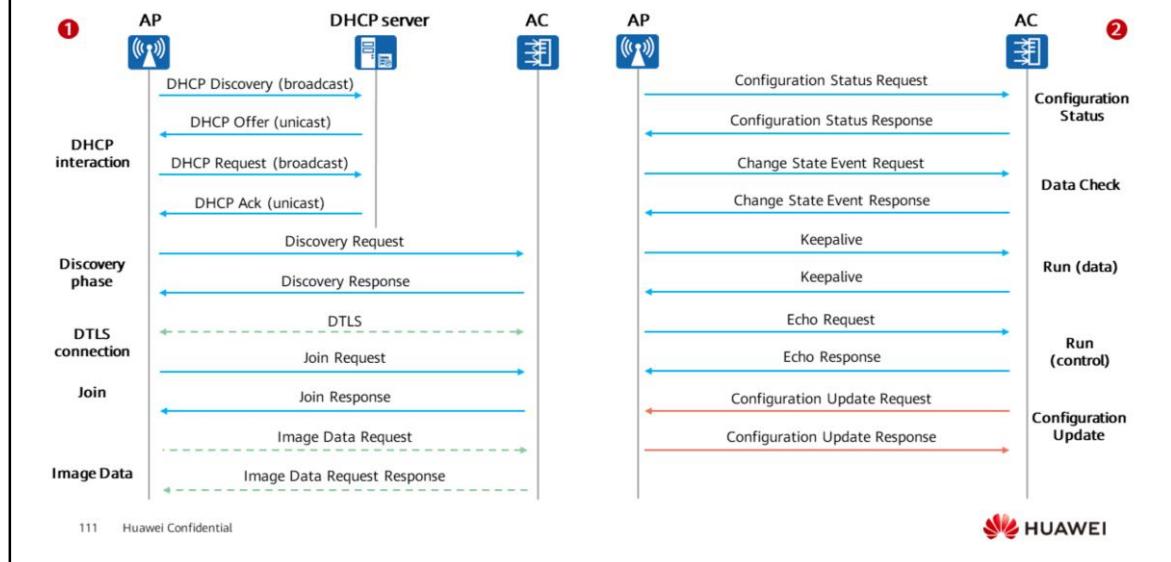
| Packet Type | Function | UDP Port | Encryption |
|----------------|-------------------------|----------|-------------------|
| Control packet | Managing APs | 5246 | Mostly ciphertext |
| Data packet | Forwarding service data | 5247 | Mostly plaintext |

The formats of the control packet and data packet are as follows:



- CAPWAP is an application-layer protocol based on UDP transmission.
- CAPWAP functions in the transmission of two types of packets:
 - Data packets, which are encapsulated and forwarded through the CAPWAP data tunnel.
 - Control packets, which are exchanged for AP management through the CAPWAP control tunnel.
- In a CAPWAP data tunnel, the information exchanged between APs and the AC is 802.11 wireless data, which is encapsulated and forwarded by using CAPWAP, and the information for maintaining the tunnel. In a CAPWAP control tunnel, the transmitted control information includes not only the control information for the AC to perform working parameter configuration on APs, but also the control information for maintaining the CAPWAP session. In control packets, except for Discovery Request and Discovery Response messages that are transmitted in plain text, the transmission of other requires DTLS encryption. As for the transmission of data packets, DTLS is optional.

CAPWAP Tunnel Establishment - Overview



- The process for establishing a CAPWAP tunnel includes phases such as DHCP interaction, Discovery, DTLS connection, Join, Image Data, Configuration Status, Data Check, Run (data), Run (control), etc.

CAPWAP Tunnel Establishment - APs Obtaining IP Addresses

- To communicate with an AC, an AP must obtain an IP address. This is the first step for wireless network communication.



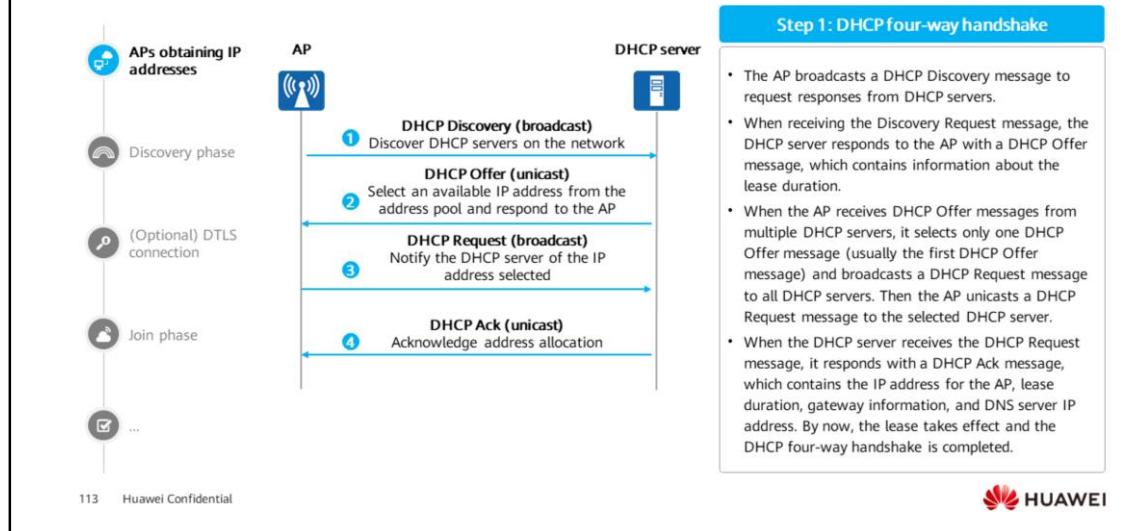
Mode in which an AP obtains an IP address

- Static mode: A user logs in to the AP and configures its IP address. (not recommended for medium- and large-scale networks)
- 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 network device, such as a core switch, to assign IP addresses to APs.

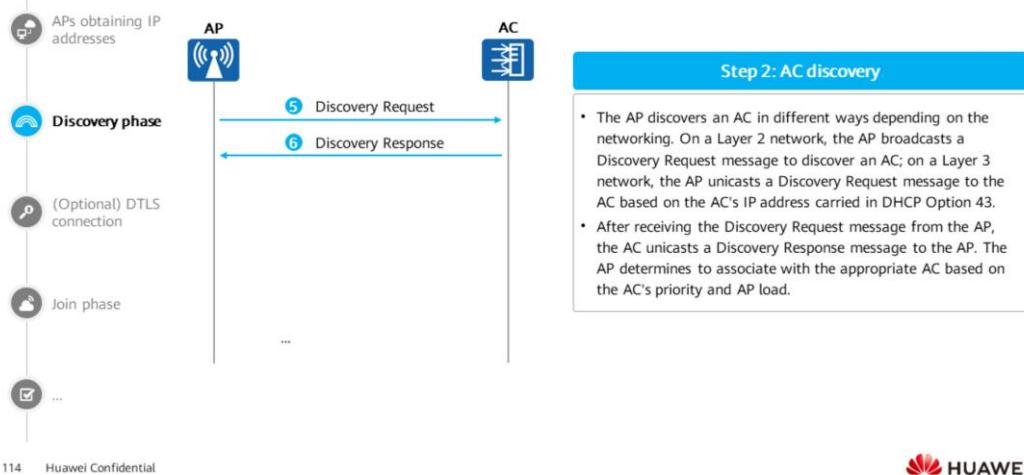
APs Obtaining IP Addresses - DHCP Interaction



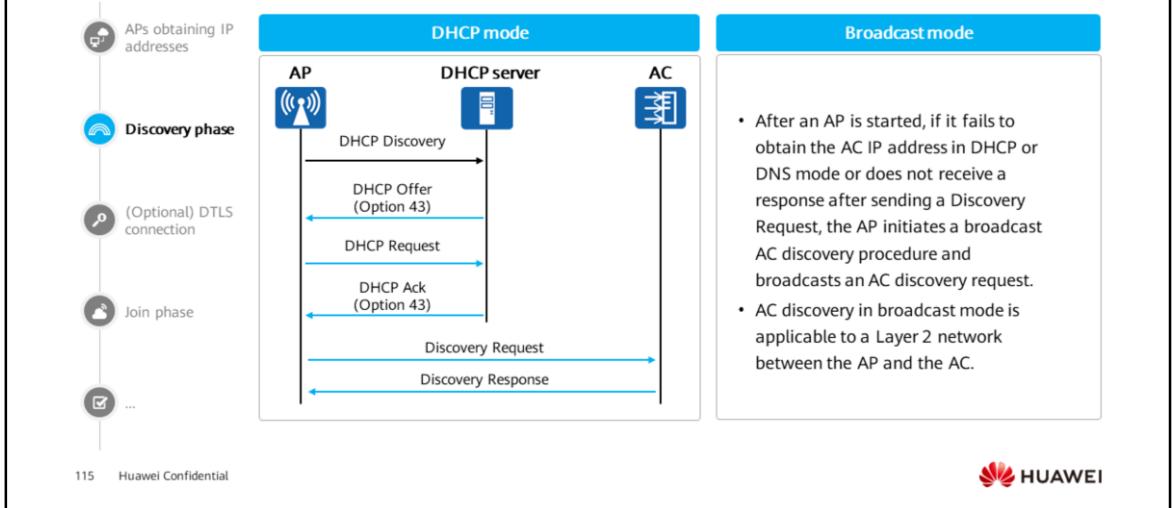
- The DHCP Ack message carries:
 - IP address of an AP
 - Lease duration
 - Gateway
 - DNS server IP
 - (Optional) AC IP address list in the Option 43 field for an AP to discover an AC
 - (Optional) Domain name of the DNS server in the Option 15 field

CAPWAP Tunnel Establishment - AC Discovery Phase

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



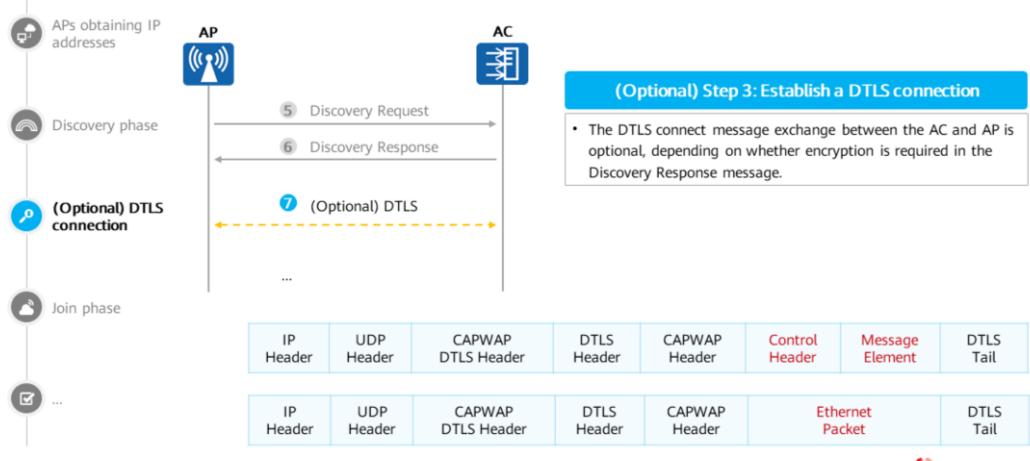
APs Dynamically Discovering the AC



- **DHCP mode:**
 - The AP obtains 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. In this process, the AP obtains an IP address through DHCP and the AC IP address list through the Option field in DHCP messages. (The DHCP server is configured to carry Option 43 in the DHCP Offer message, and Option 43 contains the AC IP address list.)
 - First, the AP broadcasts a DHCP Discovery message to the DHCP server. When receiving the DHCP Discovery message, the DHCP server encapsulates the first unleased IP address and other TCP/IP configuration in a DHCP Offer message containing the lease duration, and sends the message to the AP.
 - A DHCP Offer message can be a unicast or broadcast message. When the AP receives DHCP Offer messages from multiple DHCP servers, it selects only one DHCP Offer message (usually the first DHCP Offer message) and broadcasts a DHCP Request message to all DHCP servers. Then the AP unicasts a DHCP Request message to the selected DHCP server from which will allocate an IP address.
 - When the DHCP server receives the DHCP Request message, it responds with a DHCP Ack message, 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.

CAPWAP Tunnel Establishment - DTLS Phase

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

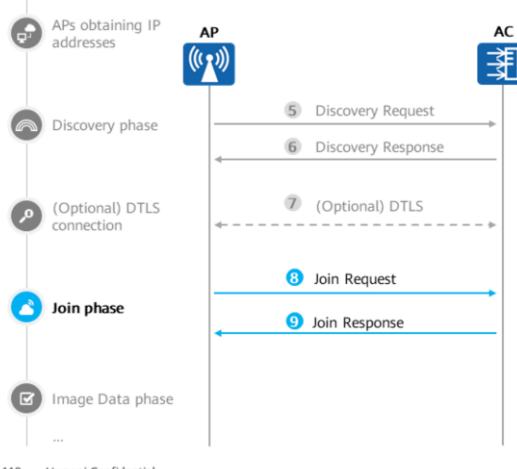


• DTLS handshake:

- After the AP obtains the AC IP address, it negotiates with the AC. After the AP receives a Discovery Response message from the AC, it starts to establish a CAPWAP tunnel with the AC. The DTLS protocol can be used to encrypt and transmit UDP packets.
- Datagram Transport Layer Security (DTLS)

CAPWAP Tunnel Establishment - Join Phase

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



Step 4: Join

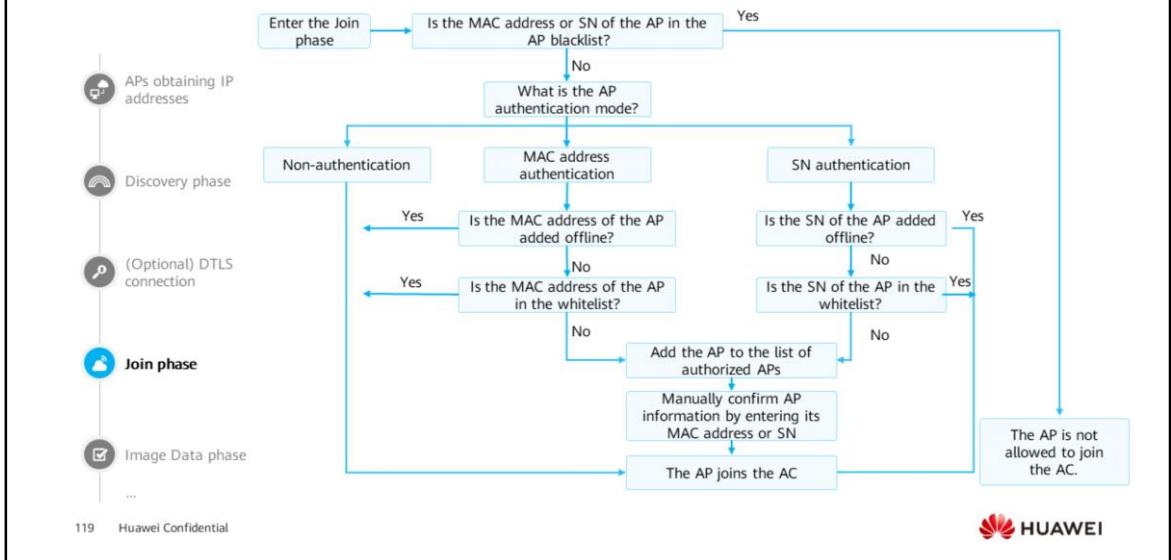
- After the DTLS handshake is completed, the AC and AP establish a control channel. The AP sends a Join Request message to request to join the AC.
- The AC sends a Join Response message containing information about user upgrade version number, the interval/timeout period of the handshake packet, and the priority of the control packets.

118 Huawei Confidential

HUAWEI

- An AC determines whether an AP is allowed to access based on the following steps:
 - 1. Check whether the AP is in the blacklist. If so, the AP access is not allowed. If not, the AC precedes the step 2.
 - 2. Check the AP authentication mode. If the AC does not have strict requirements for the AP to join and the authentication mode is non-authentication, then all APs that meet the condition in step 1 are allowed to join the AC. It is recommended that MAC address or SN authentication be used to strictly control AP access. If MAC address or SN authentication is used, the AC precedes the next step.
 - 3. Check whether the AP with corresponding MAC address or SN is added offline. If so, the AP is allowed to join the AC. Otherwise, the AC precedes the step 4.
 - 4. Check whether the MAC address or SN of the AP is in the whitelist. If so, the AP is allowed to join the AC. If not, the AC adds the AP to the unauthorized AP list.
 - 5. Unauthorized APs can be manually configured to join the AC. If an AP is not manually confirmed, it cannot connect to the AC.

AP Access Control Process



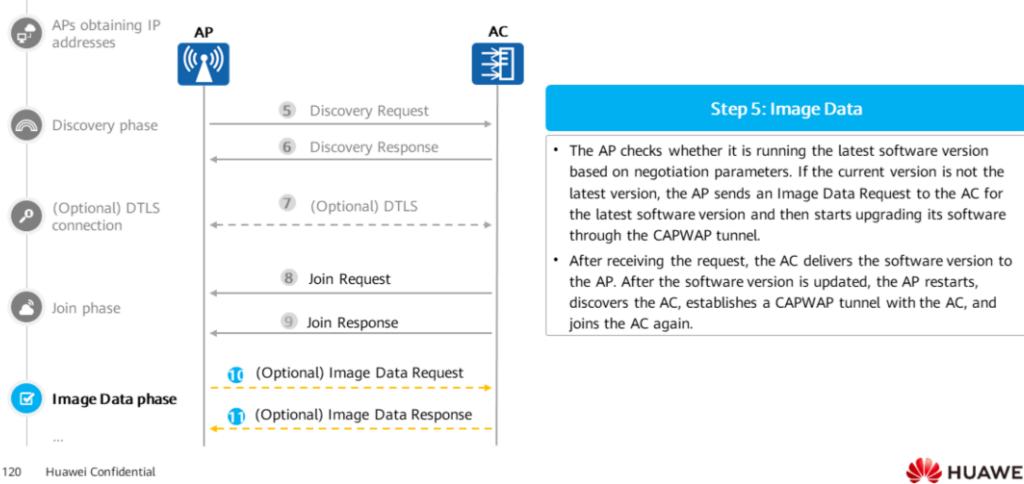
HUAWEI

- 1. Check whether the AP is in the blacklist.
 - If so, the AC rejects the access of the AP. That is, the AC does not respond to the AP's Discovery or Join Request message. As a result, the AP does not receive a Discovery or Join Response message and cannot perceive the presence of the AC. In this case, the AP continues to discover other ACs based on the preconfigured or dynamically obtained AC list. If the timer for the AP to wait for the Join Response message expires, the AP starts the AC discovery process again.
 - If not, the AC precedes the next step.
- 2. Check whether the MAC address or SN of the AP is in the preconfigured-AP list, containing the APs that went online or have been added in offline mode.
 - If so, the AP joins the AC directly.
 - If not, the AC precedes the next step.
- 3. Check whether the AP needs to be authenticated before going online.
 - If not, the AP joins the AC directly.
 - If so, the AC precedes the next step.
- 4. Check whether the MAC address or SN of the AP is in the whitelist.
 - If so, the AP can join the AC after passing authentication.
 - If not, the AC adds the AP to the unauthorized AP list. To allow the AP to join the AC, you need to enter the MAC address or SN of the AP and manually confirm the

information to bring the AP online.

CAPWAP Tunnel Establishment - Image Data Phase

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

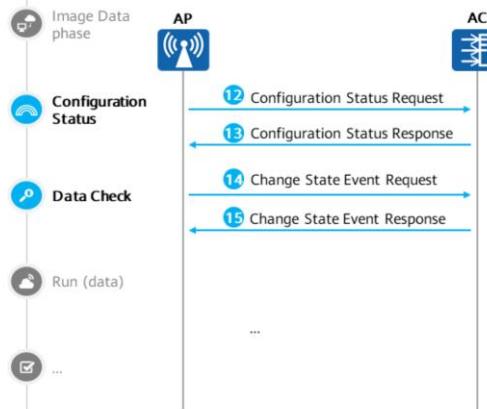


HUAWEI

- The AP determines whether its system software version is the same as that specified in the received Join Response message. If the two versions are different, the AP upgrades its software version. After the AP is upgraded, the AP restarts automatically and repeats all the previous authentication steps. If the two versions are the same or no version is specified in the Join Response message, the AP can directly enter the next phase without being upgraded.

CAPWAP Tunnel Establishment - Configuration Status and Data Check Phases

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



Step 6: Configuration Status

- The AP sends a Configuration Status Request message carrying the AC name and radio information to the AC and starts a timer for waiting for a Configuration Status Response message.
- After receiving the Configuration Status Request message, the AC changes its status and sends a Configuration Status Response message. (Currently, no configuration is delivered in this phase.) After receiving the Response message, the AP stops the timer and enters the Data Check phase.

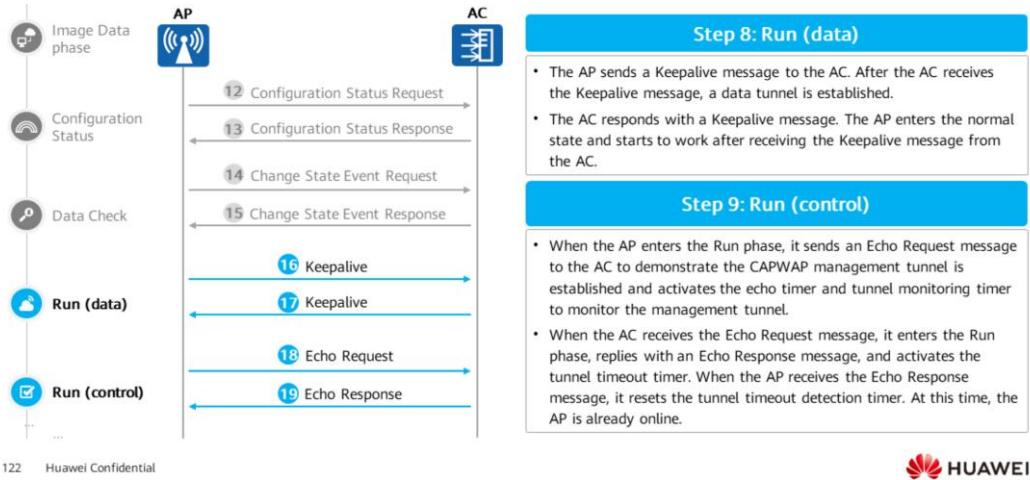
Step 7: Data Check

- The AP sends a Change State Event Request message carrying information such as the radio and result code and starts the timer for waiting for a Change State Event Response message.
- After receiving the Change State Event Request message, the AC enters the Data Check phase and sends a State Event Response message (currently, no error code is carried). After receiving the Change State Event Response message, the AP stops the timer and enters the Run phase.

HUAWEI

CAPWAP Tunnel Establishment - Run Phase

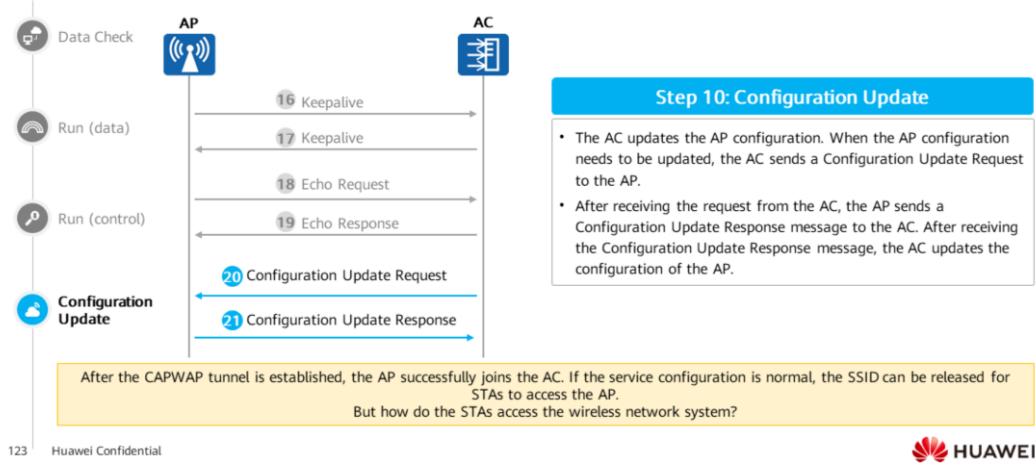
- The AC manages and controls APs in a centralized manner through CAPWAP tunnels.



- The AP sends a Keepalive message to the AC. A data tunnel is established after the message is received by the AC, and then the AP enters the normal state.
- By default, the AP sends data heartbeat messages at an interval of 25s to check whether the data link is normal.
- By default, the AP sends control heartbeat messages at an interval of 25s to check whether the control link is normal.

CAPWAP Tunnel Establishment - Configuration Update Phase

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

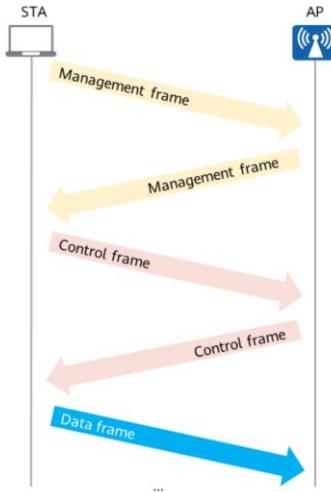


- After an AP joins an AC, it sends a Configuration Status Request message containing its configuration to the AC. This message is used to check whether the AP configuration matches that on the AC. If the AP configuration is different from that on the AC, the AC sends a Configuration Status Response message to the AP.
- Note: After an AP joins an AC, it obtains the current configuration from the AC. Then the AC manages the AP and delivers service configurations to it.

Contents

1. CAPWAP Tunnel
- 2. Key 802.11 Frames**
3. STA Going-Online Process
4. WLAN Roaming

Frame Types Defined in 802.11



- Management frame
 - Management frames perform supervisory functions; they are used to join and leave wireless networks and move associations from AP to AP.
- Control frame
 - Control frames are used in conjunction with data frames to perform area-clearing operations, channel acquisition and carrier-sensing maintenance functions, and positive acknowledgment of received data. Control and data frames work in conjunction to deliver data reliably from STA to STA.
- Data frame
 - Data frames carry data transmitted between STAs.

Key 802.11 Frames - Management Frames

| No. | Management Frame Type | Function |
|-----|--|--|
| 1 | Beacon frame | Beacon frames are sent periodically by an AP to notify STAs of a WLAN. An AP sends Beacon frames within the basic service area. |
| 2 | Probe Request frame | A STA sends Probe Request frames to scan surrounding 802.11 networks. |
| 3 | Probe Response frame | If the network scanned by a STA meets the connection requirement, the AP replies with a Probe Response frame to the STA. The AP responds to a received Probe Request frame only after it sends a Beacon frame and before it sends the next Beacon frame. |
| 4 | Authentication frame Deauthentication frame | An AP uses shared keys and Authentication frames to authenticate STA identities, and uses Deauthentication frames for deauthentication. |
| 5 | Association Request frame Reassociation Request frame | After a STA passes identity authentication, it sends an Association Request frame to request to join the network. When a STA needs to roam on a WLAN, it sends a Reassociation Request frame to reassociate with the WLAN. |
| 6 | Association Response frame | After receiving an Association Request from a STA, an AP replies with an Association Response frame. |

Key 802.11 Frames - Control Frames

| No. | Control Frame Type | Function |
|-----|-----------------------------|--|
| 1 | Request to send (RTS) frame | When a STA needs to send data to an AP, the STA sends an RTS frame to the AP. |
| 2 | Clear to send (CTS) frame | After an AP receives an RTS frame from a STA, it broadcasts CTS frames. After receiving the CTS frames, the other STAs within the AP's coverage area will not send data within a specified period. |
| 3 | Acknowledgment (ACK) frame | The receiver sends an ACK frame to confirm the receiving of a unicast packet from the sender. |
| 4 | PS-Poll frame | When a STA wakes up from the power save (PS) mode, it sends a PS-Poll frame to the associated AP to retrieve the frames buffered while it was in PS mode. |

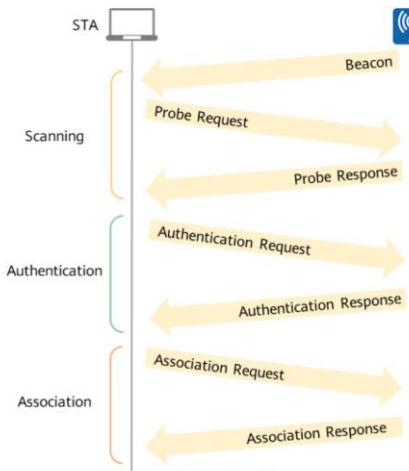
- PS-Poll mode

- IEEE 802.11 defines two working modes for STAs: active mode and PS mode.
- When a STA is in PS mode, the AP needs to buffer the data destined for the STA, and the power management bit in Beacon broadcast frames is set to 1.
- After the STA wakes up from the PS mode, it checks the power management bit in Beacon frames. If the power management bit is set to 1, the STA enters the active mode and sends a PS-Poll frame to the AP to retrieve the buffered data frames.
- By default, the duration of a PS-Poll frame is the time required to transmit an ACK frame plus one short interframe space (SIFS).

Contents

1. CAPWAP Tunnel
2. Key 802.11 Frames
- 3. STA Going-Online Process**
4. WLAN Roaming

STA Access

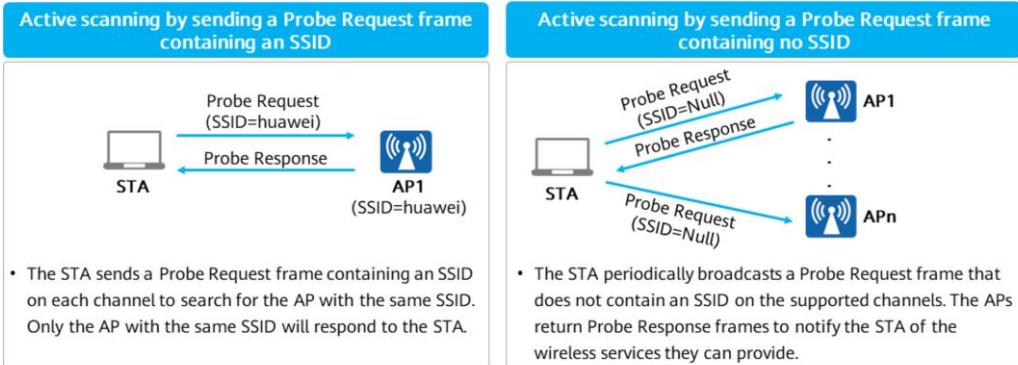


STA access

- STAs can access a WLAN after CAPWAP tunnels are established.
- STA access is divided into three stages:
 - Scanning
 - A STA periodically searches for nearby wireless networks through scanning.
 - Authentication
 - Before accessing the WLAN, a STA is authenticated, which is known as link authentication. Link authentication is usually considered as the start point for STAs to connect to an AP and access the WLAN.
 - Association
 - After link authentication is complete, the STA continues to initiate link service negotiation.

Active 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.



130 Huawei Confidential

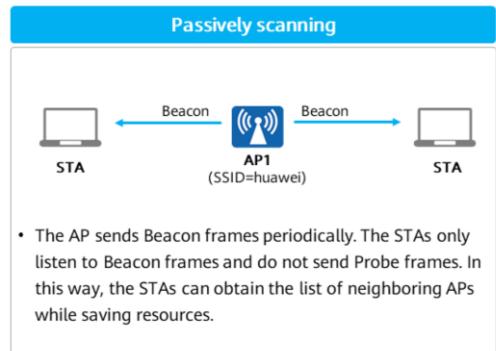
 HUAWEI

- Active scanning:

- Sending a Probe Request frame containing an SSID: applies when a STA actively scans wireless networks to access a specified wireless network.
- Sending a Probe Request frame containing no SSID: applies when a STA actively scans wireless networks to determine whether wireless services are available.

Passive Scanning

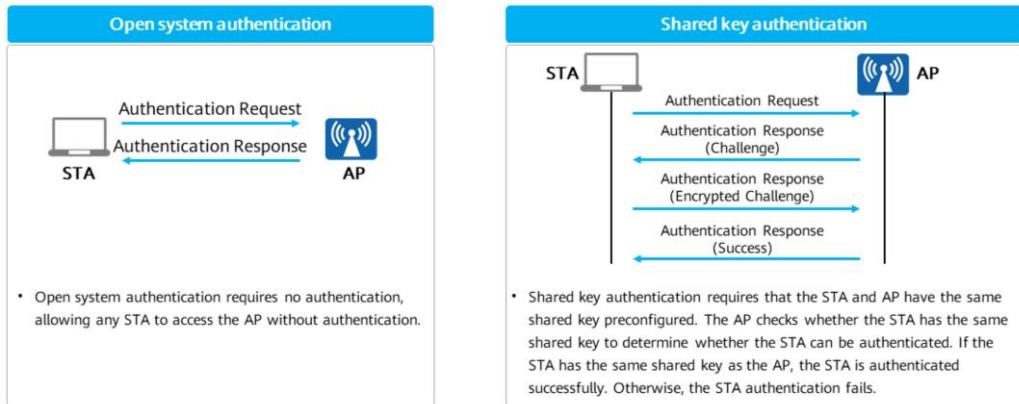
- In passive scanning mode, a STA receives Beacon frames that APs periodically send and obtains an AP list by parsing information in the Beacon frames.
- When listening to Beacon frames, the STA continuously switches channels to ensure that Beacon frames can be listened on each channel.
- By default, the interval for an AP to send Beacon frames is 100 TUs (1 TU = 1024 us).



- In passive scanning mode, a STA only listens to Beacon frames and does not send Probe frames, which saves resources. However, it takes a longer time to obtain the AP list in this mode than in active scanning mode. However, the time difference is only several seconds, which is acceptable to users.
- A STA supports both passive scanning and active scanning, so that it can discover an AP and connect to it quickly.
- After a STA is connected to an AP, both active scanning and passive scanning are allowed. However, some vendors may not implement both active scanning and passive scanning because this is not a mandatory requirement.
- The interval at which Beacon frames are sent can be dynamically adjusted. A shorter interval indicates that an AP can be discovered earlier.

Link Authentication

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



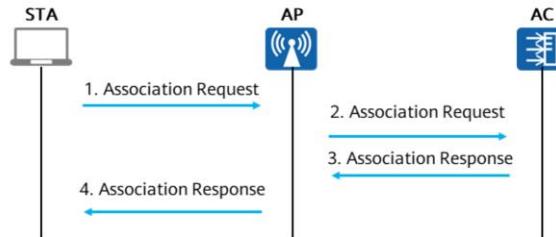
132 Huawei Confidential

HUAWEI

- A WLAN needs to ensure validity and security of STA access. Before accessing the WLAN, a STA must pass identity authentication, which is known as link authentication. Link authentication is usually considered as the start point for STAs to connect to an AP and access the WLAN.
- Shared key authentication process
 - A STA sends an Authentication Request message to an AP.
 - The AP generates a challenge and sends it to the STA.
 - The STA uses the preconfigured key to encrypt the challenge and sends it to the AP.
 - 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 authenticated successfully. Otherwise, the STA authentication fails.

Association

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

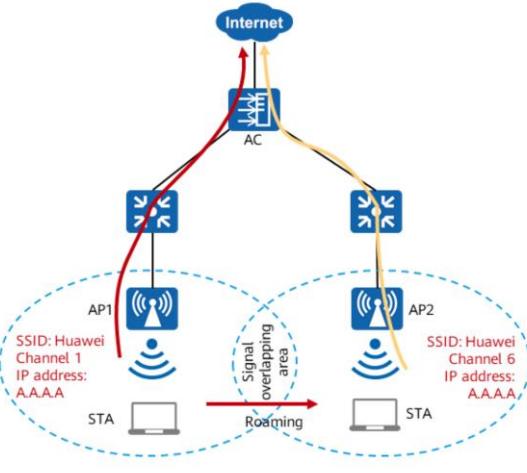


- STA association in the AC + Fit AP architecture consists of the following steps:
 - A STA sends an Association Request message to an AP. The Association Request message carries the STA's parameters and the parameters selected by the STA according to the service configuration, including the transmission rate, channel, and QoS capabilities.
 - The AP receives the Association Request message, encapsulates the message into a CAPWAP message, and sends the CAPWAP message to the AC.
 - The AC determines whether to authenticate the STA according to the received Association Request message and replies with an Association Response message.
 - The AP decapsulates the received Association Response message and sends it to the STA.

Contents

1. CAPWAP Tunnel
2. Key 802.11 Frames
3. STA Going-Online Process
- 4. WLAN Roaming**

WLAN Roaming Overview



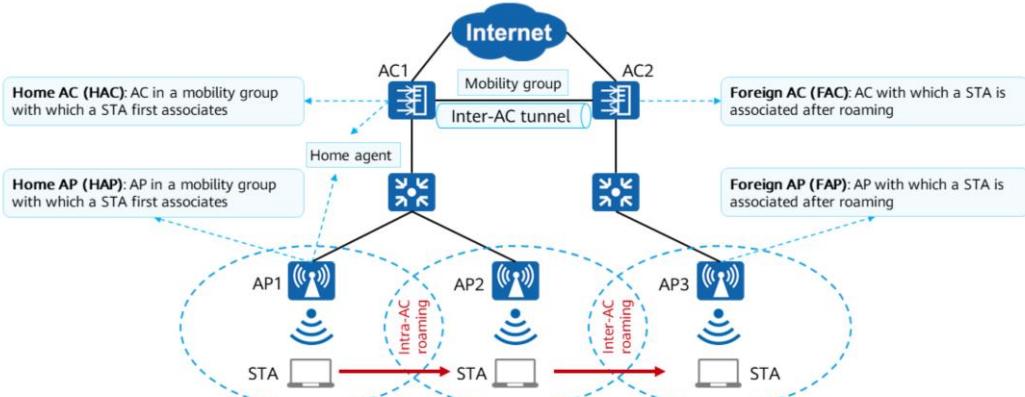
- WLAN roaming allows a STA to move between the coverage areas of different APs with nonstop service transmission.
- The APs involved in WLAN roaming must have the same SSID, same configurations in security profiles (different profile names allowed), and the same authentication mode and parameter settings in authentication profiles.
- WLAN roaming aims to achieve the following goals:
 - Avoid packet loss or service interruption caused by a long authentication duration during roaming.
 - Ensure that user's authorization information does not change during roaming.
 - Ensure that user's IP address does not change during roaming.

135 Huawei Confidential

 HUAWEI

- When a STA moves away from an AP, the link signal quality decreases gradually. If the signal quality falls below the roaming threshold, the STA proactively roams to a nearby AP with better signal quality.
- As shown in the figure, roaming is completed through the following steps:
 - The STA has set up a link with AP1 and sends Probe Request frames on various channels. After AP2 receives a Probe Request frame over channel 6 (channel used by AP2), it sends a Probe Response frame to the STA on channel 6. After the STA receives response frames, it evaluates which AP is more suitable to associate. In this case, the STA determines to associate with AP2.
 - The STA sends an Association Request frame to AP2 on channel 6, AP2 replies with an Association frame, so the association between the STA and AP2 is established. During the entire roaming process, the association relationship between the STA and AP1 is maintained.
 - To disassociate from AP1, the STA sends a Disassociation frame to AP1 over channel 1 (channel used by AP1).

Concepts in WLAN Roaming

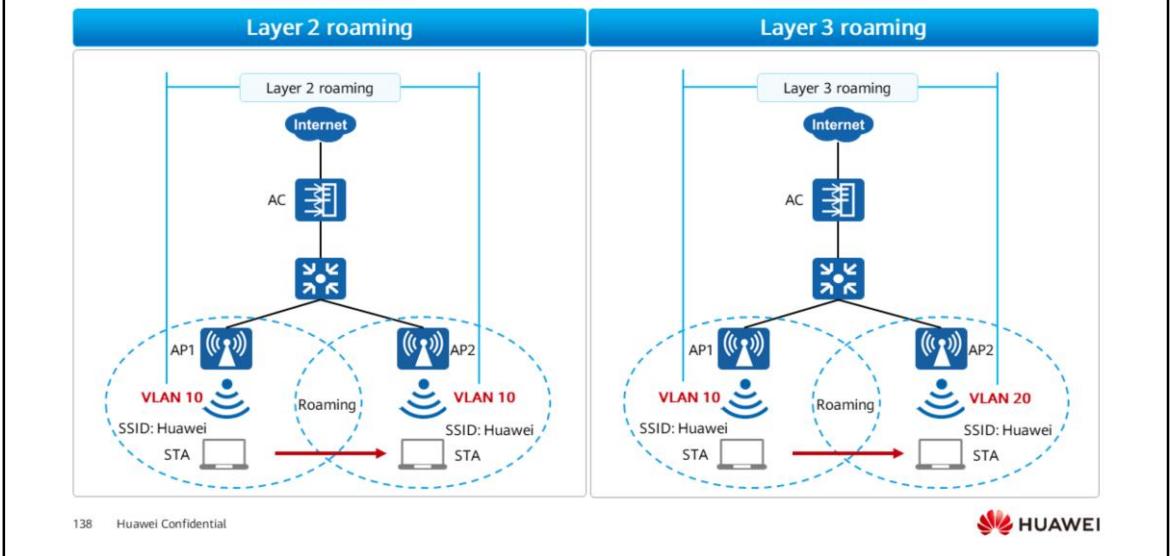


136 Huawei Confidential

HUAWEI

- Intra-AC roaming: A STA is associated with the same AC.
- Inter-AC roaming: A STA associates with different ACs.
- Inter-AC tunnel: To support inter-AC roaming, ACs in a mobility group need to synchronize STA and AP information with each other. Therefore, the ACs set up a tunnel to synchronize data and forward packets. An inter-AC tunnel is set up using the CAPWAP protocol. As shown in the figure, AC1 and AC2 set up a tunnel for data synchronization and packet forwarding.
- Mobility server
 - To enable STA roaming between ACs in a mobility group, you can configure an AC as the mobility server to maintain the membership table of the mobility group and deliver member information to ACs in the group. In this way, ACs in the mobility group can identify each other and set up inter-AC tunnels.
 - A mobility server can be an AC outside or inside a mobility group.
 - An AC can function as the mobility server of multiple mobility groups, but can be added to only one mobility group.
 - A mobility server managing other ACs in a mobility group cannot be managed by another mobility server. That is, if an AC functions as a mobility server to synchronize roaming configurations to other ACs, it cannot be managed by another mobility server or synchronize roaming configurations from other ACs. (An AC with a mobility group configured cannot be configured as a mobility server.)
 - As a centralized configuration point, a mobility server must be able to communicate with all managed ACs but does not need to provide high data forwarding capability.

WLAN Roaming Types



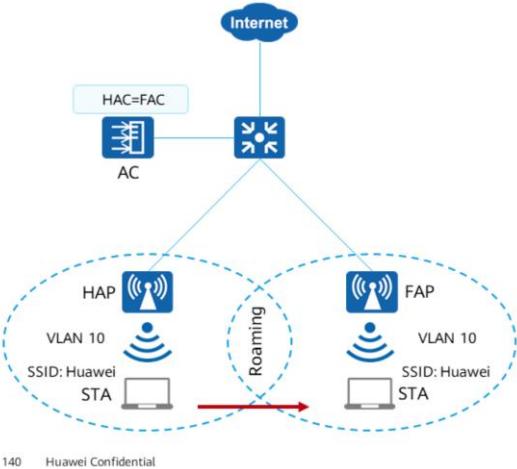
- Layer 2 roaming: A STA switches between two APs (or multiple APs) that are bound to the same SSID and have the same service VLAN ID (within the same IP address segment). During roaming, the access attributes (such as the service VLAN and obtained IP address) of the STA do not change, and packet loss and reconnection do not occur.
- Layer 3 roaming: Before and after roaming, the service VLANs of the SSIDs are different, and APs provide different Layer 3 service networks with different gateways. In this case, to ensure that the IP address of a roaming STA remains unchanged, the STA's traffic needs to be sent back to the AP on the initial access network segment to implement inter-VLAN roaming.
- Sometimes, two subnets may have the same service VLAN ID but are different subnets. Based on the VLAN ID, the system may incorrectly consider that STAs roam between the two subnets at Layer 2. To prevent this situation, configure a roaming domain to determine whether the STAs roam within the same subnet. The system determines Layer 2 roaming only when STAs roam within the same VLAN and same roaming domain; otherwise, the system determines Layer 3 roaming.

Traffic Forwarding Models in WLAN Roaming

- Depending on the WLAN data forwarding type and whether data is forwarded across Layer 3, traffic forwarding models in WLAN roaming are classified into four types, as described in the following table.

| Forwarding Model | Characteristics |
|--------------------------------------|---|
| Direct forwarding in Layer 2 roaming | STAs stay on the same subnet before and after Layer 2 roaming. Similar to packet forwarding for new STAs, the FAP or FAC forwards packets of Layer 2 roaming STAs on the local network but does not send the packets back to the home agent over a tunnel. |
| Tunnel forwarding in Layer 2 roaming | Service packets between the HAP and HAC are not encapsulated with the CAPWAP header. Therefore, whether the HAP and HAC reside on the same subnet cannot be determined. In this case, packets are forwarded back to the HAP by default. |
| Direct forwarding in Layer 3 roaming | Service packets between the HAP and HAC are encapsulated with the CAPWAP header. In this case, the HAP and HAC can be considered on the same subnet. Instead of forwarding the packets back to the HAP, the HAC directly forwards the packets to the upper-layer network. |
| Tunnel forwarding in Layer 3 roaming | |

Intra-AC Roaming



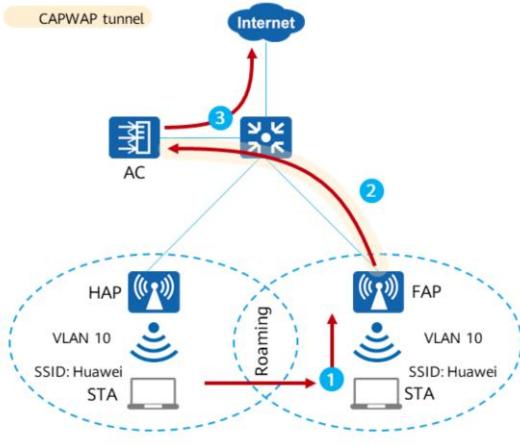
- Intra-AC roaming: If a STA roams within the coverage of the same AC, the roaming is intra-AC roaming.
- Intra-AC roaming can be regarded as a special case of inter-AC roaming where the HAC and FAC are the same AC.

140 Huawei Confidential

 HUAWEI

- Intra-AC roaming: If a STA roams within the coverage of the same AC, the roaming is intra-AC roaming. As shown in the figure, the STA roams from HAP to FAP, which is intra-AC roaming.

Intra-AC Layer 2 Roaming - Tunnel Forwarding



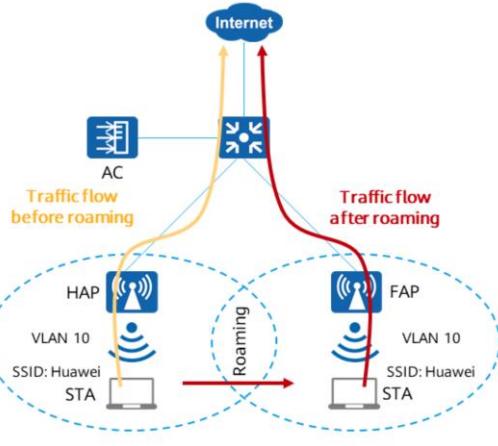
- Before roaming:

- The STA sends service packets to the HAP.
- After receiving the service packets, the HAP sends them to the AC through the CAPWAP tunnel.
- The AC forwards the service packets to the upper-layer network through the switch.

- After roaming:

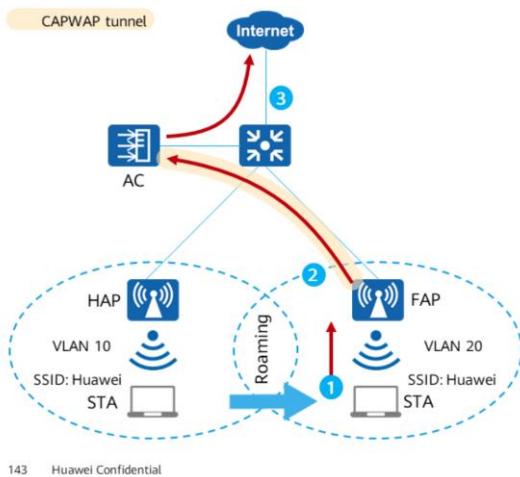
- The STA sends service packets to the FAP.
- After receiving the service packets, the FAP sends them to the AC through the CAPWAP tunnel.
- The AC forwards the service packets to the upper-layer network through the switch.

Intra-AC Layer 2 Roaming - Direct Forwarding



- Before roaming:
 - The STA sends service packets to the HAP.
 - After receiving the service packets, the HAP forwards them to the upper-layer network through the gateway (switch).
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP forwards them to the upper-layer network through the gateway (switch).

Intra-AC Layer 3 Roaming - Tunnel Forwarding

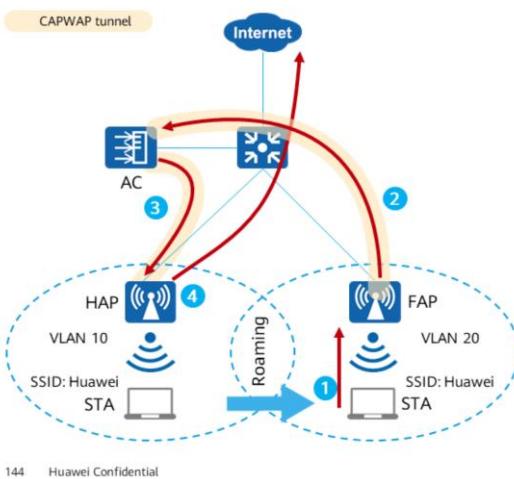


- Before roaming:
 - The STA sends service packets to the HAP.
 - After receiving the service packets, the HAP sends them to the HAC through the CAPWAP tunnel.
 - The HAC forwards the service packets to the upper-layer network through the switch.
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP sends them to the HAC through the CAPWAP tunnel.
 - The HAC forwards the service packets to the upper-layer network through the switch.

HUAWEI

- In Layer 3 roaming, the STA is not in the same subnet before and after roaming. To allow the STA to access the same network as before roaming, the STA's traffic needs to be forwarded to the original subnet through a tunnel.
- In tunnel forwarding mode, service packets exchanged between the HAP and AC are encapsulated through the CAPWAP tunnel, and the FAP and AC can be considered in the same subnet. Instead of forwarding the packets back to the HAP, the AC directly forwards the packets to the upper-layer network.

Intra-AC Layer 3 Roaming - Direct Forwarding (HAP as the Home Agent)

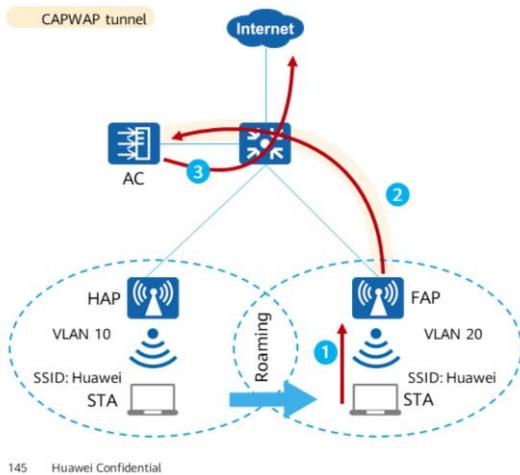


- Before roaming:
 - The STA sends service packets to the HAP.
 - After receiving the service packets, the HAP sends them to the HAC through the CAPWAP tunnel.
 - The HAC forwards the service packets to the upper-layer network through the switch.
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP sends them to the HAC through the CAPWAP tunnel.
 - After receiving the service packets, the HAC sends them to the HAP through the CAPWAP tunnel.
 - The HAP forwards the service packets to the upper-layer network through the switch.

HUAWEI

- In direct forwarding mode, the HAP functions as the home agent by default after a STA roams to another AP.
- The STA's traffic is forwarded by the home agent to ensure that the STA can still access the original network after roaming.

Intra-AC Layer 3 Roaming - Direct Forwarding (HAC as the Home Agent)

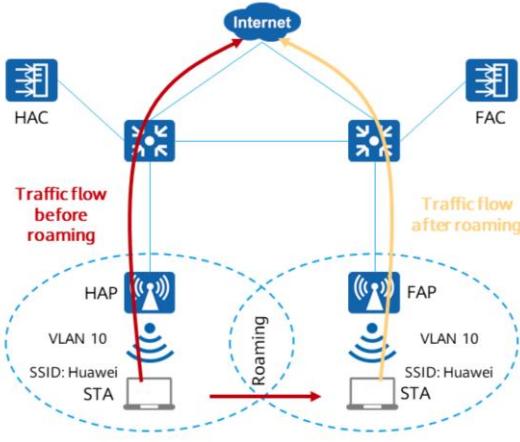


- Before roaming:
 - The STA sends service packets to the HAC.
 - After receiving the service packets, the HAC sends them to the upper-layer network through the switch.
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP sends them to the HAC through the CAPWAP tunnel.
 - The HAC forwards the service packets to the upper-layer network through the switch.

HUAWEI

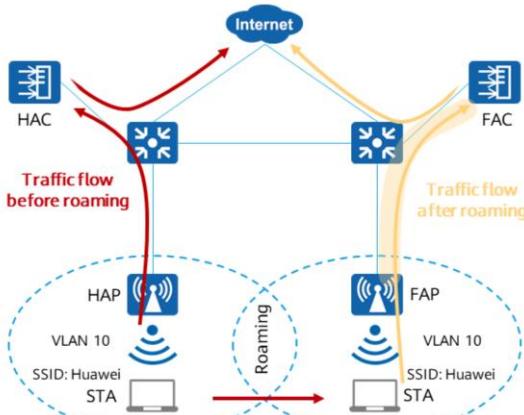
- If the AC and user gateway can communicate at Layer 2, you can configure the HAC as the home agent to reduce traffic load on the HAP. This also reduces the length of the tunnel between the FAP and the home agent, and improves the forwarding efficiency.

Inter-AC Layer 2 Roaming - Direct Forwarding



- Before roaming:
 - The STA sends service packets to the HAP.
 - After receiving the service packets, the HAP forwards them to the upper-layer network through the gateway (switch).
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP forwards them to the upper-layer network through the gateway (switch).

Inter-AC Layer 2 Roaming - Tunnel Forwarding



147 Huawei Confidential

- Before roaming:

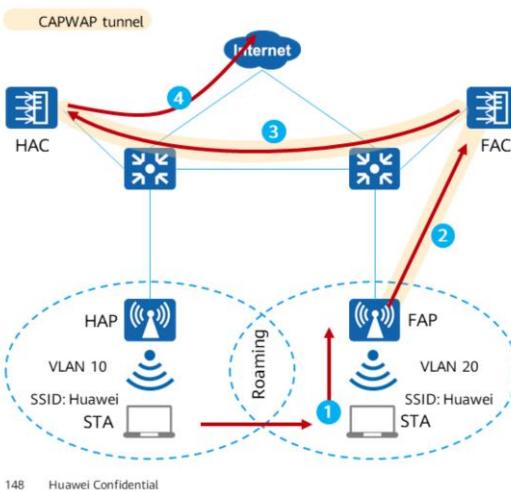
- The STA sends service packets to the HAP.
- After receiving the service packets, the HAP forwards them to the upper-layer network through the gateway (switch).

- After roaming:

- The STA sends service packets to the FAP.
- After receiving the service packets, the FAP sends them to the FAC through the CAPWAP tunnel.
- The FAC forwards the service packets to the upper-layer network through the switch.

 HUAWEI

Inter-AC Layer 3 Roaming - Tunnel Forwarding

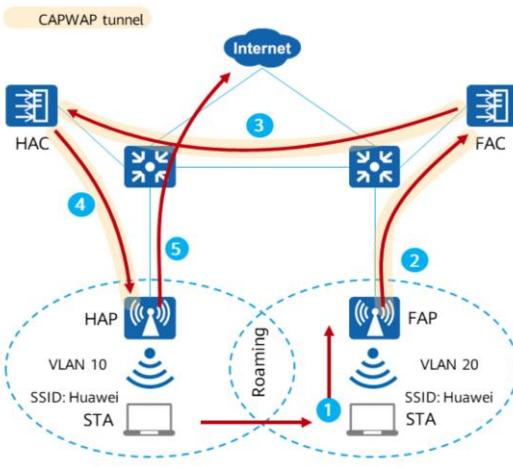


- Before roaming:
 - The STA sends service packets to the HAC.
 - After receiving the service packets, the HAC sends them to the FAC through the CAPWAP tunnel.
 - The FAC forwards the service packets to the upper-layer network through the switch.
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP sends them to the FAC through the CAPWAP tunnel.
 - The FAC forwards the service packets to the HAC through the CAPWAP tunnel between them.
 - The HAC forwards the service packets to the upper-layer network through the switch.

HUAWEI

- In Layer 3 roaming, the STA is not in the same subnet before and after roaming. To allow the STA to access the same network as before roaming, the STA's traffic needs to be forwarded to the original subnet through a tunnel.
- In tunnel forwarding mode, service packets between the HAP and HAC are encapsulated with the CAPWAP header. In this case, the HAP and HAC can be considered on the same subnet. Instead of forwarding the packets back to the HAP, the HAC directly forwards the packets to the upper-layer network.

Inter-AC Layer 3 Roaming - Direct Forwarding (HAP as the Home Agent)



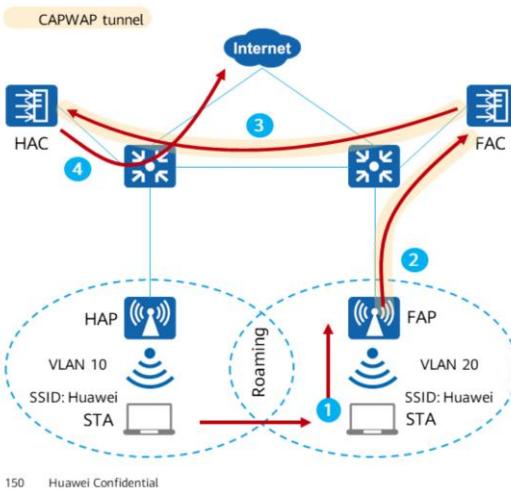
149 Huawei Confidential

- Before roaming:
 - The STA sends service packets to the HAP.
 - After receiving the service packets, the HAP sends them to the upper-layer network through the switch.
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP sends them to the FAC through the CAPWAP tunnel.
 - The FAC forwards the service packets to the HAC through the CAPWAP tunnel between them.
 - The HAC sends the service packets to the HAP through the CAPWAP tunnel.
 - The HAP forwards the service packets to the upper-layer network.

HUAWEI

- In direct forwarding mode, service packets between the HAP and HAC are not encapsulated with the CAPWAP header. Therefore, whether the HAP and HAC reside on the same subnet cannot be determined. In this case, packets are forwarded back to the HAP by default. If the HAP and HAC reside on the same subnet, you can configure a higher-performance HAC as the home agent. This reduces the load on the HAP and improves the forwarding efficiency.

Inter-AC Layer 3 Roaming - Direct Forwarding (HAC as the Home Agent)



- Before roaming:
 - The STA sends service packets to the HAP.
 - After receiving the service packets, the HAP sends them to the upper-layer network through the switch.
- After roaming:
 - The STA sends service packets to the FAP.
 - After receiving the service packets, the FAP sends them to the FAC through the CAPWAP tunnel.
 - The FAC forwards the service packets to the HAC through the CAPWAP tunnel between them.
 - The HAC forwards the service packets to the upper-layer network.

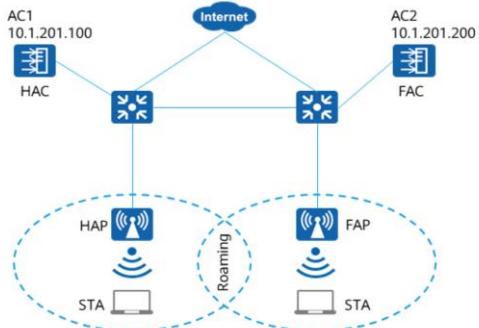
HUAWEI

- In direct forwarding mode, service packets between the HAP and HAC are not encapsulated with the CAPWAP header. Therefore, whether the HAP and HAC reside on the same subnet cannot be determined. In this case, packets are forwarded back to the HAP by default. If the HAP and HAC reside on the same subnet, you can configure a higher-performance HAC as the home agent. This reduces the load on the HAP and improves the forwarding efficiency.

Inter-AC Roaming Configuration

- Create a mobility group.
[AC-wlan-view] **mobility-group name** *group-name*
- Add a member AC to the mobility group. The IP address added in this step is the AC's source IP address.
[AC-mc-mg-group-name] **member { ip-address** *ipv4-address* **| ipv6-address** *ipv6-address* } [**description** *description*]

Example for Configuring Inter-AC Roaming



Configure WLAN roaming on AC1 and AC2.

```
[AC1-wlan-view] mobility-group name mobility  
[AC1-mc-mg-mobility] member ip-address 10.1.201.100  
[AC1-mc-mg-mobility] member ip-address 10.1.201.200  
[AC1-mc-mg-mobility] quit
```

```
[AC2-wlan-view] mobility-group name mobility  
[AC2-mc-mg-mobility] member ip-address 10.1.201.100  
[AC2-mc-mg-mobility] member ip-address 10.1.201.200  
[AC2-mc-mg-mobility] quit
```

- Deploy Layer 3 networking between the HAP and HAC and between the FAP and FAC.
- Add the HAC and FAC to a mobility group to ensure normal service traffic for STAs.

Checking the STA Roaming Track on the AC

- Check the STA roaming track on the AC after STA roaming is completed.

```
<AC> display station roam-track sta-mac 28b2-bd35-4af3
Access SSID:huawei-guest1
Rx/Tx: Rx-Rate/Tx-Rate Mbps
```

| L2/L3 | AC IP | AP name | Radio ID | BSSID | TIME | In Rx/Tx | RSSI | Out Rx/Tx | RSSI |
|-------|--------------|---------|----------|----------------|---------------------|----------|------|-----------|------|
| -- | 10.1.201.100 | ap1 | 1 | cccc-8110-2250 | 2020/06/18 14:09:06 | 130/130 | -44 | 130/130 | -44 |
| L3 | 10.1.201.200 | ap2 | 1 | cccc-8110-22b0 | 2020/06/18 14:12:24 | 130/6 | -42 | -/- | -/- |

Number of roam track: 1

Quiz

1. (Single Choice) Which of the following statements about CAPWAP tunnels are true?
 - A. CAPWAP tunnels include data tunnels and control tunnels.
 - B. A CAPWAP tunnel is established based on the TCP protocol to ensure the security of wireless data transmission.
 - C. During establishment of a CAPWAP tunnel, the AP downloads configurations from the AC after the Image Data phase is complete.
 - D. On a Layer 3 WLAN, if the DHCP Option 43 field is not configured, an AP can discover an AC using DNS.
2. (Multi-Answer Question) Which of the following phases are included in the STA going-online process?
 - A. Scanning
 - B. Access
 - C. Association
 - D. Authentication

- D
- ACD

Summary

- CAPWAP tunneling is a core technology in the AC + Fit AP networking architecture. It is necessary for those who aspire to be WLAN engineers to have a good command of the CAPWAP protocol.
- Mastering the AP join process and STA going-online process help you better understand the implementation of a WLAN. Once a fault occurs, you can quickly troubleshoot it.
- The roaming technology is indispensable for enterprise WLAN deployment. It provides mobility in workplace. Acquainting yourself with the roaming technology helps you better plan, design, and deploy WLANs.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



Wi-Fi 6 Technologies and Products



Foreword

- Nowadays, fully wireless office enables enterprises with higher communication and collaboration efficiency. Wi-Fi 6 networks bring ultra-high-speed performance of 4K conferencing and cloud-device collaboration in the case of high access concurrency.
- In the future, fully wireless production will improve the operational efficiency in scenarios such as warehousing and manufacturing production lines. Wi-Fi 6 networks enable stable experience for a broad range of applications, such as automated navigation vehicles (AGVs), industrial visual quality inspection, and wireless vehicle software loading.
- Huawei's full lineup of AirEngine products are next-generation WLAN products that comply with the Wi-Fi 6 (802.11ax) standard and are powered by Huawei's key 5G technologies. Huawei AirEngine can meet indoor and outdoor WLAN deployment requirements of customers across industries. Huawei AirEngine products adopt a brand-new industrial design and an innovative flip-type IoT card slot design, meeting the requirements of ever-changing terminals and applications in the digital space.

Objectives

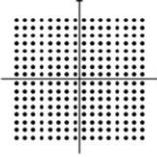
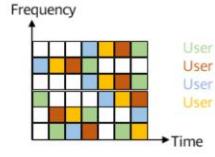
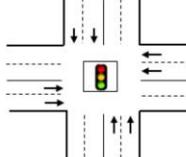
On completion of this course, you will be able to:

- Explain the WLAN development process.
- Classify Huawei WLAN products.
- Describe features of Huawei WLAN products.
- Identify power supply modes of APs.

Contents

- 1. Wi-Fi 6 Technologies**
2. Huawei WLAN Product Family
3. Features of Huawei WLAN Products
4. AP Power Supply

Wi-Fi 6 vs Wi-Fi 5

| Large bandwidth | High concurrency | Low latency | Low power consumption |
|--|---|---|---|
|  <p>1024 QAM 8x8 MU-MIMO</p> <ul style="list-style-type: none"> Rate up to 9.6 Gbps Bandwidth up by 4 times |  <p>UL/DL OFDMA UL/DL MU-MIMO</p> <ul style="list-style-type: none"> 1024 STAs connected to one AP The number of concurrent users up by 4 times. |  <p>OFDMA Spatial Reuse</p> <ul style="list-style-type: none"> The service latency down to 20 ms Average latency down by 30% |  <p>TWT 20 MHz Only</p> <ul style="list-style-type: none"> Target Wakeup Time (TWT) STA power consumption down by 30% |

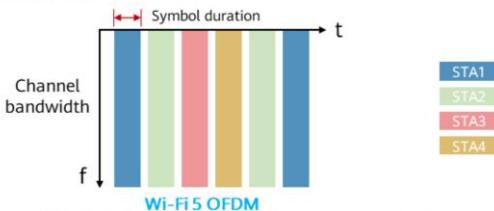
162 Huawei Confidential

 HUAWEI

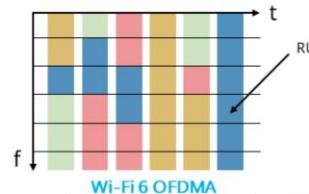
- The 4 times bandwidth increase is based on theoretical rate. Currently, the theoretical rate of the Wi-Fi 5 (wave2) is 2.5 Gbps. The theoretical rate of Wi-Fi 6 is 9.6 Gbps.
- The number of concurrent users is increased by 4 times. In real tests, at 2 Mbps per user, Wi-Fi 5 can support 100 concurrent users, while Wi-Fi 6 can support 400.
- The service latency is 20 ms in the Wi-Fi 6 standard (the average latency of Wi-Fi 5 is about 30 ms). With Huawei smart radio application acceleration technology, the service latency can be further reduced to 10 ms.
- TWT: Wi-Fi 5 does not support this feature.

Wi-Fi 6 Technology: OFDMA

- Orthogonal frequency division multiple access (OFDMA) is used to distinguish users by frequency. Compared with the traditional FDMA, OFDMA significantly improves the spectrum utilization. OFDMA enables simultaneous data transmission of multiple users, which increases air interface efficiency, greatly reduces the application latency, and lowers the conflict backoff probability.
- Resource unit (RU):
 - 802.11ax divides existing 20 MHz, 40 MHz, 80 MHz, and 160 MHz bandwidths into several RUs.
 - 802.11ax defines seven types of RUs: 26-tone, 52-tone, 106-tone, 242-tone, 484-tone, 996-tone, and 2x996-tone RUs. A user can transmit data on multiple RUs at a time.



Four users (STAs in the figure) occupy channel resources separately in different timeslots. In each timeslot, one user occupies all subcarriers for sending data packets.



Data of the four users is carried on each RU. Therefore, 802.11ax allows multiple users to transmit data at the same time point when the total time-frequency resources remain unchanged.



- OFDM:

- Users are differentiated by time. In each time segment, one user occupies all subcarriers.

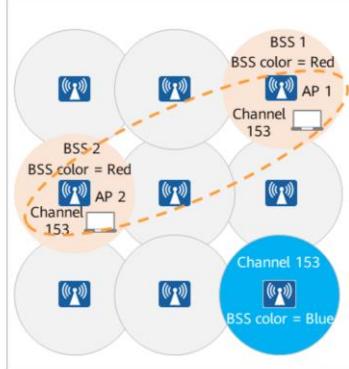
- OFDMA:

- An AP determines how to allocate channels based on communication requirements of multiple users, and always allocates all available RUs in the downlink direction. The AP may allocate the entire channel to one user at a time or partition the channel to serve multiple users concurrently.
- In OFDMA mode, channel resources can be allocated more delicately, allowing finer-grained QoS.

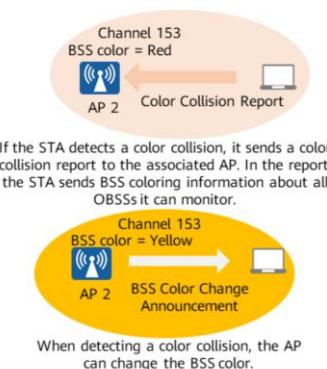
Wi-Fi 6 Technology: BSS Coloring

- BSS coloring is a method for improving the spatial reuse (SR) rate and reducing the contention overhead at the MAC layer caused by overlapping basic service sets (OBSSs). BSS coloring aims to improve the SR rate while reducing the PHY transmission rate between nodes (that is, reducing the MCS value), without being affected by inter-BSS interference.

- The AP or STA detects OBSSs with the same color.



- Color collisions and changes are reported.

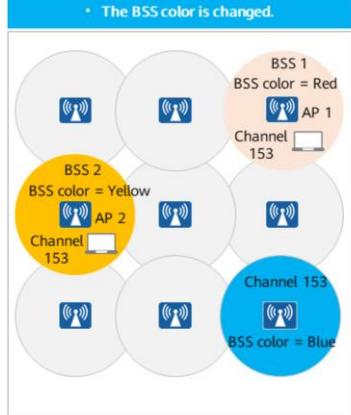


If the STA detects a color collision, it sends a color collision report to the associated AP. In the report, the STA sends BSS coloring information about all OBSSs it can monitor.

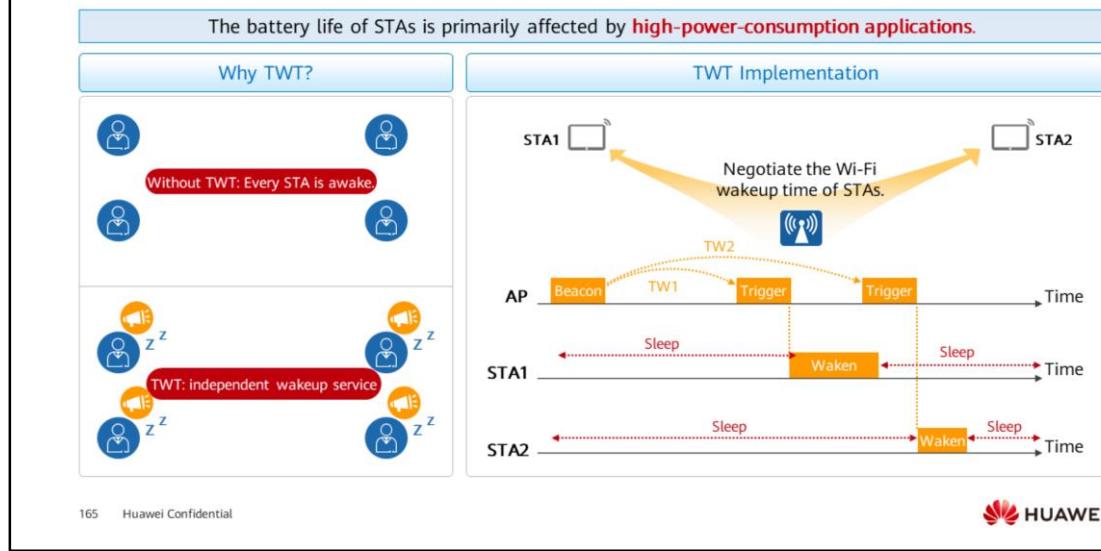


When detecting a color collision, the AP can change the BSS color.

- The BSS color is changed.



Wi-Fi 6 Technology: TWT



- Each generation of new Wi-Fi standards can extend the battery life of STAs by supporting faster and longer transmission to lower their power consumption. Wi-Fi 6 introduces target wakeup time (TWT), which allows an AP to inform a STA when to sleep and provide a scheduling table defining when the STA is awake. Even though the STA sleeps for a short period of time each time, multiple sleeps significantly prolong the battery life of the STA.
- TWT wakes up the Wi-Fi function of STAs on demand, reducing the power consumption of the STAs by 30%.
- TWT was first proposed in the 802.11ah standard. This mechanism is designed to save energy for IoT devices, especially devices with low traffic volume such as smart meters. This allows IoT devices to stay in the sleep state as long as possible, reducing power consumption. After a TWT agreement is established, a STA wakes up after a longer period of time, without the need of receiving a Beacon frame. The 802.11ax standard improves on TWT by defining rules for STA behavior and implementing channel access control on the premise of meeting energy saving requirements. TWT is classified into unicast TWT and broadcast TWT.

Contents

1. Wi-Fi 6 Technologies
2. **Huawei WLAN Product Family**
3. Features of Huawei WLAN Products
4. AP Power Supply

WLAN Product Portfolio - Wi-Fi 5

| Wi-Fi 5 (802.11ac) indoor APs | | | | | | | | | |
|---|---|--|--|--|---|---|---|--|--|
| AP7052DN | AP7152DN | AP6052DN | AP6050DN & AP6150DN | AP6750-10I | AP4051DN | AP4050DN-HD | AP4050DE-M | AP4050DN-E & AP4050DN | |
|  <ul style="list-style-type: none"> Device rate: 2.53 Gbps/3.46 Gbps (dual-5G) Spatial stream: 4x4 Built-in antennas |  <ul style="list-style-type: none"> Device rate: 2.53 Gbps/3.46 Gbps (dual-5G) Spatial stream: 4x4 External antennas |  <ul style="list-style-type: none"> Device rate: 2.53 Gbps/3.46 Gbps (dual-5G) Spatial stream: 4x4 Built-in antennas |  <ul style="list-style-type: none"> Device rate: 2.53 Gbps Spatial stream: 4x4 Built-in or external antennas |  <ul style="list-style-type: none"> Device rate: 2.53 Gbps Spatial stream: 2x2-4 Three radios Built-in smart antennas |  <ul style="list-style-type: none"> Device rate: 3 Gbps Spatial stream: 2x2 Built-in smart antennas |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 Built-in or external antennas |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 Built-in smart antennas |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 Built-in antennas | |
| Wi-Fi 5 (802.11ac) outdoor APs | | | | | | | | | |
| AP8082DN | APB182DN | APB0500N | APB1500N | APB0501N-HD | AD9431DN-24K | R2500D | R2510D & R2510-E | AP5510-W-GP | AP2051DN & AP2051DN-E |
|  <ul style="list-style-type: none"> Device rate: 2.53 Gbps Spatial stream: 4x4 Built-in directional antennas Port: 1 x SGE electrical + 1 x GE electrical + 1 x GE SFP |  <ul style="list-style-type: none"> Device rate: 2.53 Gbps/3.46 Gbps (dual-5G) Spatial stream: 4x4 External antennas Port: 1 x SGE electrical + 1 x GE electrical + 1 x GE SFP |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 Built-in directional antennas Port: 1 x SGE electrical + 1 x GE electrical + 1 x GE SFP |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 1.73 Gbps (dual-5G) Spatial stream: 2x2 External antennas Port: 1 x GE electrical + 1 x GE SFP |  <ul style="list-style-type: none"> Device rate: 2.134 Gbps Spatial stream: 2x2+2 Built-in multi-angle directional antennas External antennas Three radios Port: 1 x GE electrical + 1 x GE SFP |  <ul style="list-style-type: none"> Forwarding performance: 24 Gbps Uplink port: 4 x 10GE Downlink port: 24 x GE Managing up to 48 RUs 4000 users + 1000 concurrent users |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 Built-in smart antennas Uplink port: 4 x GE Downlink port: 4 x GE + 2 x RJ45 passthrough |  <ul style="list-style-type: none"> Device rate: 1.267 Gbps Spatial stream: 2x2 Built-in smart antennas Uplink port: 4 x GE Downlink port: 4 x GE + 2 x RJ45 passthrough |

167 Huawei Confidential



WLAN Product Portfolio - Wi-Fi 6

| Wi-Fi 6 (802.11ax) indoor APs | Wi-Fi 6 (802.11ax) agile distributed APs | |
|---|---|--|
|  AirEngine 8760-X1-PRO <ul style="list-style-type: none"> Device rate: 10.75 Gbps Spatial stream: 4x4x4 or 4x4x4 Built-in smart antennas BLE 5.0, two built-in IoT slots Port: 1 x 10GE electrical + 1 x GE electrical + 2 x GE optical + 1 x 10/100 optical  AirEngine 6760-X1 <ul style="list-style-type: none"> Device rate: 10.75 Gbps Spatial stream: 4x8/4x4 Built-in smart antennas BLE 5.0, one built-in IoT slot Port: 1 x 10GE electrical + 1 x GE electrical  AirEngine 6760-XTE <ul style="list-style-type: none"> Device rate: 5.95 Gbps Spatial stream: 4x4 or 2x2+4 External antennas BLE 5.0, two built-in IoT slots Port: 1 x 10GE electrical + 1 x GE electrical + 1 x SFP optical  AirEngine 5760-51 <ul style="list-style-type: none"> Device rate: 5.95 Gbps Spatial stream: 4x4 or 2x2+4 External antennas BLE 5.0, two built-in IoT slots Port: 1 x 10GE electrical + 1 x GE electrical + 1 x SFP optical  AirEngine 5760-10 <ul style="list-style-type: none"> Device rate: 1.77 Gbps Spatial stream: 2x2 External antennas BLE 5.0 Port: 1 x GE electrical  AP7060DN <ul style="list-style-type: none"> Device rate: 5.95 Gbps Spatial stream: 4x8 Built-in smart antennas BLE 5.0 Port: 1 x GE electrical + 1 x GE optical |  AirEngine 9700D-M <ul style="list-style-type: none"> Forwarding performance: 216 Gbps Uplink port: 4 x 10GE Downlink port: 24 x GE Managing up to 48 RUs Port: 1 x 2.5GE electrical + 1 x GE electrical  AirEngine 5760-Z2WD <ul style="list-style-type: none"> Device rate: 5.37 Gbps Spatial stream: 2x4 Built-in smart antennas BLE 5.0 Uplink port: 1 x GE electrical + 1 x 2.5GE optical Downlink port: 4 x GE electrical + 2 x RJ45 passthrough | |
| Wi-Fi 6 (802.11ax) outdoor APs | Wi-Fi 6 (802.11ax) wall plate APs | ACs |
|  AirEngine 8760R-X1 <ul style="list-style-type: none"> Device rate: 10.75 Gbps Spatial stream: 8x8/4x4 Built-in outdoor smart antennas BLE 5.0, PoE OUT Port: 1 x 10GE electrical + 1 x GE electrical + 1 x 10GE optical  AirEngine 8760R-X1E <ul style="list-style-type: none"> Device rate: 10.75 Gbps Spatial stream: 8x8/4x4 Built-in outdoor smart antennas BLE 5.0, PoE OUT Port: 1 x 10GE electrical + 1 x GE electrical + 1 x 10GE optical  AirEngine 6760R-51 <ul style="list-style-type: none"> Device rate: 5.95 Gbps Spatial stream: 4x4 External antennas BLE 5.0, PoE OUT Port: 1 x 10GE electrical + 1 x GE electrical + 1 x 10GE optical  AirEngine 6760R-51E <ul style="list-style-type: none"> Device rate: 5.95 Gbps Spatial stream: 4x4 External antennas BLE 5.0 Port: 1 x 10GE electrical + 1 x GE electrical + 1 x 10GE optical |  AirEngine 5760-22W <ul style="list-style-type: none"> Device rate: 5.37 Gbps Spatial stream: 2x4 Built-in smart antennas BLE 5.0 Uplink port: 1 x 2.5GE + 1 x 10GE optical Downlink port: 4 x GE + 2 x RJ45 passthrough |  AC6800V <ul style="list-style-type: none"> Maximum throughput: 60 Gbps Managing up to 10K APs Up to 100K access users  AC6805 <ul style="list-style-type: none"> Maximum throughput: 40 Gbps Managing up to 6K APs Up to 64K access users  AC6508 <ul style="list-style-type: none"> Maximum throughput: 6 Gbps Managing up to 256 APs Up to 4K access users |

AC6800V



| Specification Item | Details |
|----------------------------------|---|
| Dimensions (H x W x D) | 86 mm x 708 mm x 447 mm |
| Port | 6 x GE + 6 x 10GE Note: Different port requirements can be met through GE, 10GE, or 40GE NICs. |
| Forwarding performance | 60 Gbps |
| Maximum number of manageable APs | 10K |
| Maximum number of access users | 100K |
| Networking between APs and ACs | L2/L3 network topology |
| AC backup mode | 1+1 hot backup, N+1 backup |
| Wireless protocol | 802.11a/b/g/n/ac/ac Wave 2/ax |
| Application scenario | Large enterprises |

- AC6800V is a high-performance wireless access controller (AC) designed for large enterprise campuses, enterprise branches, and campus networks. Working with Huawei-developed server platform, AC6800V can manage a maximum of 10K APs and provide up to 60 Gbps forwarding performance.
- Large capacity and high performance: AC6800V provides 6 GE ports and 6 10GE ports, as well as up to 60 Gbps forwarding performance. AC6800V can manage up to 10K APs and 100K access users.
- Flexible data forwarding modes: direct forwarding and tunnel forwarding; flexible user rights control: user- and role-based access control
- Abundant O&M methods: various network O&M methods, including eSight, web platform, and Command Line Interface (CLI)

Hardware Structure of AC6800V

Front view of AC6800V



Rear view of AC6800V



Components of AC6800V (Front View)

| | | | |
|---|------------------------------------|---|-------------------------------|
| 1 | USB 2.0 port | 2 | Built-in DVD drive (optional) |
| 3 | USB 3.0 port | 4 | VGA port |
| 5 | Label card (including an SN label) | 6 | Hard disk |

Components of AC6800V (Rear View)

| | | | |
|----|--------------------|----|--------------------|
| 1 | 10GE optical port | 2 | 10GE optical port |
| 3 | GE electrical port | 4 | 10GE optical port |
| 5 | VGA port | 6 | GE electrical port |
| 7 | Management port | 8 | Console port |
| 9 | USB 3.0 port | 10 | Flexible NIC |
| 11 | Power module | 12 | Power module port |
| 13 | I/O module | | |

AC6805

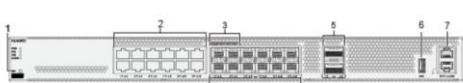


| Specification Item | Details |
|----------------------------------|---|
| Dimensions (H x W x D) | 43.6 mm x 420 mm x 442 mm |
| Port | 12 x GE + 12 x 10GE + 2 x 40GE (one 40GE port and four 10GE ports cannot be available at the same time) |
| Forwarding performance | 40 Gbps |
| Maximum number of manageable APs | 6K |
| Maximum number of access users | 64K |
| Networking between APs and ACs | L2/L3 network topology |
| AC backup mode | 1+1 hot backup, N+1 backup |
| Wireless protocol | 802.11a/b/g/n/ac/ac Wave 2/ax |
| Application scenario | Large enterprises |

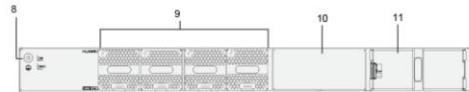
- AC6805 is a high-end wireless AC for large enterprise campuses, enterprise branches, and school campuses. It can manage up to 6K access points (APs) and provide 40 Gbps forwarding performance. It features high scalability and offers users considerable flexibility in configuring the number of managed APs. Working with Huawei's full series 802.11ax, 802.11ac, and 802.11n APs, AC6805 delivers an adaptable solution for large and midsize campus networks, enterprise office networks, wireless metropolitan area networks (MANs), and hotspot coverage networks.

Hardware Structure of AC6805

Front view of AC6805



Rear view of AC6805



Components of AC6805 (Front View)

| | | | |
|---|--------------------------------------|---|-----------------------|
| 1 | Reset button | 2 | GE electrical port |
| 3 | Combo port | 4 | 10GE SFP+ port |
| 5 | 40GE QSFP+ port | 6 | Standard USB 3.0 port |
| 7 | ETH management port and console port | | |

Components of AC6805 (Rear View)

| | | | |
|----|-------------------|----|--|
| 8 | Ground point | 9 | Pluggable fan module |
| 10 | Power module slot | 11 | Filler panel for the backup power module |

- Reset button:
 - Press the reset button (for no more than 3 seconds) to reset the AC manually. Resetting the AC will cause service interruption. Exercise caution when you press the reset button.
 - Press and hold down the reset button (for more than 5 seconds) to restore factory defaults of the AC.
- Combo port:
 - The combo port can be used as one 40GE QSFP+ Ethernet port or four 10GE SFP+ Ethernet ports. By default, QSFP+ port 1 works, and SFP+ ports 1 to 4 are unavailable. When any SFP+ port is enabled, QSFP+ port 1 becomes unavailable.

AirEngine 9700-M



| Specification Item | Details |
|--------------------------------|--|
| Dimensions (H x W x D) | 43.6 mm x 420 mm x 442 mm |
| Port | 16 x GE + 12 x 10 GE + 2 x 40 GE (one 40GE port and four 10GE ports cannot be available at the same time) |
| Forwarding performance | 20 Gbps |
| Number of manageable APs | 2048 |
| Maximum number of access users | 32K |
| Networking between APs and ACs | L2/L3 network topology |
| AC backup mode | 1+1 hot backup, N+1 backup |
| Wireless protocol | 802.11a/b/g/n/ac/ac Wave 2/ax |
| Application scenario | Midsize and large enterprises |

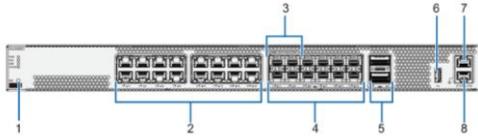
173 Huawei Confidential

 HUAWEI

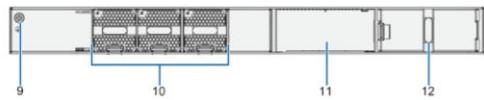
- AirEngine 9700-M is a high-specification wireless access controller (AC) for midsize and large enterprise campuses, enterprise branches, and school campuses. It can manage up to 2000 access points (APs) and provide up to 20 Gbps forwarding performance. Working with Huawei's full series 802.11ac and 802.11ax APs, AirEngine 9700-M delivers an adaptable solution for midsize and large campus networks, enterprise office networks, wireless metropolitan area networks (MANs), and hotspot coverage networks.

Hardware Structure of AirEngine 9700-M

Front view of AirEngine 9700-M



Rear view of AirEngine 9700-M



Components of AirEngine 9700-M (Front View)

| | | | |
|---|-----------------|---|-----------------------|
| 1 | Reset button | 2 | GE electrical port |
| 3 | Combo port | 4 | 10GE SFP+ port |
| 5 | 40GE QSFP+ port | 6 | Standard USB 2.0 port |
| 7 | Console port | 8 | ETH management port |

Components of AirEngine 9700-M (Rear View)

| | | | |
|----|-------------------|----|--|
| 9 | Ground point | 10 | Pluggable fan module |
| 11 | Power module slot | 12 | Filler panel for the backup power module |

- Reset button:
 - Press the reset button (for no more than 3 seconds) to reset the AC manually. Resetting the AC will cause service interruption. Exercise caution when you press the reset button.
 - Press and hold down the reset button (for more than 5 seconds) to restore factory defaults of the AC.
- Combo port:
 - The combo port can be used as one 40GE QSFP+ Ethernet port or four 10GE SFP+ Ethernet ports. By default, QSFP+ port 1 works, and SFP+ ports 1 to 4 are unavailable. When any SFP+ port is enabled, QSFP+ port 1 becomes unavailable.

AC6508



| Specification Item | Details |
|----------------------------------|-------------------------------|
| Dimensions (H x W x D) | 43.6 mm x 210 mm x 250 mm |
| Port | 10 x GE + 2 x 10GE SFP+ |
| Forwarding performance | 6 Gbps |
| Maximum number of manageable APs | 256 |
| Maximum number of access users | 4K |
| Networking between APs and ACs | L2/L3 network topology |
| AC backup mode | 1+1 hot backup, N+1 backup |
| Wireless protocol | 802.11a/b/g/n/ac/ac Wave 2/ax |
| Application scenario | Small enterprises |

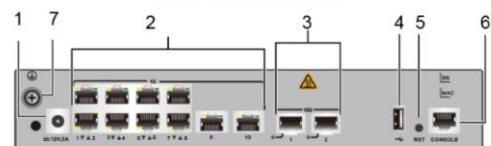
- AC6508 is a small-capacity box wireless access controller (AC) for small and midsize enterprises. It can manage up to 256 APs. In addition, the device integrates the GE Ethernet switch function, achieving integrated access for wired and wireless users. The number of APs that can be managed by the AC can be flexibly configured, providing good scalability. Working with Huawei's full series 802.11ax, 802.11ac, and 802.11n APs, AC6508 delivers an adaptable solution for small and midsize campus networks, enterprise office networks, wireless metropolitan area networks (MANs), and hotspot coverage networks.

Hardware Structure of AC6508

Front view of AC6508



Rear view of AC6508



| Components of AC6508 (Rear View) | | | |
|----------------------------------|-------------------|---|--------------------|
| 1 | DC input terminal | 2 | GE electrical port |
| 3 | 10GE optical port | 4 | USB 2.0 port |
| 5 | Reset button | 6 | Console port |
| 7 | Ground point | | |

- **Reset button:**

- Press the reset button (for no more than 3 seconds) to reset the AC manually.
Resetting the AC will cause service interruption. Exercise caution when you press the reset button.
- Press and hold down the reset button (for more than 5 seconds) to restore factory defaults of the AC.

AirEngine 8760-X1-PRO



Features of the indoor AP — AirEngine 8760-X1-PRO

- Working simultaneously on the 2.4 GHz and 5 GHz bands, providing a rate of up to 1.15 Gbps at 2.4 GHz, 9.6 Gbps at 5 GHz, and 10.75 Gbps for the device
- Dual-radio mode: 2.4 GHz (4x4:4) + 5 GHz (12x12:8)
- Triple-radio mode: 2.4 GHz (4x4:4) + 5 GHz (8x8:8) + 5 GHz (4x4:4)
- Dual-radio + independent scanning mode: 2.4 GHz (4x4) + 5 GHz (8x8) + independent scanning radio
- 2 x 10GE electrical ports + 1 x 10GE optical port
- Built-in smart antennas that automatically adjust the coverage direction and signal strength based on the intelligent switchover algorithm to adapt to application environment changes, and provide accurate and stable coverage as STAs move
- Built-in IoT module, supporting IoT expansion such as BLE 5.0, ZigBee, RFID, and Thread
- Built-in independent dual-band scanning module, achieving real-time detection for interference and rogue devices as well as timely network optimization
- Built-in Bluetooth module: Bluetooth serial interface-based O&M by collaborating with CloudCampus APP; accurately locating Bluetooth terminals and tags by collaborating with a location server
- Working modes: Fit, Fat, and cloud management

177 Huawei Confidential

 HUAWEI

- Huawei AirEngine 8760-X1-PRO is a next-generation flagship indoor access point (AP) that complies with the Wi-Fi 6 standard. The AP uses built-in smart antennas to move Wi-Fi signals with users, significantly enhancing users' wireless network experience. The AP provides uplink optical and electrical ports, allowing customers to select different deployment modes based on scenarios. These strengths make AirEngine 8760-X1-PRO ideal for scenarios such as enterprise office, government, higher education, and primary/secondary education.

Hardware Structure of AirEngine 8760-X1-PRO



| AirEngine 8760-X1-PRO | | | |
|-----------------------|---------------|---|--------------|
| 1 | Security slot | 2 | 10GE1/PoE_IN |
| 3 | 10GE0/PoE_IN | 4 | USB |
| 5 | SFP+ | 6 | Default |
| 7 | 48 V DC | 8 | IoT slot |
| 9 | Radio port | | |

- Security slot: connects to a security lock.
- 10GE1/PoE_IN: 100M/1000M/2.5G/5G/10G port that connects to the wired Ethernet and supports PoE input.
- 10GE0/PoE_IN: 100M/1000M/2.5G/5G/10G port that connects to the wired Ethernet and supports PoE input.
- USB: USB 2.0 port that connects to a USB flash drive or extends an IoT application.
- SFP+: Ethernet port that can work at the rate of 1 Gbps or 10 Gbps through auto-sensing and works with a matching optical module.
- Default button: Reset button used to restore factory defaults and restart the device if you press and hold down the button for more than 3 seconds.
- 48 V DC: input port for 48 V DC power supply.
- IoT slot: accommodates an IoT card to provide IoT functions.
- Radio port: a port of the built-in IoT antenna on the device.

AirEngine 6760-X1



179 Huawei Confidential

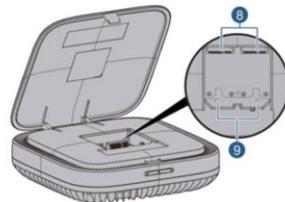
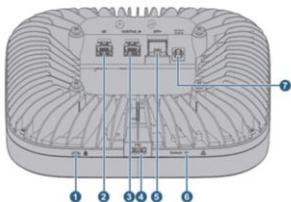
Features of the indoor AP — AirEngine 6760-X1

- Working simultaneously on the 2.4 GHz and 5 GHz bands, providing a rate of up to 1.15 Gbps at 2.4 GHz, 9.6 Gbps at 5 GHz, and 10.75 Gbps for the device
 - Dual-radio mode: 2.4 GHz (4x4:4) + 5 GHz (8x8:8)
 - Triple-radio mode: 2.4 GHz (4x4:4) + 5 GHz (4x4:4) + 5 GHz (4x4:4)
 - Dual-radio + independent scanning mode: 2.4 GHz (4x4) + 5 GHz (6x6) + independent scanning radio
- 1 x 10GE electrical port + 1 x GE electrical port + 1 x 10GE optical port
- Built-in smart antennas that automatically adjust the coverage direction and signal strength based on the intelligent switchover algorithm to adapt to application environment changes, and provide accurate and stable coverage as STAs move
- Built-in IoT module, supporting IoT expansion such as BLE 5.0, ZigBee, RFID, and Thread
- Built-in independent scanning radio, achieving real-time detection for interference and rogue devices as well as timely network optimization
- Built-in Bluetooth module: Bluetooth serial interface-based O&M by collaborating with CloudCampus APP; accurately locating Bluetooth terminals and tags by collaborating with a location server
- Working modes: Fit, Fat, and cloud management



- Huawei AirEngine 6760-X1 is an indoor AP in compliance with Wi-Fi 6 (802.11ax). AirEngine 6760-X1 uses built-in smart antennas to move Wi-Fi signals with users, significantly enhancing users' wireless network experience. AirEngine 6760-X1 provides uplink optical and electrical ports, allowing customers to select different deployment modes and saving customers' investment. These strengths make AirEngine 6760-X1 ideal for scenarios such as enterprise office and education.

Hardware Structure of AirEngine 6760-X1



| AirEngine 8760-X1-PRO | | | |
|-----------------------|---------------|---|----------|
| 1 | Security slot | 2 | GE |
| 3 | 10GE/PoE_IN | 4 | USB |
| 5 | SFP+ | 6 | Default |
| 7 | 48 V DC | 8 | IoT slot |
| 9 | Radio port | | |

180 Huawei Confidential

 HUAWEI

- Security slot: connects to a security lock.
- GE: 10M/100M/1000M port that connects to the wired Ethernet.
- 10GE/PoE_IN: 100M/1000M/2.5G/5G/10G port that connects to the wired Ethernet and supports PoE input.
- USB: USB 2.0 port that connects to a USB flash drive or extends an IoT application.
- SFP+: Ethernet port that can work at the rate of 1 Gbps or 10 Gbps through auto-sensing and works with a matching optical module.
- Default button: Reset button used to restore factory defaults and restart the device if you press and hold down the button for more than 3 seconds.
- 48 V DC: input port for 48 V DC power supply.
- IoT slot: accommodates an IoT card to provide IoT functions.
- Radio port: a port of the built-in IoT antenna on the device.

AirEngine 5760-51



181 Huawei Confidential

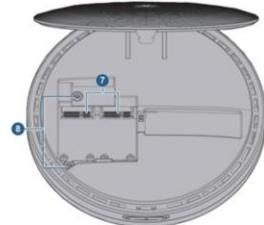
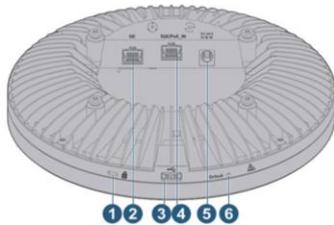
Features of the indoor AP — AirEngine 5760-51

- Working simultaneously on the 2.4 GHz and 5 GHz bands, providing a rate of up to 1.15 Gbps at 2.4 GHz, 4.8 Gbps at 5 GHz, and 5.95 Gbps for the device
 - Dual-radio mode: 2.4 GHz (4x4:4) + 5 GHz (4x4:4)
 - Triple-radio mode: 2.4 GHz (2x2:2) + 5 GHz (2x2:2) + 5 GHz (4x4:4)
 - Dual-radio + independent scanning mode: 2.4 GHz (2x2) + 5 GHz (4x4) + independent radio scanning
- 1 x 5GE electrical port + 1 x GE electrical port
- Built-in smart antennas that automatically adjust the coverage direction and signal strength based on the intelligent switchover algorithm to adapt to application environment changes, and provide accurate and stable coverage as STAs move
- Built-in IoT module, supporting IoT expansion such as BLE 5.0, ZigBee, RFID, and Thread
- Built-in Bluetooth module: Bluetooth serial interface-based O&M by collaborating with CloudCampus APP; accurately locating Bluetooth terminals and tags by collaborating with a location server
- Working modes: Fit, Fat, and cloud management

 HUAWEI

- Huawei AirEngine 5760-51 is a wireless access point (AP) in compliance with the Wi-Fi 6 standard. The AP uses built-in smart antennas to move Wi-Fi signals with users, significantly enhancing users' wireless network experience. These strengths make AirEngine 5760-51 ideal for small and midsize enterprises, airports, railway stations, stadiums, cafes, and recreation centers.

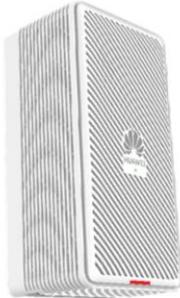
Hardware Structure of AirEngine 5760-51



| AirEngine 5760-51 | | | |
|-------------------|---------------|---|------------|
| 1 | Security slot | 2 | GE |
| 3 | USB | 4 | 5GE/PoE_IN |
| 5 | 48 V DC | 6 | Default |
| 7 | IoT slot | 8 | Radio port |

- Security slot: connects to a security lock.
- GE: 10M/100M/1000M port that connects to the wired Ethernet.
- USB: USB 2.0 port that connects to a USB flash drive or extends an IoT application.
- 5GE/PoE_IN: 100M/1000M/2.5G/5G port that connects to the wired Ethernet and supports PoE input.
- 48 V DC: input port for 48 V DC power supply.
- Default button: Reset button used to restore factory defaults and restart the device if you press and hold down the button for more than 3 seconds.
- IoT slot: accommodates an IoT card to provide IoT functions.
- Radio port: a port of the built-in IoT antenna on the device.

AirEngine 5760-22W

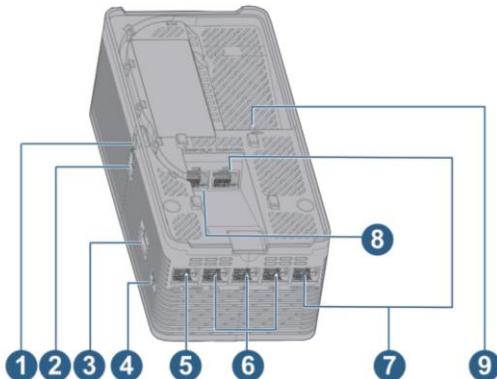


Features of the wall plate AP — AirEngine 5760-22W

- Working simultaneously on the 2.4 GHz and 5 GHz bands, providing a rate of up to 574 Mbps at 2.4 GHz, 4.8 Gbps at 5 GHz, and 5.37 Gbps for the device
 - Dual-radio mode: 2.4 GHz (2x2:2) + 5 GHz (4x4:4)
- 1 x 2.5GE electrical port + 1 x 10GE optical port + 4 x GE electrical ports + 2 x RJ45 passthrough ports
- Mounted on a junction box or wall, facilitating deployment
- Built-in smart antennas that automatically adjust the coverage direction and signal strength based on the intelligent switcheroo algorithm to adapt to application environment changes, and provide accurate and stable coverage as STAs move
- USB port for storage and external power supply
- PoE OUT, supplying power to terminals such as IP phones and external IoT modules
- Working modes: Fit, Fat, and cloud management

- AirEngine 5760-22W is a Huawei's Wi-Fi 6 wall plate access point (AP). With mounting brackets, the AP can be easily mounted on junction boxes (86/118/120 mm) or on a wall. The AP uses built-in smart antennas to move Wi-Fi signals with users, significantly enhancing users' wireless network experience. The AP provides uplink optical and electrical ports, allowing customers to select different deployment modes and saving customers' investment. These strengths make AirEngine 5760-22W ideal for scenarios with high-density rooms such as hotel guest rooms, dormitory rooms, and hospital wards.

Hardware Structure of AirEngine 5760-22W



| AirEngine 5760-22W | | | |
|--------------------|--------------------|---|--------------|
| 1 | Captive screw hole | 2 | 48 V DC |
| 3 | USB | 4 | Default |
| 5 | GE3/PoE_OUT | 6 | GE0 to GE2 |
| 7 | PASS-THRU | 8 | 2.5GE/PoE_IN |
| 9 | SFP+ | | |

184 Huawei Confidential

 HUAWEI

- AirEngine 5760-22W can be used independently as a wall plate AP or as an RU working with the central AP in an agile distributed Wi-Fi networking architecture.
- Captive screw hole: used to install a captive screw.
- 48 V DC: input port for 48 V DC power supply.
- USB port: USB 2.0 port that connects to a USB flash drive or other storage devices to extend the storage space of the AP.
- Default button: Reset button used to restore factory defaults and restart the device if you press and hold down the button for more than 3 seconds.
- GE3/PoE_OUT: 10M/100M/1000M auto-sensing port that connects to the wired Ethernet and supports PoE output.
- GE0 to GE2: 10M/100M/1000M auto-sensing port that connects to the wired Ethernet.
- PASS-THRU: a pair of RJ45 passthrough ports for transparent data transmission and interconnection with Ethernet cables or telephone lines.
- 2.5GE/PoE_IN: 100M/1000M/2.5G auto-sensing port that connects to the wired Ethernet. The port can connect to a PoE power supply device to provide power for APs.
- SFP+: Ethernet port that can work at the rate of 1 Gbps or 10 Gbps through auto-sensing and works with a matching optical module.

AirEngine 9700D-M



| Specification Item | Details |
|----------------------------------|---|
| Dimensions (H x W x D) | 43.6 mm x 420 mm x 442 mm |
| Port | 24 x 10/100/1000BASE-T (PoE OUT) + 4 x SFP+ (10GE) |
| Maximum number of manageable APs | Direct connection: 24 Extension through a switch: 48 Note: AirEngine 9700D-M can be connected only to AirEngine 5760-22WD. |
| Maximum number of access users | 4096 |
| Wireless protocol | 802.11a/b/g/n/ac/ac Wave 2/ax |
| Application scenario | Hotel, dormitory, and hospital |

- AirEngine 9700D-M is a central AP launched by Huawei, and has four 10GE uplink ports and twenty-four GE downlink ports. AirEngine 9700D-M can connect to remote units (RUs) in compliance with Wi-Fi 6 through Ethernet cables to centrally process and forward services. Such a wireless network formed by the central AP and RUs can fully utilize the RU throughput. Additionally, only one AP license is required, reducing customer investment. AirEngine 9700D-M can be deployed in an equipment room, weak-current well, or corridor, and RUs are deployed in rooms. Such an architecture is recommended for environments with high-density rooms and complex wall structure, such as schools, hotels, hospitals, and office meeting rooms.
- The RUs do not occupy AC licenses. The AC needs to manage only the AirEngine 9700D-M. As a result, only 200 APs are required to cover nearly 10,000 rooms.

Hardware Structure of AirEngine 9700D-M



Figure 1 Components of AirEngine 9700D-M (Front View)

| Components of AirEngine 9700D-M (Front View) | | | |
|--|--------------------|---|------|
| 1 | GE electrical port | 2 | SFP+ |
| 3 | Console | 4 | ETH |
| 5 | USB | 6 | PNP |

| Components of AirEngine 9700D-M (Rear View) | | | |
|---|--------------|---|--------------|
| 7 | Ground point | 8 | Power socket |

- AirEngine 9700D-M is a central AP launched by Huawei, and has four 10GE uplink ports and twenty-four GE downlink ports. AirEngine 9700D-M can connect to remote units (RUs) in compliance with Wi-Fi 6 through Ethernet cables to centrally process and forward services. Such a wireless network formed by the central AP and RUs can fully utilize the RU throughput. Additionally, only one AP license is required, reducing customer investment. AirEngine 9700D-M can be deployed in an equipment room, weak-current well, or corridor, and RUs are deployed in rooms. Such an architecture is recommended for environments with high-density rooms and complex wall structure, such as schools, hotels, hospitals, and office meeting rooms.
- GE electrical port: twenty-four 10M/100M/1000M auto-sensing Ethernet ports that are used for downlink data transmission and support PoE output.
- SFP+: four 10GE SFP+ Ethernet ports that can work at the rate of 1000 Mbps through auto-sensing. They can transmit and receive data at a rate of 1000 Mbps or 10 Gbps.
- Console port: connects to the maintenance terminal for AP configuration and management.
- ETH: reserved for later use.
- USB port: USB 2.0 port that connects to a USB flash drive to transfer configuration files and upgrade files.
- PNP: reset button. Pressing this button will restart the AP. Pressing and holding down this button for more than 6 seconds will restore factory defaults of the AP and restart the AP.
- Ground point: connects a ground cable to the AP.
- Power socket: connects to the power supply through an AC power cable.

AirEngine 8760R-X1E

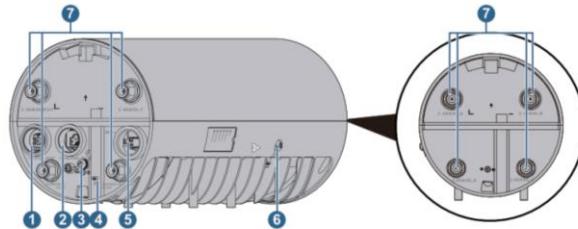


Features of the outdoor AP — AirEngine 8760R-X1E

- Working simultaneously on the 2.4 GHz and 5 GHz bands, providing a rate of up to 1.15 Gbps at 2.4 GHz, 9.6 Gbps at 5 GHz, and 10.75 Gbps for the device
 - Long-distance coverage mode: 2.4 GHz (8x8:8) + 5 GHz (8x8:8)
 - Triple-radio mode: 2.4 GHz (4x4:4) + 5 GHz (4x4:4) + 5 GHz (4x4:4)
 - Dual-radio + independent scanning mode: 2.4 GHz (4x4) + 5 GHz (4x4) + independent radio scanning
- 1 x 10GE electrical port + 1 x GE electrical port + 1 x 10GE optical port
- 6 kA/6 kV surge protection for Ethernet ports, IP68 waterproof and dustproof design, and extended operating temperature range of -40° C to +65° C, meeting industrial-grade requirements
- 5 kA surge protection for external antenna ports, eliminating the need to install an external surge protector, simplifying installation, and reducing costs
- Built-in independent scanning radio, achieving real-time detection for interference and rogue devices as well as timely network optimization
- Built-in Bluetooth module: Bluetooth serial interface-based O&M by collaborating with CloudCampus APP; accurately locating Bluetooth terminals and tags by collaborating with a location server
- Working modes: Fit, Fat, and cloud management

- AirEngine 8760R-X1E is a next-generation flagship outdoor AP in compliance with the Wi-Fi 6 standard. It provides excellent outdoor coverage performance and IP68 waterproof, dustproof, and surge protection capabilities. AirEngine 8760R-X1E provides uplink optical and electrical ports, allowing customers to select different deployment modes and saving customers' investment. These strengths make AirEngine 8760R-X1E ideal for high-density scenarios such as stadiums, squares, pedestrian streets, and amusement parks.

Hardware Structure of AirEngine 8760R-X1E



| AirEngine 8760R-X1E | | | |
|---------------------|--------------|---|---------------|
| 1 | GE/PoE_OUT | 2 | 10GE/PoE_IN |
| 3 | Ground screw | 4 | Security slot |
| 5 | SFP+ | 6 | Default |
| 7 | Antenna port | | |

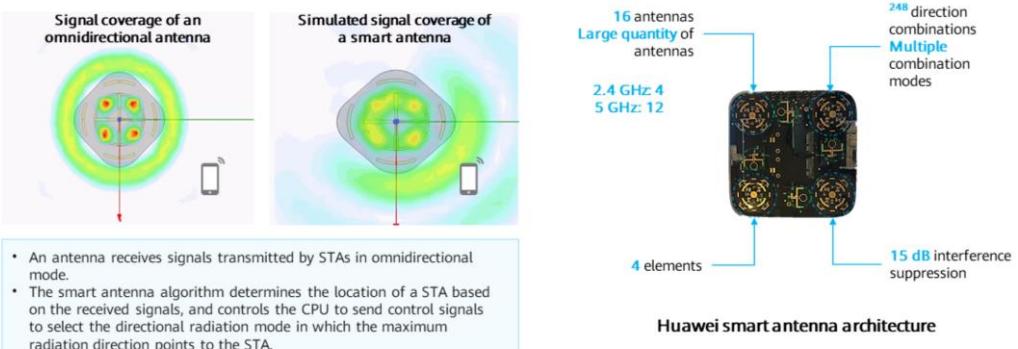
- GE/PoE_OUT: 10M/100M/1000M port that connects to the wired Ethernet and supports PoE output.
- 10GE/PoE_IN: 100M/1000M/2.5G/5G/10G port that connects to the wired Ethernet and supports PoE input.
- Ground screw: connects a ground cable to the AP.
- Security slot: connects to a security lock.
- SFP+: Ethernet port that can work at the rate of 1 Gbps or 10 Gbps through auto-sensing and works with a matching optical module.
- Default button: Reset button used to restore factory defaults and restart the device if you press and hold down the button for more than 3 seconds.
- Antenna port: connects to a 2.4 GHz/5 GHz dual-band antenna for transmitting and receiving service signals. The port type is N-type female. The 2.4G&5G_E/IoT port can be connected to an IoT antenna.

Contents

1. Wi-Fi 6 Technologies
2. Huawei WLAN Product Family
- 3. Features of Huawei WLAN Products**
4. AP Power Supply

Smart Antenna

- A smart antenna is an array of low-gain antennas that have the same polarization and are arranged and activated in a certain order. Based on the wave interference theory, they provide radiation patterns with high directivity and form the beams in expected directions.
- A smart antenna has multiple directional radiation patterns and one omnidirectional radiation pattern on the horizontal plane.



190 Huawei Confidential

 HUAWEI

- Advantages of smart antennas:

- Wide coverage: A smart antenna concentrates energy more effectively and has a high gain, therefore providing wide coverage. A smart omnidirectional antenna's coverage scope is equivalent to a directional antenna's coverage scope.
- High anti-interference capability: A smart antenna produces directional beams in space, with the main lobe pointing to useful signals' direction of arrival and side lobes and nulling beams point to interference signals' direction of arrival.
- Low radio pollution: Smart antennas provide satisfied power for STAs using low transmit power. This reduces the pollution of electromagnetic waves to the environment.

SDR

- Software Defined Radio (SDR) defines radios through software, and allows an AP to flexibly switch among three radio modes: dual-radio, triple-radio, and dual-radio + independent scanning radio.



Benefits of SDR

- In high-bandwidth scenarios, the dual-radio mode is used to provide higher throughput.
- In high-concurrency scenarios, the triple-radio mode is used to allow more STAs to access the network concurrently.
- In scenarios with severe interference, the dual-radio + independent scanning radio mode is used. In this mode, the independent radio is used to monitor and optimize the network quality in real time without compromising the network performance.
- On a large-scale network, APs working in different radio modes can be deployed together, meeting requirements of different services and traffic types, improving network-wide performance, and saving the total cost of ownership (TCO).

VIP Users Come First

| VIP users enjoy unlimited rate | VIP users enjoy priority scheduling |
|---|--|
| <p>After rate limiting is deployed on a network:</p> <ul style="list-style-type: none">• After a user is identified as a VIP user, the service rate of the VIP user is not limited.• The service rate of non-VIP users is still limited. | <ul style="list-style-type: none">• After a user is identified as a VIP subscriber, the service packet priority of the VIP subscriber is increased, improving the air interface competitiveness of the user.• Schedule VIP and common users in a certain proportion. When the air interface is congested, the service performance of VIP users is better than that of common users. |

Contents

1. Wi-Fi 6 Technologies
2. Huawei WLAN Product Family
3. Features of Huawei WLAN Products
- 4. AP Power Supply**

PoE Power Supply

- PoE power supply is recommended in most scenarios, such as enterprise offices, classrooms, dormitories, and stadiums.
- PoE transmits Ethernet data and supplies power over a single Ethernet cable. This technology facilitates construction and simplifies power supply, delivering stable and secure power supply.
- PoE switches are typically used to supply power to APs and are usually deployed in the central equipment room or an intermediate cabinet. In addition, different PoE switch models provide 8, 16, 24, 32, or 64 ports to connect to different numbers of APs.



PoE Power Supply Media

- Limited by Ethernet cable loss, IEEE 802.3 Ethernet data transmission complies with Ethernet cable requirements of ANSI/TIA/EIA-568-B. IEEE 802.3 defines various Ethernet cable types, such as CAT5/5e/6/6A, to meet different requirements for signal transmission bandwidth in the case of 100 m data transmission distance.

| Ethernet Cable Type | Signal Transmission Bandwidth | Ethernet Transmission Rate |
|---------------------|-------------------------------|----------------------------|
| CAT5e | 100 MHz | 100 Mbps, 1 Gbps, 2.5 Gbps |
| CAT6 | 250 MHz | 5 Gbps |
| CAT6A | 500 MHz | 10 Gbps |

- When Ethernet cables are used as the power supply medium, DC resistance will cause voltage drop and consumes power of the power supply end. Considering this, an Ethernet cable with smaller DC resistance consumes less power of the system.

PoE Power Supply Standards

- PoE power supply standards — IEEE 802.3af/at/bt — define the DC resistance of a 100 m Ethernet cable in compliance with the ISO/IEC11801 standard.
- When selecting a PoE switch, check whether the transmission rate and power supply standard of the PoE port match those of the AP. For example, if a Wi-Fi 6 AP is deployed, the maximum transmission rate and maximum power consumption of the AP are 6 Gbps and 30 W, respectively. To make full use of the AP capability, the PoE port of the PoE switch must provide a transmission rate of 10 Gbps. In this case, 802.3at or 802.3bt must be used.

| Standard | DC Resistance of a 100 m Ethernet Cable (Ω) | Output Power (W) |
|----------|--|------------------|
| 802.3af | 20 | ≤ 15.4 |
| 802.3at | 12.5 | ≤ 30 |
| 802.3bt | 12.5 | ≤ 90 |

- Ethernet cable routing accounts for 50% to 60% of the entire network engineering workload. In addition, there are some engineering activities that affect the buildings, such as cable routing through walls and pipes, and cable burying. As such, high-spec Ethernet cables are generally used to meet future network upgrade requirements. In addition, signal crosstalk and Ethernet cable twisting, or even jumper connections may exist in actual environments. With this in mind, it is recommended that the maximum length of an Ethernet cable be 80 m.

PoE Power Supply Module



- In actual networking, PoE power modules can be used to supply power to outdoor APs or some indoor APs that cannot be powered by PoE switches. Note that the PoE power module only functions as a network relay agent but not a network node. The total length of Ethernet cables at both ends of the PoE power module cannot exceed the length required by the network node.

- In outdoor scenarios, power supply and data transmission of an AP are generally separated. PoE modules are connected to the nearest power grid (AC) to supply power to APs. However, Ethernet cables are not long enough to meet data access requirements. In this case, optical fibers are used to transmit data. Optical fibers can significantly increase the data transmission distance between network nodes. For example, the transmission distance can reach 550 m when multimode optical modules are used together with multimode optical fibers. The transmission distance can reach 2 km, 10 km, or even 80 km when single-mode optical modules are used together with single-mode optical fibers.

DC Adapter



- If PoE power supply is unavailable at some indoor locations, DC power supply can be used. Select an appropriate mains AC-DC adapter to directly supply power to the AP. In this case, the AP's uplink network still needs to use Ethernet cables for data transmission.

Quiz

1. (Single Choice) Which of the following ACs has the highest forwarding performance?
 - A. AC6800V
 - B. AC6805
 - C. AirEngine 9700-M
 - D. AC6508

- 1. A

Summary

- This document describes the WLAN development process and key Wi-Fi 6 technologies.
- This document also describes Huawei's WLAN products in various scenarios, including ACs and APs. APs are classified into indoor settled APs, wall plate APs, agile distributed APs, and outdoor APs.
- Finally, this document describes some features of Huawei WLAN products.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



WLAN Networking Models



Foreword

- Different enterprises have varying requirements for WLANs. As WLANs are widely used on enterprise networks, how to build a WLAN that meets service needs becomes a key issue for enterprises. To build a good network, you need to design a good architecture and select a proper networking mode.
- This course describes the WLAN networking design and typical networking solutions.

Objectives

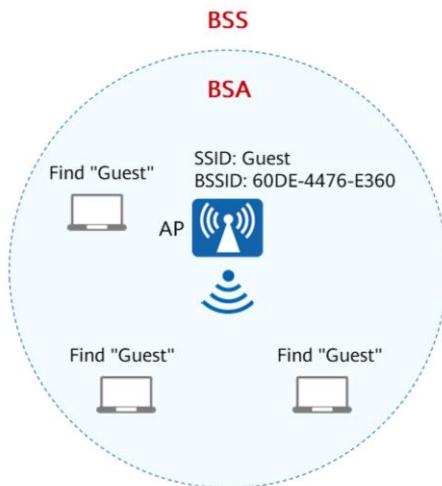
Upon completion of this course, you will be able to:

- Describe basic concepts in WLAN.
- Describe WLAN networking modes.
- Differentiate WLAN forwarding models.
- Evaluate Huawei's typical WLAN networking solutions.

Contents

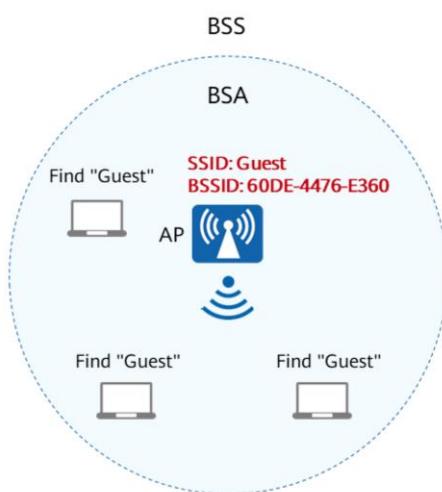
- 1. Basic Concepts in WLAN**
2. WLAN Networking Architectures
3. Typical WLAN Networking Solutions

BSS and BSA



- A basic service set (BSS) is the basic building block of a WLAN, and each BSS includes one fixed AP and more than one STA. The AP is used as a WLAN infrastructure that provides wireless communication services for STAs.
- The AP is in the center of the BSS and has a relatively fixed location. The BSS is located in the place where an AP resides. STAs in a BSS are distributed around the AP, and their locations are not fixed relative to the AP. Therefore, STAs can move freely, close to or away from the AP. The coverage area of an AP is referred to as a basic service area (BSA). STAs can freely enter or leave a BSA, and only STAs entering a BSA can communicate with the corresponding AP.

SSID and BSSID



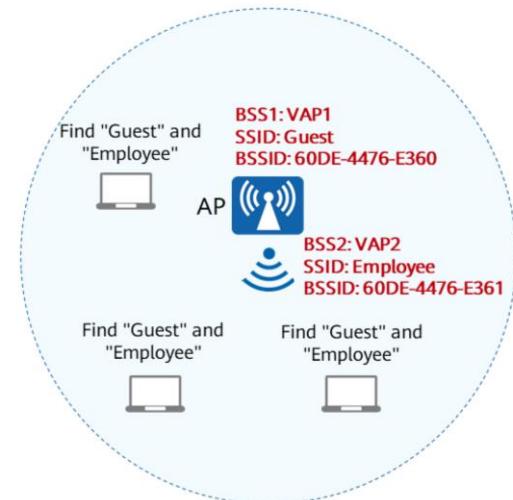
208 Huawei Confidential

- To discover an AP, a STA requires the AP to notify it of its identity, that is, the basic service set identifier (BSSID).
- A STA can see multiple BSSIDs in one airspace with multiple BSSs deployed, and only the desired BSSID needs to be selected. A STA does not automatically select a BSSID. Instead, you need to select one for it. As a BSSID is typically the MAC address of the AP in the BSS, you may not know which BSSID is the desired one if you see just character strings of MAC addresses. Therefore, to identify an AP's identity more easily, a character string that can be set is required as the name of an AP. This character string is called service set identifier (SSID).



- To distinguish BSSs, each BSS must have a unique BSSID. Therefore, the BSSID uses the MAC address of the AP to ensure its uniqueness. BSSIDs reside at 802.11 MAC layer and are used by APs to forward 802.11 packets.
- An SSID cannot be equal to a BSSID. Different BSSs can have the same SSID. If a BSSID is compared to the "ID card" of a BSS, the SSID is the name of the BSS. The WLAN names you search for on your STA are SSIDs.

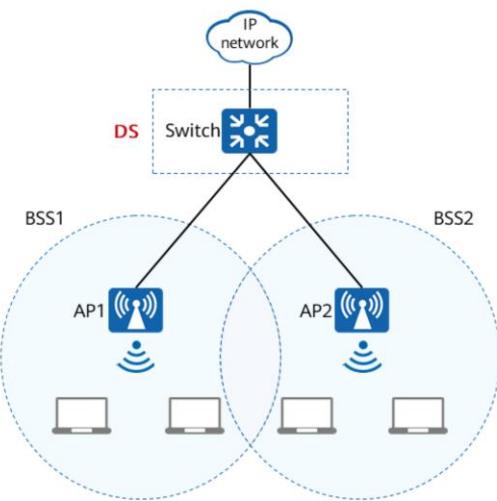
VAP



- An AP can be configured with multiple virtual access points (VAPs), and each VAP corresponds to one BSS. Therefore, only one AP needs to be deployed to provide multiple BSSs, for which different SSIDs can be set. By doing so, multiple WLANs can coexist in one airspace, which is also referred to as "multi-SSID".

- A BSSID uses the MAC address of an AP. Therefore, the number of required MAC addresses is the same as the number of VAPs supported by an AP.
- 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 makes 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 the same channel resources. The capacity of an AP will not change or multiply with the increasing number of VAPs.

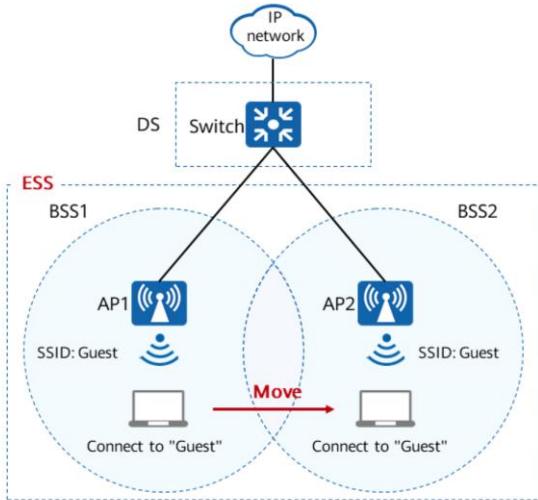
DS



- The BSS allows for wireless communication of multiple STAs within one area. The communication objects of STAs, however, are often scattered in different areas, even at the other end of the earth. In this case, the AP needs to be connected to a larger network to connect BSSs in different areas so that STAs can communicate. This network is the uplink network of the AP, which is called the distribution system (DS) of the BSS.

- The uplink network of an AP is usually an Ethernet network. Therefore, to connect to an uplink network, the AP must provide wired interfaces in addition to wireless radios. After receiving wireless packets from a STA, an AP converts the packets into wired packets and sends them to the uplink network. The uplink network then forwards the packets to another AP. The uplink network of an AP can also be a wireless network. For example, in areas where cables are difficult to lay out, APs can wirelessly connect to other APs working in bridge mode or connect to a mobile network by extending the LTE function on the APs.

ESS



- Generally, the effective coverage radius of a BSS is 10 m to 15 m. To cover a larger area, multiple BSSs can be used.
- In addition, to prevent users from being aware of BSS changes, multiple BSSs can share the same SSID. By implementing this, regardless of where you move, it can be considered that you use the same WLAN.
- This is called an extended service set (ESS), which extends the BSS range, allows flexible combination of BSSs, and makes WLAN deployment very flexible.
- In this case, the SSID of each BSS is called an extended service set identifier (ESSID), which is used to notify STAs of a continuous WLAN.

- The SSID of each BSS is called an extended service set identifier (ESSID), which is used to notify STAs of a continuous WLAN.

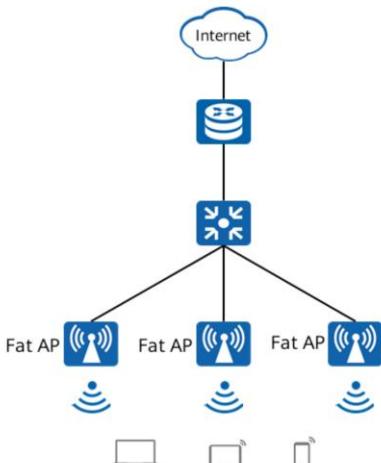
Basic Concepts in WLAN

| Concept | Full Name | Description |
|---------|---------------------------------|--|
| BSS | Basic Service Set | A BSS provides a basic building block of a WLAN and consists of one AP and some STAs associated with the AP. |
| ESS | Extended Service Set | An ESS is a set of two or more BSSs that share the same SSID, and is used to extend the coverage range of a BSS. |
| SSID | Service Set Identifier | An SSID identifies a wireless network. |
| ESSID | Extended Service Set Identifier | An ESSID identifies one or a group of wireless networks. |
| BSSID | Basic Service Set Identifier | BSSIDs identify VAPs on the same physical AP at the link layer. They are also used to identify BSSs in an ESS. |
| VAP | Virtual Access Point | A VAP is a functional entity on an AP. Different VAPs can be created on an AP to provide wireless access services for different user groups. |

Contents

1. Basic Concepts in WLAN
2. **WLAN Networking Architectures**
3. Typical WLAN Networking Solutions

Fat AP Architecture

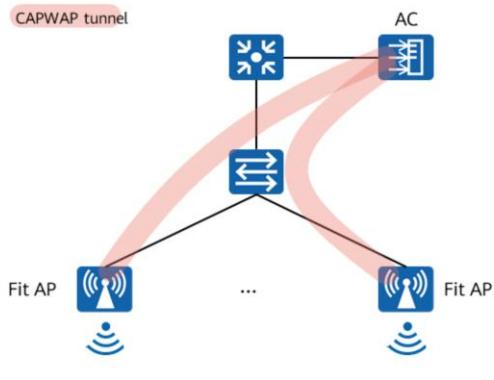


- The Fat AP architecture is also called autonomous network architecture.
- A Fat AP is independent and requires no additional centralized control device. Therefore, the Fat AP networking architecture is easy to deploy and cost-effective.
- However, the increase in the WLAN coverage area and the number of access users in enterprises requires more and more Fat APs. No unified control device is available for these independently working Fat APs, making it difficult to manage and maintain the Fat APs.
- Therefore, the Fat AP architecture is not recommended for enterprises. Instead, the "AC + Fit AP", cloud management, and leader AP architectures are more suitable.

- Fat AP architecture

- This architecture is also called autonomous network architecture because it does not require a dedicated device for centralized control and can implement functions such as wireless user access, service data encryption, and service data packet forwarding.
- Applicable scope: home
- Characteristics: A Fat AP works independently and requires separate configurations. It provides only simple functions and is cost-effective.
- 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



- An AC is responsible for WLAN access control, data forwarding and statistics collection, AP configuration and 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, collects air interface statistics, and is managed by an AC.
- The AC and Fit APs communicate through Control and Provisioning of Wireless Access Points (CAPWAP).
- Compared with the Fat AP architecture, the "AC + Fit AP" architecture has the following advantages:
 - Easier configuration and deployment
 - Higher security
 - Easier update and expansion

- The AC and Fit APs communicate through CAPWAP. With CAPWAP, APs automatically discover the AC, the AC authenticates the APs, and the APs obtain the software package and the initial and dynamic configurations from the AC. CAPWAP tunnels are established between the AC and APs. CAPWAP tunnels include control and data tunnels. The control tunnel is used to transmit control packets (also called management packets, which are used by the AC to manage and control APs). The data tunnel is used to transmit data packets. The CAPWAP tunnels allow for Datagram Transport Layer Security (DTLS) encryption, so that transmitted packets are more secure.
- Compared with the Fat AP architecture, the "AC + Fit AP" architecture has the following advantages:
 - Configuration and deployment: The AC centrally configures and manages the wireless network so that you do not need to configure each AP separately. In addition, the channels and power of APs on the entire network are automatically adjusted, eliminating the need for manual adjustment.
 - Security: Fat APs cannot be upgraded in a unified manner, which cannot ensure the latest security patches are installed for all AP versions. In the "AC + Fit AP" architecture, security capabilities are mainly implemented on the AC, and we only

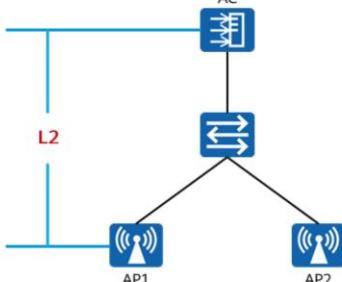
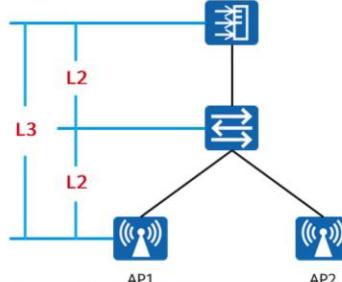
need to perform the software upgrade and security configuration on the AC. This allows for quick global security settings. Additionally, to prevent malicious code from being loaded, the AC performs digital signature authentication on the software, enhancing the security of the update process. The AC also implements some security functions that are not supported by the Fat AP architecture, including advanced security features such as virus detection, uniform resource locator (URL) filtering, and stateful inspection firewall.

- Upgrade and extension: The centralized management mode of this architecture enables APs on the same AC to run the same software version. When an upgrade is required, the AC obtains the new software package or patch and then upgrades the AP version. The separation of AP and AC functions prevents frequent AP version upgrades. We only need to update the user authentication, network management, and security functions on the AC.

"AC + Fit AP" Networking



Layer 2 Networking vs. Layer 3 Networking

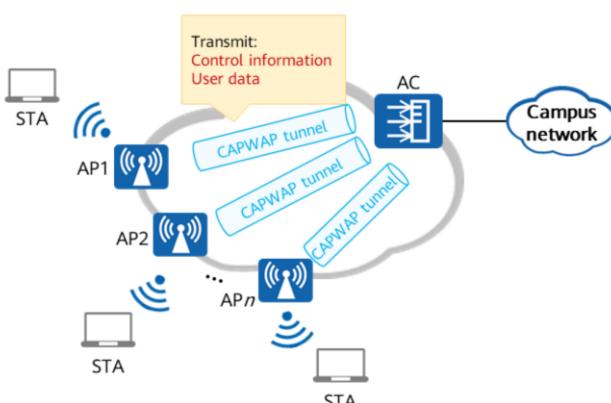
| Layer 2 Networking | Layer 3 Networking |
|--|---|
|  <ul style="list-style-type: none">Description: The AC and Fit APs are in the same broadcast domain. The Fit APs can directly discover the AC through local broadcast. The networking, configuration, and management are simple.Application scope: Layer 2 networking applies to small-scale networks, such as small-sized enterprise networks and is not recommended for large-sized enterprises that use complex WLAN networking, and require fine-grained management. |  <ul style="list-style-type: none">Description: The AC and Fit APs are in different network segments. The intermediate network must ensure that the Fit APs and AC are reachable to each other. Additional configurations are required to enable the Fit APs to discover the AC. The networking is flexible and easy to expand.Application scope: Layer 3 networking is suitable for medium- and large-scale networks. For example, on a large-scale campus network, APs are deployed in each building for wireless coverage, and the AC is deployed in the core equipment room for unified management and control. In this case, a complex Layer 3 network must be deployed between the AC and Fit APs. |

- In Layer 2 networking, the AC and Fit APs are in the same broadcast domain. The Fit APs can discover the AC through local broadcast. The networking, configuration, and management are simple. However, this mode is not applicable to large-scale networks.
- In Layer 3 networking, the AC and Fit APs are in different network segments, making the configuration complex. The intermediate network must ensure that the Fit APs and AC are reachable to each other. Additional configurations are required to enable the Fit APs to discover the AC. Layer 3 networking is suitable for medium- and large-scale networks. When ACs and APs are connected through a Layer 3 network and the APs discover an AC in DHCP/DNS mode (the AC functioning as the DHCP server), the devices between the APs and the AC must support the DHCP relay function.

In-Path Networking vs. Off-Path Networking

| In-Path Networking | Off-Path Networking |
|--|---|
| <p>The diagram illustrates In-Path Networking. At the top is a router labeled R1. Below it is an AC (Aggregation Controller) unit, which is connected to two APs (Access Points) labeled AP1 and AP2. A central vertical line with a double-headed arrow symbol connects the AC to the APs. Additionally, there is a direct connection between the AC and the router R1.</p> <ul style="list-style-type: none">Description: An AC functions as both a wireless access controller and an aggregation switch to centrally forward and process the data and management services of APs.Application scope: newly deployed small- and medium-scale centralized WLANs | <p>The diagram illustrates Off-Path Networking. At the top is a router labeled R1. Below it is an AC (Aggregation Controller) unit, which is connected to two APs (Access Points) labeled AP1 and AP2. A central vertical line with a double-headed arrow symbol connects the APs to the AC. Additionally, there is a direct connection between the AC and the router R1.</p> <ul style="list-style-type: none">Description: An AC is connected to the live network in off-path mode and processes only the management services of APs. The service data of APs reaches the uplink network without passing through the AC.Application scope: network reconstruction or construction of large- and medium-sized campus networks |

CAPWAP Overview



What Is a CAPWAP Tunnel?

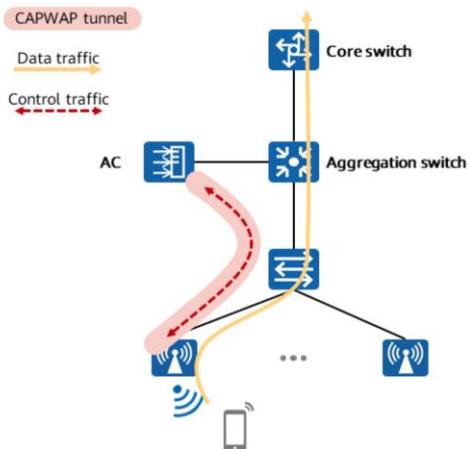
- **CAPWAP:** This protocol defines how to manage and configure APs. That is, an AC manages and controls APs in a centralized manner through CAPWAP tunnels.

CAPWAP Tunnel Functions

- Allows APs to automatically discover the AC.
- Maintains the connectivity state between 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, multiple APs on the network need to be centrally managed. The traditional WLAN architecture cannot meet the requirements of large-scale networking. Therefore, the Internet Engineering Task Force (IETF) sets up the CAPWAP working group and formulates the CAPWAP protocol. This protocol defines how an AC manages and configures APs. That is, a CAPWAP tunnel is established between an AC and an AP, through which the AC manages and controls the AP.
- CAPWAP is an application-layer protocol based on UDP.
 - CAPWAP transports two types of messages at the transport layer:
 - Service data traffic, which is encapsulated and forwarded through the CAPWAP data tunnel
 - Management traffic, which manages messages exchanged between the AP and AC through the CAPWAP control tunnel.
 - CAPWAP data and control packets are transmitted on different UDP ports:
 - Management traffic: UDP port 5246
 - Service data traffic: UDP port 5247

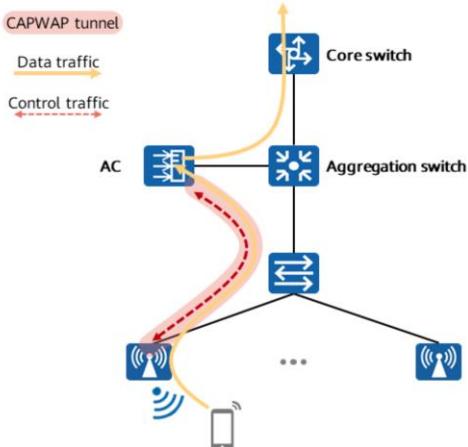
Direct Forwarding



- Direct forwarding: An AP directly forwards user data packets to an upper-layer network without encapsulating them over a CAPWAP tunnel. The AC only manages APs, and all service data is forwarded locally.
- Advantages: Data traffic does not pass through the AC, so the AC load is light. This mode is recommended for 10GE campus networks.

- In direct forwarding mode, wireless user service data is translated on the AP from 802.3 packets into 802.11 packets, which are then forwarded by an upstream aggregation switch.
- The AC only manages APs, and service data is forwarded locally. Management traffic is encapsulated in the CAPWAP tunnel and terminated on the AC, whereas AP service data traffic is directly forwarded by the AP to a switching device without CAPWAP encapsulation.
- The data forwarding mode is commonly used. Wireless user service data does not need to be processed by an AC, eliminating the bandwidth bottleneck and facilitating the usage of existing security policies. Therefore, this mode is recommended for converged network deployment.
- Direct forwarding is often used in in-path networking mode. This networking mode simplifies the network architecture and applies to small- and medium-scale centralized WLANs.
- Direct forwarding can also be used in off-path networking mode. In this mode, wireless user service data does not need to be processed by an AC, eliminating the bandwidth bottleneck and facilitating the usage of existing security policies. This mode applies to wired and wireless converged large-scale campus networks or HQ-branch scenarios.

Tunnel Forwarding



- Tunnel forwarding: Service data packets are encapsulated by APs and then transmitted to the AC for forwarding. The AC manages the APs and forwards AP traffic.
- User data packets are encapsulated in the CAPWAP tunnel and forwarded by the AC to the upper-layer network.
- Advantages: All service data traffic and management traffic pass through the AC, making it easier to implement security control policies on wireless users.

- Tunnel forwarding is usually used together with off-path networking. The AC centrally forwards data packets, which is secure and facilitates centralized management and control. New devices can be easily deployed and configured, with small changes to the live network. This forwarding mode applies to independent WLAN deployment or centralized management and control on large-scale campus networks.

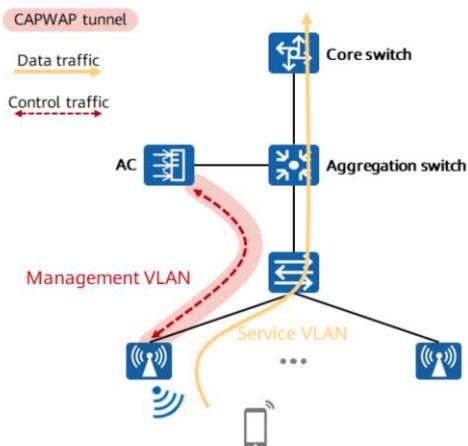
Comparison of "AC + Fit AP" Networking Modes

| Networking | Characteristics |
|--|---|
| In-path mode + Layer 2 networking + direct forwarding | No data bypassing and high forwarding efficiency |
| Off-path mode + Layer 2 networking + direct forwarding | No data bypassing and high forwarding efficiency, facilitating WLAN deployment on the live network and deployment of the hot standby (HSB) solution |
| Off-path mode + Layer 2 networking + tunnel forwarding | Simple data VLAN configuration and Layer 2 tunnels provided by tunnel forwarding for supporting 802.1X authentication, facilitating WLAN deployment on the live network and deployment of the HSB solution. |
| Off-path mode + Layer 3 networking + tunnel forwarding | Simple data VLAN configuration and Layer 2 tunnels provided by tunnel forwarding for supporting 802.1X authentication, facilitating WLAN deployment on the live network and deployment of the HSB solution. |
| Off-path mode + Layer 3 networking + direct forwarding | No data bypassing and high forwarding efficiency, facilitating WLAN deployment on the live network and deployment of the HSB solution |

"AC + Fit AP" Architecture Planning

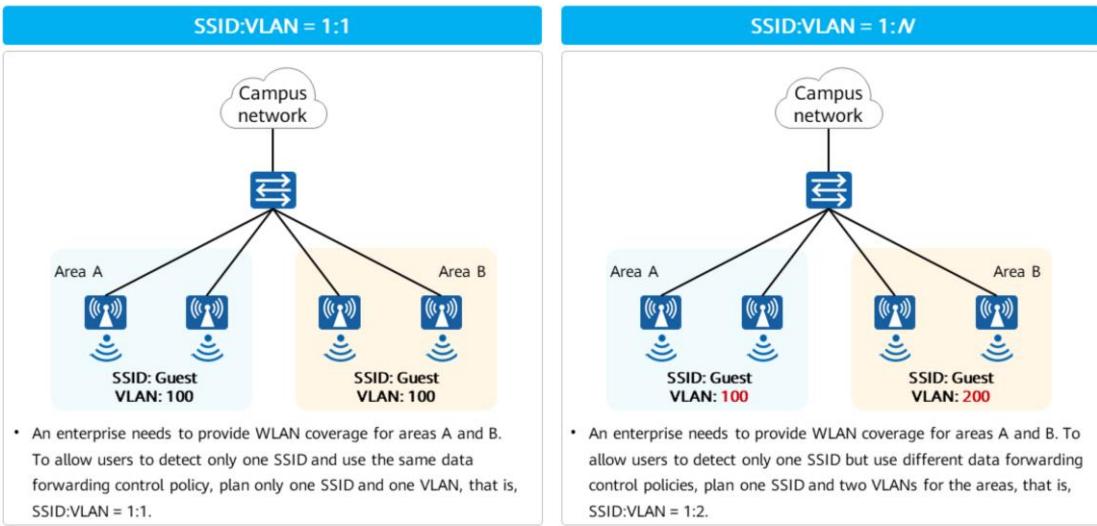


VLAN Planning



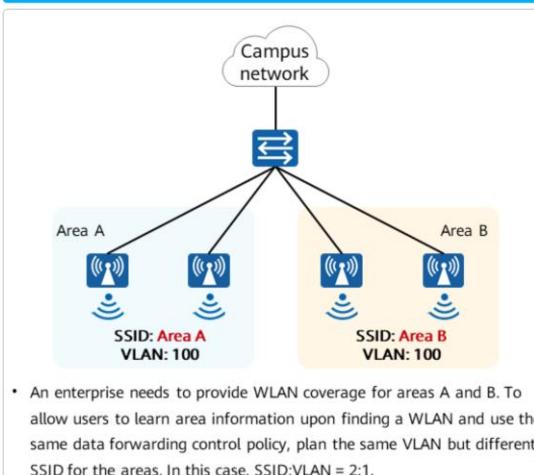
- Two types of VLANs on a WLAN:
 - **Management VLAN:** transmits packets that are forwarded through CAPWAP tunnels, including management packets and service data packets forwarded through CAPWAP tunnels.
 - **Service VLAN:** transmits service data packets.
- Note the following principles when planning VLANs:
 - The management VLAN is isolated from the service VLAN.
 - Service VLANs need to map to SSIDs based on service requirements.

Mapping Between SSIDs and Service VLANs (1)



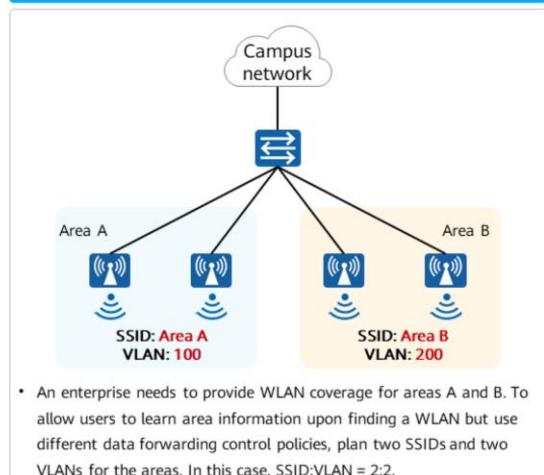
Mapping Between SSIDs and Service VLANs (2)

SSID:VLAN = $N:1$



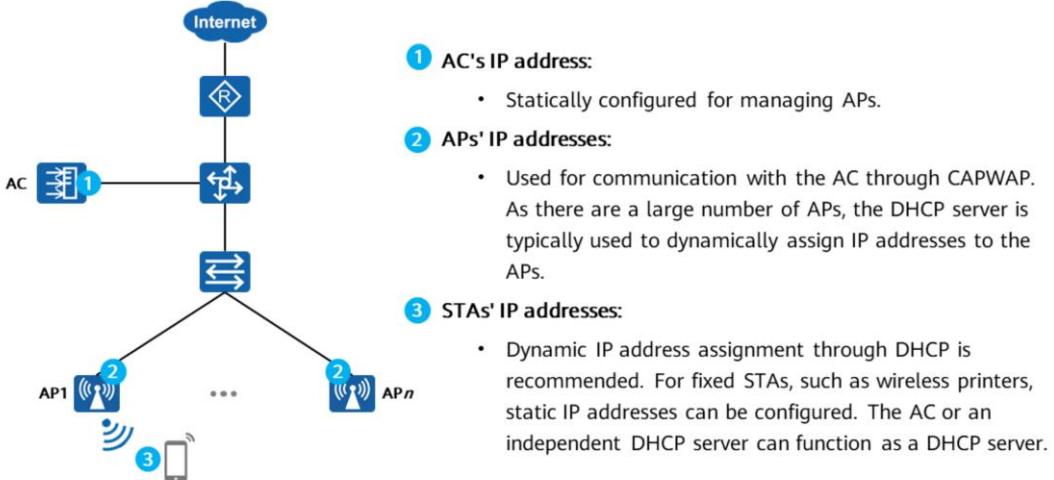
- An enterprise needs to provide WLAN coverage for areas A and B. To allow users to learn area information upon finding a WLAN and use the same data forwarding control policy, plan the same VLAN but different SSID for the areas. In this case, SSID:VLAN = 2:1.

SSID:VLAN = $N:M$



- An enterprise needs to provide WLAN coverage for areas A and B. To allow users to learn area information upon finding a WLAN but use different data forwarding control policies, plan two SSIDs and two VLANs for the areas. In this case, SSID:VLAN = 2:2.

IP Address Planning

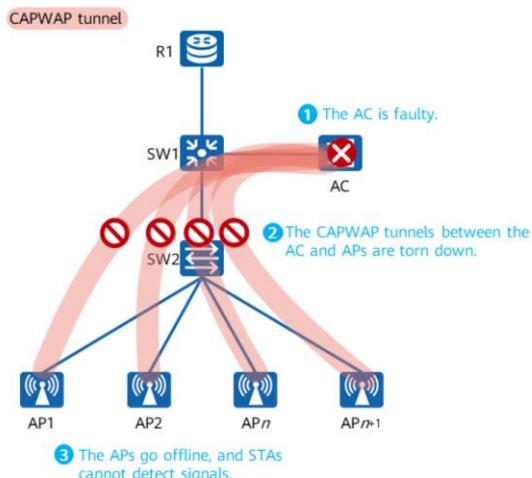


- The AC or an independent DHCP server (or a network device) can function as a DHCP server to assign IP addresses to APs.
- If the AC or independent DHCP server is connected to APs across a Layer 3 network, they must have a route between each other and a DHCP relay agent must be configured on the intermediate network.

"AC + Fit AP" Architecture Reliability

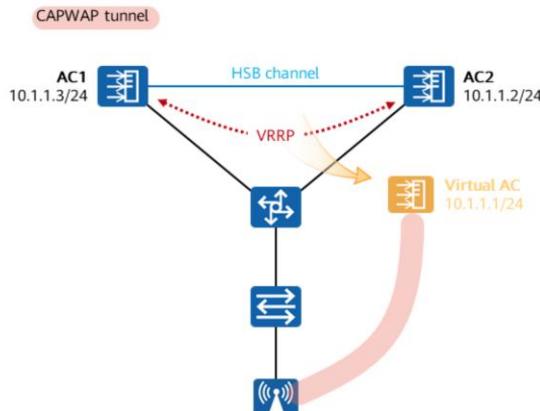


Single Point of Failure on an AC



- On a WLAN that uses the "AC + Fit AP" architecture, the AC centrally manages all APs and delivers configurations to them through CAPWAP tunnels.
- Once the AC is faulty, the CAPWAP tunnels between the AC and all APs are disconnected. As a result, the APs go offline and STAs cannot detect WLAN signals. All WLAN users on the network cannot access the Internet.

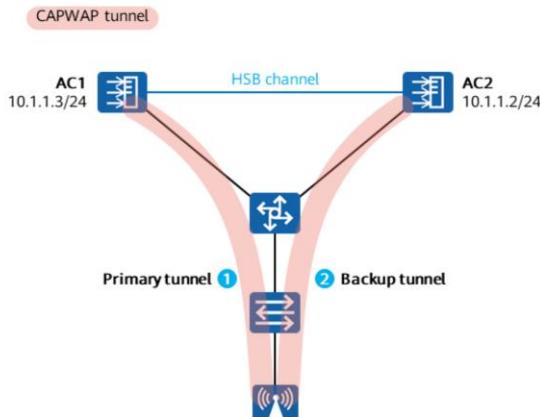
AC Reliability: VRRP HSB



- Two ACs are added to a VRRP group to share a virtual IP address. The master AC synchronizes service information to the backup AC through an HSB channel.
- By default, the master and backup ACs are virtualized into one virtual AC. If the master AC fails, the backup AC takes over services. All APs establish CAPWAP tunnels with the virtual AC.
- The switchover between ACs is determined by the VRRP. To APs, there is only one AC.
- This mode restricts deployment locations of the two ACs but supports a faster switchover speed than other backup modes.

- Currently, the AC supports HSB of a single VRRP instance, but does not support load balancing. HSB has the following characteristics:
 - Uplinks can back up each other. The master and backup devices in a VRRP group can track the status of uplink interfaces. The master/backup status of an AC may be different from its downlink status.
 - MSTP is used to prevent loops on multiple downlinks (including wired and wireless links). When the MSTP status changes, the MAC/ARP entries on the links are automatically deleted.
- During the network design, consider the redundancy design for devices and links and deploy switchover policies. In this way, even if a single point of failure occurs, the system functions are not affected. The AC backup design is essential to the "AC + Fit AP" architecture.

AC Reliability: Dual-Link HSB



- An AP sets up CAPWAP tunnels with both the active and standby ACs. ACs synchronize service information through an HSB channel.
- When the tunnel between the AP and active AC fails, the AP instructs the standby AC to take over services from the active AC.
- The active and standby ACs are determined based on AC priorities. When ACs have the same priority, the active and standby ACs are determined based on the AC load (number of online APs and STAs).

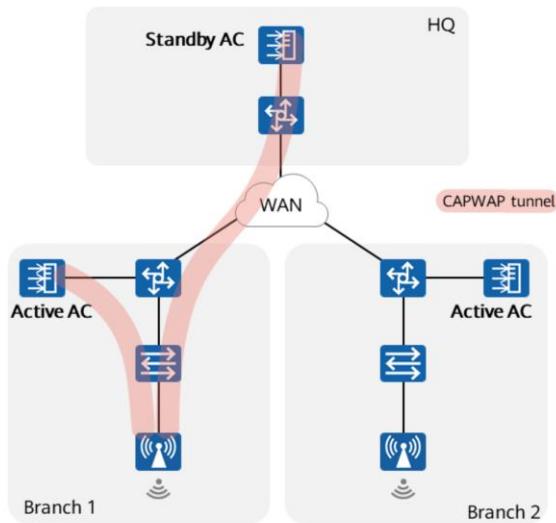
- In addition to the active/standby HSB mode, the load balancing mode is supported. In load balancing mode, you can specify AC1 as the active AC for some APs and AC2 as the active AC for other APs, so that the APs set up primary CAPWAP tunnels with their own active ACs.
- Dual-link HSB frees active and standby ACs from location restrictions and allows for flexible deployment. The two ACs can implement load balancing to make efficient use of resources. However, service switching takes a relatively long time.

HSB

- HSB is Huawei's public active/standby mechanism.
- HSB service: establishes and maintains an HSB channel, and notifies the active and standby service modules of channel connect/disconnect events.
- HSB group: has an HSB service bound to provide a data backup channel for each of active and standby service modules. An HSB group is bound to a VRRP instance, and the active and standby instances are negotiated using the VRRP mechanism. Additionally, the HSB group instructs service modules to process events such as batch backup, real-time backup, and active/standby switchover.

- When the active AC fails, service traffic can be switched to the standby AC only if the standby AC has the same session entries as the active AC. Otherwise, the session may be interrupted. Therefore, a mechanism is required to synchronize session information to the standby device when session entries are created or modified on the active device. The HSB module provides the data backup function. It establishes an HSB channel between two devices that back up each other, maintains the link status of the HSB channel, and sends and receives packets.
- HSB service backup in real time involves backup for the following information:
 - User data information
 - CAPWAP tunnel information
 - AP entries
 - DHCP address information
- The HSB channel can be carried by a directly connected physical link between two ACs or by a switch.

AC Reliability: N+1 Backup



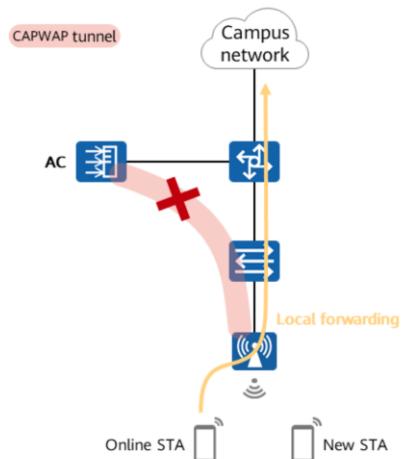
- N+1 backup uses one AC to provide backup services for multiple active ACs.
- When the network runs properly, an AP sets up a CAPWAP tunnel only with the active AC to which it belongs.
- If the active AC or the CAPWAP tunnel fails, the standby AC replaces the active AC to manage the AP and establishes a CAPWAP tunnel with the AP to provide services.
- Active/Standby switchover and switchback are supported.

- When the CAPWAP tunnel between an AP and the active AC is disconnected, the AP attempts to establish a CAPWAP tunnel with the standby AC. After the new CAPWAP tunnel is established, the AP restarts and obtains configurations from the standby AC. During this process, services are affected.

AC Reliability: Summary

| Comparison Item | VRRP HSB | Dual-Link HSB | N+1 Backup |
|--|--|--|---|
| Switching speed | The switchover speed is fast, with little impact on services. The configuration of the VRRP preemption delay implements a faster switchover than other backup modes. | The AP status switchover is slow and occurs only when CAPWAP link disconnection timeout is detected. After the AP status is switched, STAs do not need to go offline and online again. | The AP status switchover is slow and occurs only when CAPWAP link disconnection timeout is detected. APs and STAs need to go online again, and services are interrupted for a short period of time. |
| Deployment of active and standby ACs at different places | VRRP is a Layer 2 protocol and does not support deployment of active and standby ACs at different places. | Supported | Supported |
| Application scope | Scenarios that require high reliability, without the need for AC deployment at different places | Scenarios that require high reliability and AC deployment at different places | Scenarios with low reliability but high cost control requirements |

Service Reliability: Service Holding upon CAPWAP Link Disconnection in Local Forwarding Mode



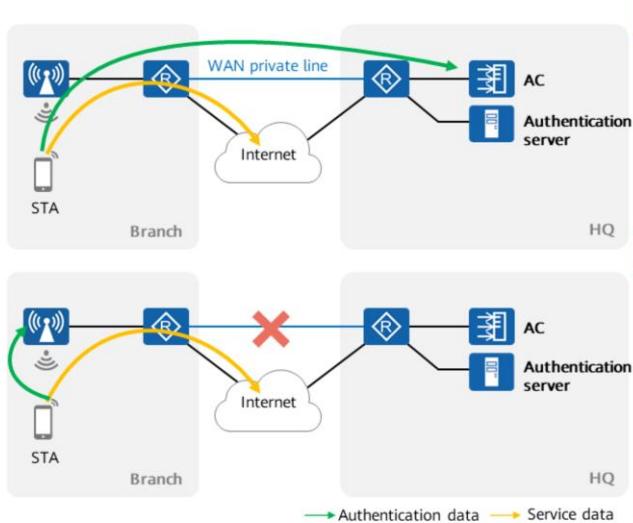
Function

- If the CAPWAP link between the AP and AC is disconnected, services of online STAs are not interrupted and user data can be forwarded normally.
- User data is forwarded in local forwarding mode.
- When the security policy on the AP wireless side is open system, shared key (WEP), or WPA/WPA2-PSK, new STAs can access the network and go online.

Application Scenario

On a small-scale WLAN without the AC backup design, this feature ensures uninterrupted user data forwarding when an AP disconnects from an AC, improving service reliability.

Service Reliability: WAN Authentication Bypass



Function

- Traditionally, user authentication is performed on the AC. When the communication between the AC and AP is interrupted, new users cannot access the network because they cannot be authenticated.
- WAN authentication bypass: When the link between the AC and AP is disconnected, the AP provides the local authentication function to authenticate newly connected users, ensuring service reliability.

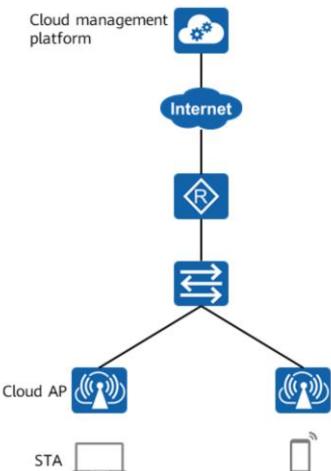
Application Scenario

The HQ and branches are connected across a WAN. The AC is deployed at the HQ, and APs are deployed at branches. If the branch APs are disconnected from the AC at the HQ, services of online STAs run properly after service holding upon CAPWAP link disconnection is configured. However, new STAs cannot connect to the network, affecting user experience. The WAN authentication bypass solution can be deployed on the campus network so that new STAs can still connect to the network after branch APs are disconnected from the AC at the HQ.

- WAN authentication bypass typically applies to HQ-branch networks where branch networks connect to the HQ network across a WAN. In traditional solutions, most WLAN services are centrally processed by ACs, posing high requirements for the WAN, for example, large bandwidth, low delay, and high stability. However, in actual scenarios, enterprise private lines are not often used between the HQ and branches. They often lease carrier networks, so the quality of intermediate networks cannot be ensured, resulting in poor network security and user experience.
- To solve the preceding problems, branch AP groups are created in branches, and services such as user access and access authentication are processed by APs. This approach reduces the dependency of branches on the HQ. If a branch is disconnected from the HQ, branch users can still use the WLAN.
- Implementation process: In the "AC + Fit AP" architecture, user authentication is performed on the AC, and only rights control is performed on the AP. Therefore, access authentication configurations are not deployed on the AP. When the WAN is interrupted and the AC and APs are disconnected, the APs need to have the local authentication function configured and authenticate newly accessed STAs. In this case, the AC needs to deliver access authentication configurations to the APs.
 - Delivery of the same configuration information on the AP and AC: To reduce the workload of the administrator, configurations in the VAP profile are reused for the same configuration on the AP and AC. Delivered configurations include the authentication profile bound to the VAP profile, as well as the 802.1X and MAC access profiles bound to the authentication profile.
 - Delivery of different configuration information on the AP and AC: Different

information includes local accounts required when local authentication is performed for STAs and configurations related to the authentication mode. For 802.1X users, a built-in RADIUS server needs to be configured for processing EAP authentication packets. Different information on the AP and AC is configured in the branch AP group view, and APs in the same branch AP group have the same delivered information.

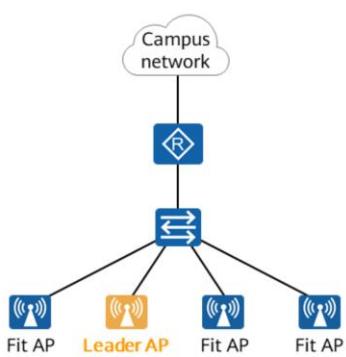
Cloud Management Architecture



- The cloud management platform manages and configures cloud APs and manages STA access in a unified manner.
- Compared with the traditional "AC + Fit AP" architecture, the cloud management architecture has the following advantages:
 - Plug-and-play and automatic deployment reduce network deployment costs.
 - Unified O&M: All cloud managed NEs are centrally monitored and managed on the cloud management platform.
- This architecture applies to small to midsize WLANs and allows for flexible deployment and low O&M costs

- 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. The cloud management architecture can solve these problems. Using this architecture, devices can be managed and maintained 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 being powered 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 AP through the cloud management platform at anytime and anywhere, facilitating batch service configurations.

Leader AP Architecture



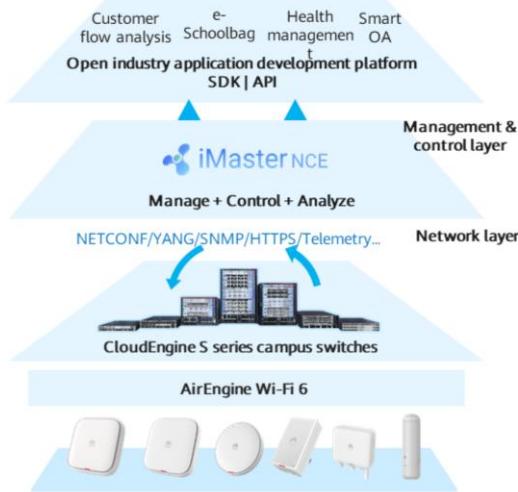
- The leader AP architecture involves APs only. After one AP is configured as the leader AP, the other APs will access the network in Fit AP mode and can communicate with the leader AP at Layer 2.
- The leader AP broadcasts its role on the Layer 2 network, and the other APs automatically discover and connect to the leader AP.
- Similar to the AC, the leader AP provides unified access management, configuration, and O&M based on CAPWAP tunnels, enabling centralized wireless resource management and roaming management.
- Users only need to log in to the leader AP and configure wireless services. After the configuration, all APs provide the same wireless services, and STAs can roam between different APs.

- Some micro and small enterprises need to build their own wireless networks that are managed independently without the cloud management architecture. If the Fat AP architecture is used, APs cannot be managed and maintained in a unified manner, and users cannot enjoy good roaming experience. If the "AC + Fit AP" architecture is used, only a few APs are required due to the small number of STAs and the small wireless coverage area, but the AC and license costs are high. If an AP can manage other APs and provide unified O&M capability and continuous roaming experience, the enterprises' requirement can be met. The leader AP architecture designed by Huawei will work.
- The leader AP architecture involves APs only. After purchasing APs, a user can set one AP to the leader AP mode and connect the other APs to the network in Fit AP mode. The other APs communicate with the leader AP at Layer 2. After the leader AP broadcasts its role on the Layer 2 network, the other APs automatically discover and connect to the leader AP. Similar to the AC, the leader AP provides unified access management, configuration, and O&M based on CAPWAP tunnels, enabling centralized wireless resource management and roaming management. Users only need to log in to the leader AP and configure wireless services. After the configuration, all APs provide the same wireless services, and STAs can roam between different APs.

WLAN Networking Architecture Comparison

| Networking Architecture | Characteristics | Application Scenario |
|-------------------------------|---|------------------------------|
| Fat AP architecture | Fat APs need to be independently deployed and configured, complicating management and maintenance. | SOHO |
| "AC + Fit AP" architecture | The AC centrally manages and configures APs, simplifying configuration and deployment. | Large- and medium-sized WLAN |
| Cloud management architecture | The cloud management platform centrally manages and configures APs, simplifying deployment and O&M. | Small- and medium-sized WLAN |
| Leader AP architecture | The leader AP centrally manages and configures APs, simplifying configuration and deployment. | Small-sized WLAN |

Next-Generation Networking Architecture: CloudCampus



242 Huawei Confidential



- Huawei CloudCampus Solution for small- and medium-sized campus networks uses cloud computing technology to implement automatic and centralized network management, and provides data collection and analysis capabilities that are unavailable on traditional networks, so as to achieve network (LAN/WLAN) as a service (NaaS). It has the following features:
 - Simple network planning and deployment
 - On-demand network and management expansion
 - Network data and network platform openness

- Simple network planning: The cloud-based or offline WLAN planning tool (WLAN Planner) provides building drawings, automatic deployment, and many more capabilities, making network planning easy and efficient.
- Simple network deployment: The cloud-based plug-and-play solution enables cloud managed devices to automatically register with iMaster NCE-Campus over the Internet, implementing zero touch provisioning (ZTP) and convenient deployment of vast quantities of network devices.
- On-demand network expansion: iMaster NCE-Campus supports access management of ultra-large-scale and cross-regional devices. Enterprises can purchase devices and cloud services on demand to implement network expansion.
- On-demand management expansion: iMaster NCE-Campus supports multiple tenants. Enterprises can select a network management mode based on their capabilities and service requirements. In this way, enterprises can either manage and maintain their networks by themselves, or authorize a managed service provider (MSP) to manage and maintain their networks.
- Network data openness: iMaster NCE-Campus provides tenant-based terminal authentication and statistics analysis data. Enterprise tenants can obtain data on demand and analyze the data to boost business optimization.
- Network platform openness: Based on the software-defined networking (SDN) architecture, iMaster NCE-Campus provides standard northbound APIs for partners and enterprise customers to develop third-party applications and value-added services (VASS), further building a cloud ecosystem together with Huawei and promoting

business innovation.

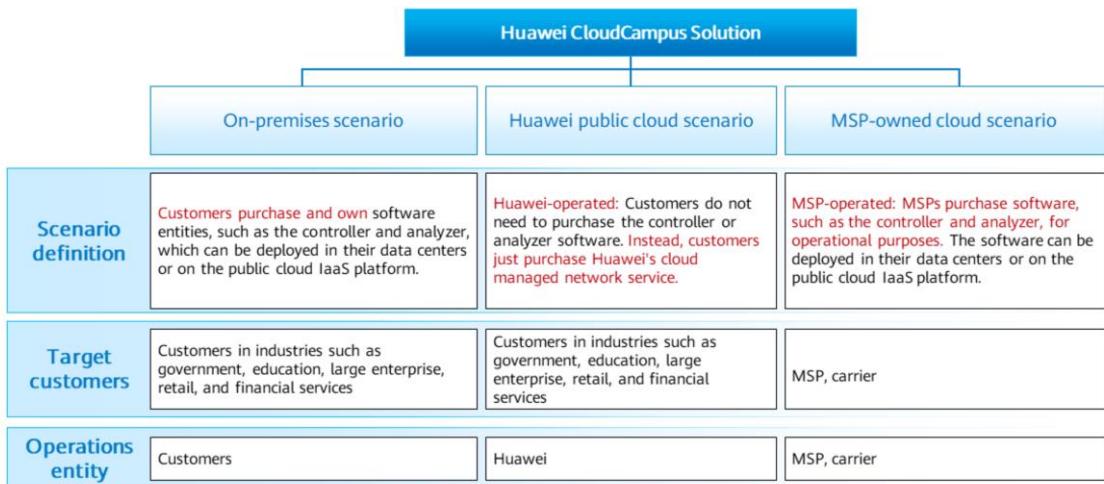
Highlights of the CloudCampus Solution for Small- and Medium-Sized Campus Networks

- Huawei CloudCampus Solution for small- and medium-sized campus networks uses cloud computing technology to implement automatic and centralized network management, and provides data collection and analysis capabilities that are unavailable on traditional networks, so as to achieve network (LAN/WLAN) as a service (NaaS).
 - Automatic deployment: Devices can be easily and quickly deployed.
 - Cloud-based WLAN planning and mobile O&M: WLAN design and device O&M are simplified.
 - Diversified product portfolios: Full series of network devices (switches, firewalls, ARs, and APs) of Huawei's Enterprise Networking Product Line can be used to provide different product portfolios, meeting diversified network requirements of tenants.
 - Dual-working-mode support and smooth evolution: All network devices used in this solution can work in either cloud or traditional management mode. Tenants can implement cloud-based network management after devices are upgraded.
 - Value-added services: Terminal behavior analysis is a value-added application of iMaster NCE. More value-added services can be developed based on terminal behavior analysis.

iMaster-NCE

- iMaster NCE is a controller that integrates management, control, and analysis functions. It supports simple-service campus networks, virtual campus networks, and interconnection among multi-branch campus networks, and includes the following parts:
 - iMaster NCE-Campus: provides management and control functions, integrates the management function of traditional devices as a service, and provides one-click redirection to iMaster NCE-CampusInsight based on the proxy service.
 - Authentication component of iMaster NCE-Campus: can be integrated into iMaster NCE-Campus as a service or deployed independently. A maximum of 20 authentication components can be deployed remotely to provide local authentication for remote branches. Authentication components and iMaster NCE-Campus can automatically synchronize user authentication information and terminal identification data through TCP channels.
 - iMaster NCE-CampusInsight: Huawei's intelligent network analysis platform. Based on existing O&M data (such as device performance indicators and terminal logs), iMaster NCE-CampusInsight uses big data, AI algorithms, and more advanced analysis technologies to digitize user experience on the network, helping customers detect network issues in a timely manner and improve user experience.

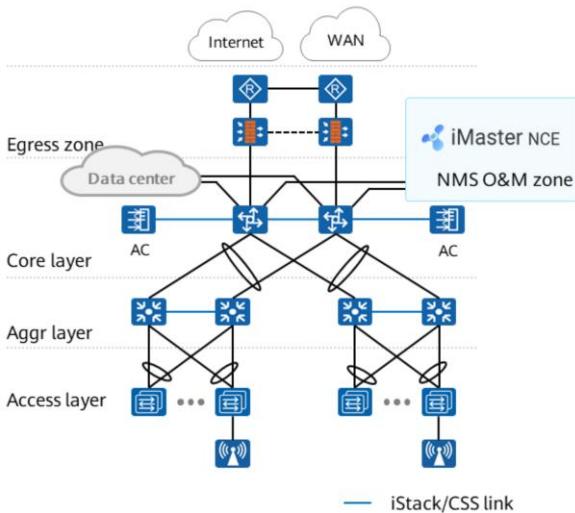
Three Deployment Modes of Huawei CloudCampus Solution



Contents

1. Basic Concepts in WLAN
2. WLAN Networking Architectures
- 3. Typical WLAN Networking Solutions**

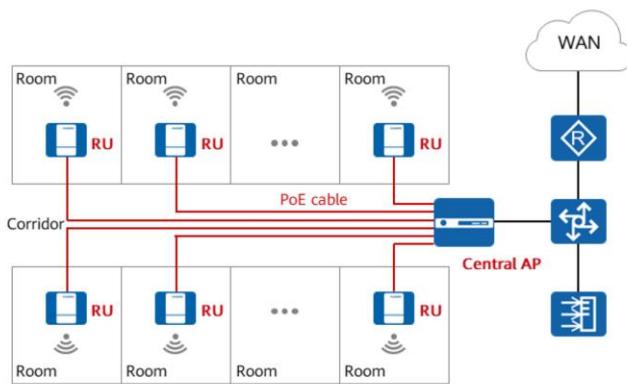
Large-Sized Campus Network Solution



Solution Description

- If a campus wired network has been deployed and a wireless network needs to be deployed independently or the wireless network scale is large, it is recommended that independent ACs be deployed.
- On a large-sized campus network, an AC is usually connected to an aggregation or core switch in off-path mode.
- To reduce changes to the existing wired network and facilitate centralized management and control of the AC, tunnel forwarding is recommended. To improve AC reliability, VRRP HSB is typically deployed in the independent AC solution.

Agile Distributed Wi-Fi Solution



Solution Description

- In the agile distributed architecture, the traditional AP is divided into two independent devices: a central AP and a remote unit (RU).
- Central APs are deployed in equipment rooms, weak-current wells, or corridors, while RUs are installed in rooms through network cables, providing high-quality, exclusive wireless access services to each room.

Application Scenario

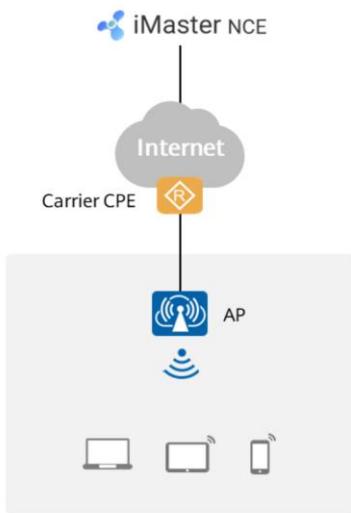
Scenarios with densely distributed rooms, such as dormitories, hotels, and wards

Advantages

- Simple management
- Flexible deployment and full signal coverage without coverage holes
- Long-distance coverage

- In scenarios with densely distributed rooms, such as dormitories, hotels, and wards, a large number of packets are sent to the AC if the "AC + Fit AP" architecture is used and an AP is deployed in each room. As a result, the AC may become a performance bottleneck. To address the performance bottleneck and signal coverage problems, we can deploy the APs on corridors and install antennas in each room to provide signal coverage. However, this solution has restrictions on the coverage distance because the signal attenuation increases at a long distance. If multiple rooms share one AP, the signal quality and performance are poor.
- Customer benefits:
 - Simple management:** The AC only needs to manage a small number of central APs, and only 200 APs require management to cover about 10,000 rooms.
 - Flexible deployment and full signal coverage without coverage holes:** A central AP connects to RUs through network cables, causing no wall penetration loss or feeder loss and providing high-quality signal coverage. The RUs support various mounting modes such as junction box-, wall-, and ceiling-mounting.
 - Long-distance coverage:** Different from traditional APs with antennas that support only 15 m coverage distance, the central AP can connect to RUs through network cables at a maximum distance of 100 m, expanding the network deployment scope by several times. If the central AP is deployed in a corridor, it can provide long-distance coverage (exceeding 100 m).

Small and Mini Chain Store Solution



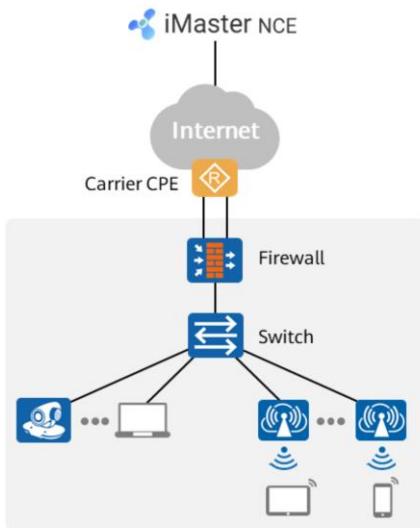
- **Solution Description**

- In single-AP networking, an AP functions as the gateway of STAs.

- **Application Scenario**

- Small stores (such as agent stores and gas stations) with an area of less than 50 m².
 - A maximum of 50 concurrent online STAs are supported.
 - Only wireless user access needs to be supported.
 - Only one wired Internet egress link is required.

Small and Midsize Chain Store Solution



- **Solution Description**

- Multiple APs are connected to the switch through PoE to provide wireless coverage. The firewall provides egress features, such as WAN access, DHCP, and NAT, and functions as the user gateway. The switch provides extended PoE access and wired terminal access functions. APs provide access for STAs at the site.

- **Application Scenario**

- Small and midsize experience stores, logistics stores, and insurance stores with an area of less than 3000 m² and fewer than 2000 concurrent online terminals.
- Multiple APs need to be deployed to provide wireless access, high security requirements (URL filtering/IPS/security protection/antivirus) need to be met, and multiple uplinks are required for Internet access.

Quiz

1. (Single Choice) An enterprise needs to implement device redundancy on a WLAN to ensure network stability. The enterprise requires that ACs have high reliability, the switchover speed be high when a link fault occurs, and the active and standby ACs are deployed at the HQ. In this scenario, which AC high reliability solution can the enterprise use?
 - A. VRRP HSB
 - B. Dual-link HSB
 - C. Dual-link cold standby
 - D. N+1 backup

- A

Summary

- This course describes basic WLAN concepts and various WLAN networking architectures, including the Fat AP architecture, "AC + Fit AP" architecture, cloud management architecture, leader AP architecture, and Huawei's CloudCampus architecture. After learning this course, you can understand the networking modes and forwarding models used in the "AC + Fit AP" architecture, and be able to perform simple networking design, including VLAN design, IP address design, and high reliability design.
- This course also introduces several typical Huawei WLAN networking solutions.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors
that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



Huawei VRP and Device Upgrade



Foreword

- The Versatile Routing Platform (VRP) is a universal operating system (OS) platform for Huawei datacom products. It is based on IP and adopts a component-based architecture. It provides rich features and functions, including application-based tailorable and extensible functions, greatly improving the running efficiency of the devices that use this OS. To efficiently manage such devices, you must be familiar with VRP and VRP-based configuration.
- In the mobile Internet era, with the increasing requirements of customers, we need to upgrade devices to improve system security and stability and develop new functions to improve user experience.

Objectives

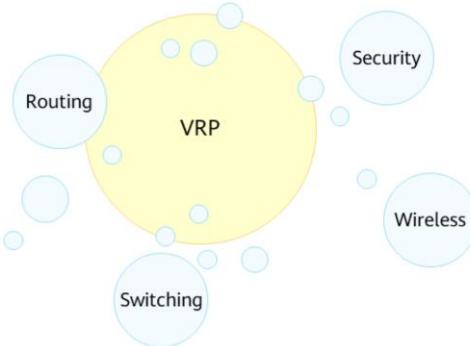
Upon completion of this course, you will be able to:

- Describe development of the VRP.
- Use VRP basic operation commands.
- Learn the methods of upgrading ACs and APs.
- Distinguish characteristics of Fit and Fat APs.
- Perform service configuration of Fat APs.

Contents

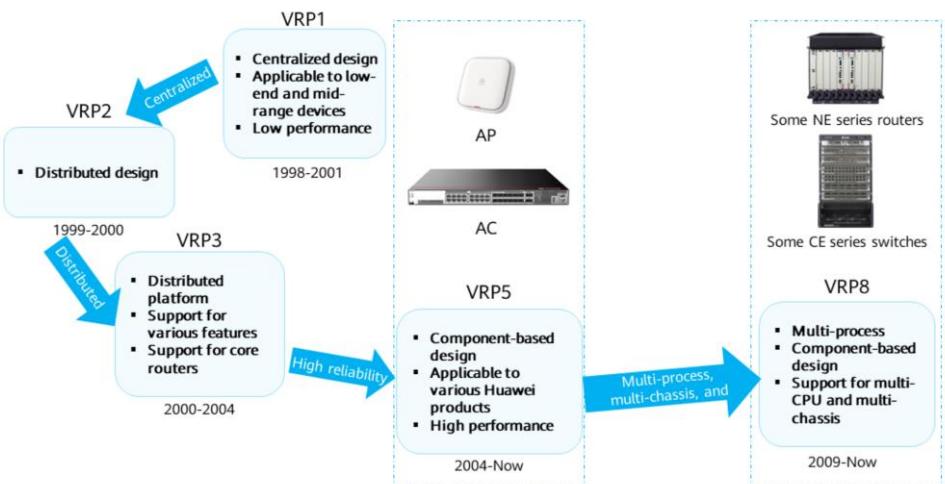
- 1. Huawei VRP Overview**
2. Command Line Basics
3. WLAN Device Upgrade
4. Fat AP Configuration

What Is VRP?



- VRP is a universal OS platform for Huawei datacom products. It serves as the software core engine of Huawei's full series of routers from low-end to core ones, Ethernet switches, service gateways, and so on.
- VRP provides the following functions:
 - Provides a unified user interface and a unified management interface.
 - Implements the functions of the control plane and defines the interface specifications of the forwarding plane.
 - Implements communication between the device forwarding plane and VRP control plane.
 - Shields the differences between the link layer and the network layer of each product.

Development of the VRP



File System

- The file system manages files and directories in storage media, allowing users to view, create, rename, and delete directories and copy, move, rename, and delete files.
- Mastering the basic operations of the file system is crucial for network engineers to efficiently manage the configuration files and VRP system files of devices.

The system software is a must for device startup and operation, providing support, management, and services for a device. The common file name extension is .cc.



A configuration file stores configuration commands, enabling a device to start with the configurations in the file. The common file name extensions are .cfg, zip, and .dat.

A patch is a kind of software compatible with the system software. It is used to fix bugs in system software. The common file name extension is .pat.

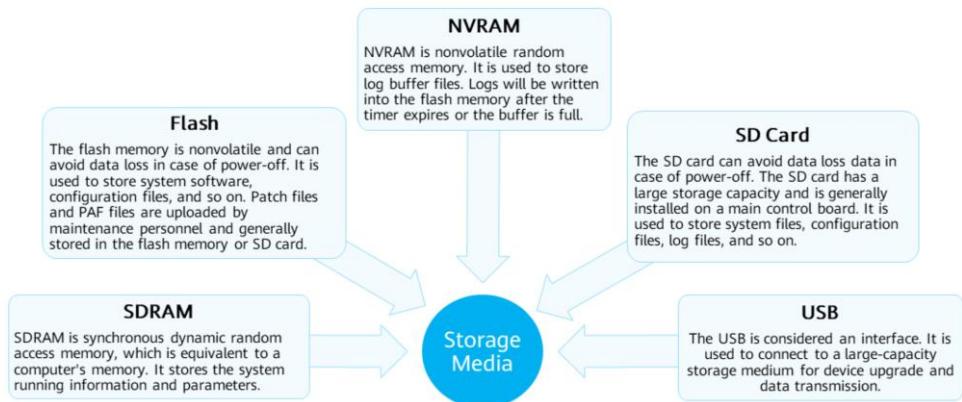
A PAF file effectively controls product features and resources. The common file name extension is .bin.

Common File Types

- A configuration file is a collection of command lines. Current configurations are stored in a configuration file so that the configurations are still effective after the device restarts. Users can view configurations in the configuration file and upload the configuration file to other devices to implement batch configuration.
- A patch is a kind of software compatible with the system software. It is used to fix bugs in system software. Patches can also fix system defects and optimize some functions to meet service requirements.
- To manage files on a device, log in to the device through either of the following modes:
 - Local login through the console port or Telnet.
 - Remote login through FTP, TFTP, or SFTP.

Storage Media

- Storage media include SDRAM, flash memory, NVRAM, SD card, and USB.



262 Huawei Confidential

HUAWEI

- Storage media include SDRAM, flash memory, NVRAM, SD card, and USB.
 - SDRAM stores the system running information and parameters. It is equivalent to a computer's memory.
 - NVRAM is nonvolatile. Writing logs to the flash memory consumes CPU resources and is time-consuming. Therefore, the buffer mechanism is used. Specifically, logs are first saved to the buffer after being generated, and then written to the flash memory after the timer expires or the buffer is full.
 - The flash memory and SD card are nonvolatile. Configuration files and system files are stored in the flash memory or SD card. For details, see the product documentation.
 - SD cards are external memory media used for memory expansion. The USB is considered an interface. It is used to connect to a large-capacity storage medium for device upgrade and data transmission.
 - Patch and PAF files are uploaded by maintenance personnel and can be stored in a specified directory.

Device Initialization Process

- After a device is powered on, it runs the Boot Read-Only Memory (BootROM) software to initialize the hardware and display hardware parameters. Then, it runs the system software and reads the configuration file from the default storage path to perform initialization.

```
BIOS Creation Date : Jan 5 2020, 18:00:24
DDR DRAM init : OK
Start Memory Test ? ('t' or 'T' is test):skip
Copying Data : Done
Uncompressing : Done
.....
Press Ctrl+B to break auto startup ... 1
Now boot from flash:/AC6508_V200R019C00SPC500.cc,
.....
```

- BootROM is a set of programs added to the ROM chip of a device. BootROM stores the device's most important input and output programs, system settings, startup self-check program, and system automatic startup program.
- The startup interface provides the information about the running program of the system, the running VRP version, and the loading path.

Device Management

- There are two commonly used device management modes: CLI and web system.
- To use a device management mode, you must first log in to a device through a login mode supported by this device management mode.

Web system

- The web system provides a graphical user interface (GUI) for easy device management and maintenance. This method, however, can be used to manage and maintain only some, not all, device functions.
- The web system supports the HTTP and HTTPS login modes.

CLI

- The CLI requires users to use commands provided by a device to manage and maintain the device. This mode implements refined device management but requires users to be familiar with the commands.
- The CLI supports the console port, Telnet, and SSH login modes.

VRP User Interfaces

- When a user logs in to a device through a CLI-supported mode, the system allocates a user interface to manage and monitor the current session between the user terminal and device.
- Such a user interface can be a console user interface or virtual type terminal (VTY) user interface.

Console user interface

- A console user interface is used to manage and monitor users who log in to a device through the console port.
- The serial port of a user terminal can be directly connected to the console port of a device for local access.

VTY user interface

- The VTY user interface is used to manage and monitor users who log in to a device by means of VTY.
- After a Telnet or STelnet connection is established between a user terminal and a device, a VTY channel is established to implement remote access to the device.

VRP User Levels

- VRP provides basic permission control functions. It defines the levels of commands that each level of users can execute to restrict the operations of users at different levels.

| User Level | Command Level | Name | Available Command |
|------------|----------------|---------------------|--|
| 0 | 0 | Visit level | Network diagnosis commands (such as ping and tracert), commands for accessing external devices from the local device (such as Telnet client commands), and some display commands |
| 1 | 0 and 1 | Monitoring level | System maintenance commands, including display commands |
| 2 | 0, 1, and 2 | Configuration level | Service configuration commands, including routing commands and IP configuration commands, to directly provide users with network services |
| 3-15 | 0, 1, 2, and 3 | Management level | Commands for controlling basic system operations and providing support for services, including the file system, FTP, TFTP download, user management, and command level commands, as well as debugging commands for fault diagnosis |

- To limit users' access permissions to a device, the device manages users by level and establishes a mapping between user levels and command levels. After a user logs in to a device, the user can use only commands of the corresponding levels or lower. By default, the user command level ranges from 0 to 3, and the user level ranges from 0 to 15. The mapping between user levels and command levels is shown in the table.

Login to the Web System

The web system for a Huawei AC is used as an example. Start a browser on a PC, enter <https://169.254.1.1> in the address bar, and press **Enter**. Then, the web system login page is displayed.

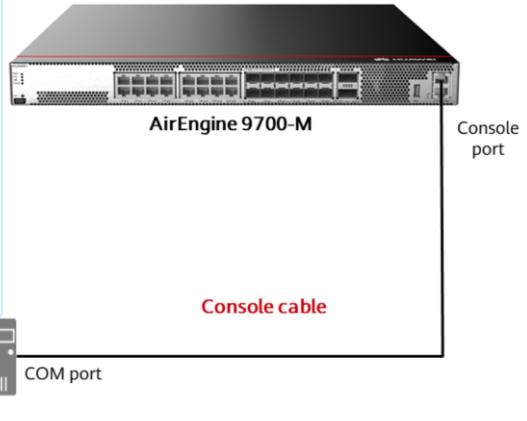


- Note: The login page, mode, and IP address may vary according to devices. For details, see the product documentation.

CLI - Local Login (1)

You can log in to a device in local or remote mode. Local login mode:

- Use this mode when you need to configure a device that is powered on for the first time. You can use the console port of the device for a local login.
- The console port is a serial port provided by the main control board of a device.
- To implement the login, directly connect your terminal's serial port to the device's console port, and use PuTTY to log in to the device. You can then configure the device after the login succeeds.

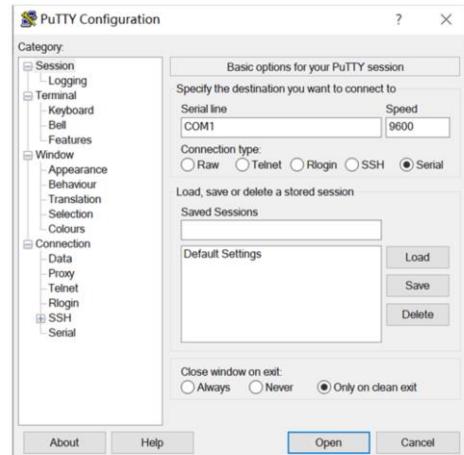


- Use a console cable to connect the console port of a device with the COM port of a computer. You can then use PuTTY on the computer to log in to the device and perform local commissioning and maintenance. A console port is an RJ45 port that complies with the RS232 serial port standard. At present, the COM ports provided by most desktop computers can be connected to console ports. In most cases, a laptop does not provide a COM port. Therefore, a USB-to-RS232 conversion port is required if you use a laptop.
- The console port login function is enabled by default and does not need to be pre-configured.

CLI - Local Login (2)

PutTY is a connection software for login through Telnet, SSH, serial interfaces, and so on.

In local login, the terminal is connected to the console port of the Huawei device through a serial port. Therefore, set **Connection type** to **Serial**. Set **Serial line** based on the actually used port on the terminal. Set **Speed** to **9600**.



 HUAWEI

- Many terminal simulators can initiate console connections. PuTTY is one of the options for connecting to VRP. If PuTTY is used for access to VRP, you must set port parameters. The figure in the slide shows examples of port parameter settings. If the parameter values were ever changed, you need to restore the default values.
- After the settings are complete, click Open. The connection with VRP is then set up.

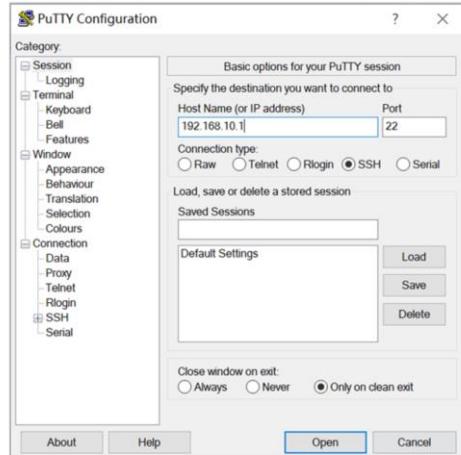
CLI - Remote Login

Remote login means that you log in to a device that can function as a remote login server, allowing you to centrally manage and maintain network devices. Remote login methods include Telnet and SSH.

- If you use the SSH login mode, set **Connection type** to **SSH**, enter the IP address of the remote login server, and use the default port number 22.
- If you use the Telnet login mode, set **Connection type** to **Telnet**, enter the IP address of the remote login server, and use the default port number 23.



270 Huawei Confidential

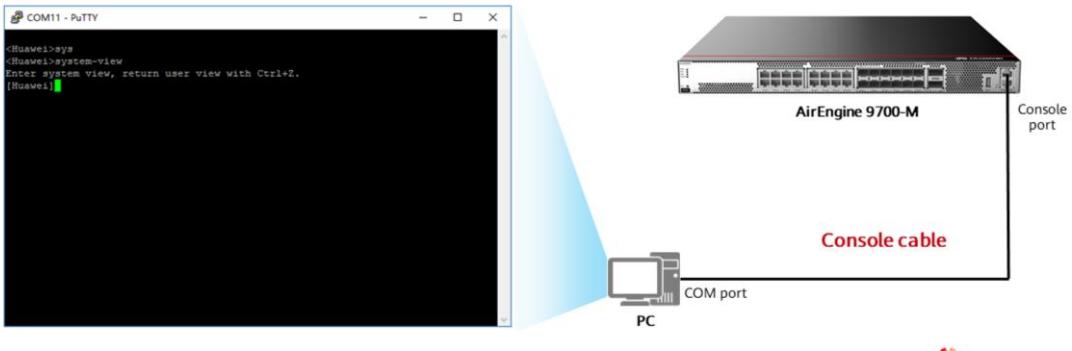


HUAWEI

- By default, the SSH login function is disabled on a device. You need to log in to the device through the console port and configure mandatory parameters for SSH login before using the SSH login function.

CLI

- After a login succeeds, the command line interface (CLI) is displayed.
- The CLI is a common tool for engineers to interact with network devices.



271 Huawei Confidential



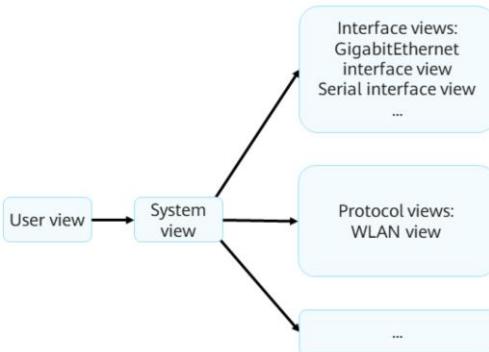
- The CLI is an interface through which users can interact with a device. When the command prompt is displayed after a user logs in to a device, it means that the user has entered the CLI successfully.

Contents

1. Huawei VRP Overview
2. **Command Line Basics**
 - CLI Overview
 - Basic Configuration Commands
 - Case Analysis
3. WLAN Device Upgrade
4. Fat AP Configuration

Command Views (1/2)

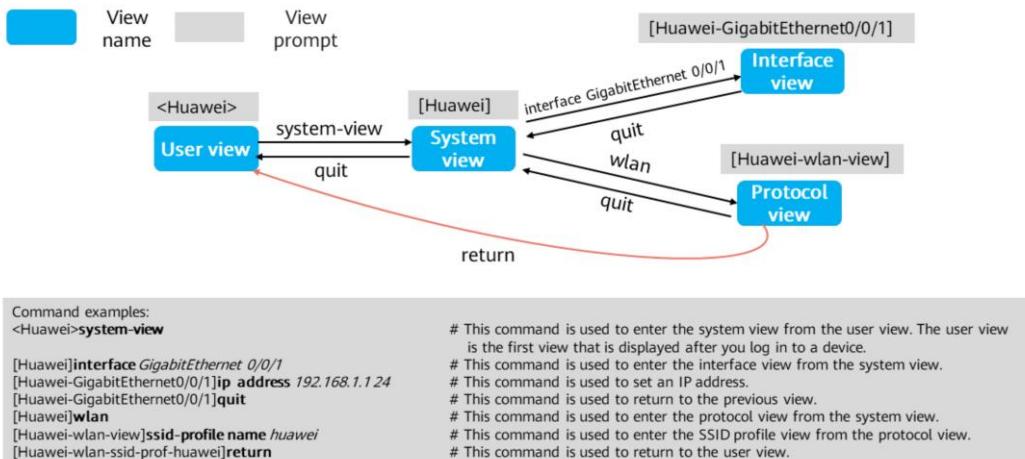
- A device provides various configuration and query commands. To facilitate the use of these commands, VRP registers the commands in different views according to their functions.



- User view: In this view, you can check the running status and statistics of a device.
- System view: In this view, you can set system parameters and enter the configuration views of other commands.
- Other views: In other views, such as the interface view and protocol view, you can set interface parameters and protocol parameters.

- The user view is the first view displayed after you log in to a device. Only query and tool commands are provided in the user view.
- In the user view, only the system view can be accessed. Global configuration commands are provided in the system view. If the system has a lower-level configuration view, the command for entering the lower-level configuration view is provided in the system view.

Command Views (2/2)



- After you log in to the system, the user view is displayed first. This view provides only display commands and tool commands, such as ping and telnet. It does not provide any configuration commands.
- You can run the system-view command in the user view to enter the system view. The system view provides some simple global configuration commands.
- In a complex configuration scenario, for example, multiple parameters need to be configured for an Ethernet interface, you can run the interface GigabitEthernet X command (X indicates the number of the interface) to enter the GE interface view. Configurations performed in this view take effect only on the specified GE interface.

Editing a Command (1/1)

- Command editing through function keys
 - Backspace: deletes the character before the cursor and moves the cursor to the left. When the cursor reaches the beginning of the command, an alarm is generated.
 - Left cursor key ← or Ctrl+B: moves the cursor one character to the left. When the cursor reaches the beginning of the command, an alarm is generated.
 - Right cursor key → or Ctrl+F: moves the cursor one character to the right. When the cursor reaches the end of the command, an alarm is generated.
- Incomplete keyword input
 - A device allows the input of incomplete keywords. Specifically, if an entered character string can match a unique keyword, you do not need to enter the remaining characters of the keyword.

```
<Huawei>d cu
<Huawei>di cu
<Huawei>dis cu
<Huawei>d c
^
Error:Ambiguous command found at '^' position.
<Huawei>dis c
^
Error:Ambiguous command found at '^' position.
```

For example, the **display current-configuration** command is identified when you enter **d cu**, **di cu**, or **dis cu**. However, the command cannot be identified if you enter **d c** or **dis c** because the character string **d c** or **dis c** matches more than one command.

- Note: "keyword" mentioned in this section means any character string except a parameter value string in a command. The meaning is different from that of "keyword" in the command format.

Editing a Command (1/2)

- Command editing through the Tab key

- If an entered character string matches a unique keyword, the system automatically supplements the keyword after you press Tab. If the keyword is complete, it remains unchanged even if you press Tab repeatedly.

```
[Huawei] info-          #Press Tab.  
[Huawei] info-center
```

- If an entered character string matches more than one keyword, you can press Tab repeatedly. The system will then circularly display the keywords beginning with the entered character string to help you find the desired keyword.

```
[Huawei] info-center log      #Press Tab.  
[Huawei] info-center logbuffer #Press Tab repeatedly to circularly display all matched keywords.  
[Huawei] info-center logfile  
[Huawei] info-center loghost
```

- If an entered character string cannot identify any keyword, the entered string remains unchanged after you press Tab.

```
[Huawei] info-center loglog    #Enter an incorrect keyword and press Tab.  
[Huawei] info-center loglog
```

Using Command Line Online Help

- You can use command line online help to obtain real-time help without memorizing a large number of complex commands.
- The online help can be classified into full help and partial help. To obtain the online help, enter a question mark (?) when using a command.

Full Help

- To obtain full help, press ? after a view displayed. The system will then display all commands in the view and their descriptions.

```
<Huawei> ?
```

User view commands:

| | |
|----------|--------------------------------|
| arp-ping | ARP-ping |
| autosave | <Group> autosave command group |
| backup | Backup information |
| cd | Change current directory |
| clear | Clear |
| clock | Specify the system clock |
| ... | |

Partial Help

- To obtain partial help, press ? after you enter the start character or character string of a command. The system will then display all the commands that start with this character or character string.

```
<Huawei> d?
```

| | |
|-----------|---------------------------------|
| debugging | <Group> debugging command group |
| delete | Delete a file |
| dialer | Dialer |
| dir | List files on a filesystem |
| display | Display information |

- The command help information displayed in this slide is for reference only, which varies according to devices.

Interpreting Command Line Error Messages

- If a command passes the syntax check, the system executes it. Otherwise, the system reports an error message.

```
[Huawei] sysname ^  
Error:Incomplete command found at '^' position. #A supplement needs to be made at the position pointed by the arrow.  
[Huawei] router if 1.1.1.1 ^  
Error: Unrecognized command found at '^' position. #An identification failure occurs at the position pointed by the arrow. Check whether the command is correct.  
[Huawei] a ^  
Error: Ambiguous command found at '^' position. #More than one command matches the keyword at the position pointed by the arrow. In this example, it indicates that there are multiple keywords starting with a.  
[Huawei-GigabitEthernet0/0/0]ospf cost 800000 ^  
Error: Wrong parameter found at '^' position. #The parameter value at the position pointed by the arrow is invalid.
```

Using Undo Command Lines

- If a command begins with the keyword undo, it is an undo command. An undo command is generally used to restore a default configuration, disable a function, or delete a configuration. For example:

- Run an undo command to restore a default configuration.

```
<Huawei> system-view  
[Huawei] sysname Server  
[Server] undo sysname  
[Huawei]
```

- Run an undo command disable a function.

```
<Huawei> system-view  
[Huawei] ftp server enable  
[Huawei] undo ftp server
```

- Run an undo command to delete a configuration.

```
[Huawei]interface g0/0/1  
[Huawei-GigabitEthernet0/0/1]ip address 192.168.1.1 24  
[Huawei-GigabitEthernet0/0/1]undo ip address
```

Using Command Line Shortcut Keys

- A device provides command shortcut keys to speed up and simplify command input.
- Command shortcut keys are classified into user-defined shortcut keys and system shortcut keys.

User-defined Shortcut Keys

- There are four user-defined shortcut keys: **Ctrl+G**, **Ctrl+L**, **Ctrl+O**, and **Ctrl+U**.
- You can associate a user-defined shortcut key with any command. After you press a shortcut key, the system will automatically run the command associated with the shortcut key.

```
<Huawei> system-view  
[Huawei] hotkey ctrl_l "display tcp status"
```

System Shortcut Keys

- **CTRL_A**: moves the cursor to the beginning of the current line.
- **CTRL_B**: moves the cursor one character to the left.
- **CTRL_C**: stops the running of the current command.
- **CTRL_E**: moves the cursor to the end of the current line.
- **CTRL_X**: deletes all characters on the left of the cursor.
- **CTRL_Y**: deletes the character at the cursor and all characters on the right of the cursor.
- **CTRL_Z**: returns to the user view.
- **CTRL_I**: terminates the current connection or switches to another connection.

Contents

1. Huawei VRP Overview
2. **Command Line Basics**
 - CLI Overview
 - Basic Configuration Commands
 - Case Analysis
3. WLAN Device Upgrade
4. Fat AP Configuration

Common File System Operation Commands (1/3)

- Check the current directory.
`<Huawei>pwd`
- Display information about files in the current directory.
`<Huawei>dir`
- Display the content of a text file.
`<Huawei>more`
- Change the current working directory.
`<Huawei>cd`
- Create a directory.
`<Huawei>mkdir`

- VRP uses the file system to manage files and directories on a device. To manage files and directories, you often need to run basic commands to query file or directory information. Such commonly used basic commands include `pwd`, `dir [/all] [filename | directory]`, and `more [/binary] filename [offset] [all]`.
- The `pwd` command displays the current working directory.
- The `dir [/all] [filename | directory]` command displays information about files in the current directory.
- The `more [/binary] filename [offset] [all]` command displays the content of a text file.
- In this example, the `dir` command is run in the user view to display information about files in the flash memory.
- Common commands for operating directories include `cd` directory, `mkdir` directory, and `rmdir` directory.
- The `cd` directory command changes the current working directory.
- The `mkdir` directory command creates a directory. A directory name can contain 1 to 64 characters.

Common File System Operation Commands (2/3)

- Delete a directory.

```
<Huawei>rmdir
```

- Copy a file.

```
<Huawei>copy
```

- Move a file.

```
<Huawei>move
```

- Rename a file.

```
<Huawei>rename
```

- Delete a file.

```
<Huawei>delete
```

- The rmdir directory command deletes a directory from the file system. A directory to be deleted must be empty; otherwise, it cannot be deleted using this command.
- The copy source-filename destination-filename command copies a file. If the target file already exists, the system displays a message indicating that the target file will be replaced. The target file name cannot be the same as the system startup file name. Otherwise, the system displays an error message.
- The move source-filename destination-filename command moves a file to another directory. The move command can be used to move files only within the same storage medium.
- The rename old-name new-name command renames a directory or file.
- The delete [/unreserved] [/force] { filename | devicename } command deletes a file. If the unreserved parameter is not specified, the deleted file is moved to the recycle bin. A file in the recycle bin can be restored using the undelete command. However, if the /unreserved parameter is specified, the file is permanently deleted and cannot be restored any more. If the /force parameter is not specified in the delete command, the system displays a message asking you whether to delete the file. However, if the /force parameter is specified, the system does not display the message. filename specifies the name of the file to be deleted, and devicename specifies the name of the storage medium.

Common File System Operation Commands (3/3)

- Restore a deleted file.
`<Huawei>undelete`
- Permanently delete a file in the recycle bin.
`<Huawei>reset recycle-bin`

- The reset recycle-bin [filename | devicename] command permanently deletes all or a specified file in the recycle bin. filename specifies the name of the file to be permanently deleted, and devicename specifies the name of the storage medium.

Basic Configuration Commands (1/4)

- Configure a system name.
`[Huawei] sysname name`

- Configure a system clock.
 - This command configures a local time zone.
`<Huawei> clock timezone time-zone-name { add | minus } offset`
 - This command configures the current or UTC date and time.
`<Huawei> clock datetime [utc] HH:MM:SS YYYY-MM-DD`
 - This command configures the daylight saving time.
`<Huawei> clock daylight-saving-time`

- Generally, more than one device is deployed on a network, and the administrator needs to manage all devices in a unified manner. The first task of device commissioning is to set a system name. A system name uniquely identifies a device. The default system name of an AR series router is Huawei, and that of an S series switch is HUAWEI. A system name takes effect immediately after being set.
- To ensure successful coordination with other devices, you need to correctly set the system clock. System clock = Coordinated Universal Time (UTC) ± Time difference between the UTC and the time of the local time zone. Generally, a device has default UTC and time difference settings.
 - You can run the `clock datetime` command to set the system clock of the device. The date and time format is `HH:MM:SS YYYY-MM-DD`. If this command is run, the UTC is the system time minus the time difference.
 - You can also change the UTC and the system time zone to change the system clock.
 - The `clock datetime utc HH:MM:SS YYYY-MM-DD` changes the UTC.
 - The `clock timezone time-zone-name { add | minus } offset` command configures the local time zone. The UTC is the local time plus or minus the offset.
 - If a region adopts the daylight saving time, the system time is adjusted according to the user setting at the moment when the daylight saving time starts. VRP supports the daylight saving time function.

Basic Configuration Commands (2/4)

- Configure a command level.

```
[Huawei] command-privilege level level view view-name command-key
```

- This command configures a level for commands in a specified view. Command levels are classified into visit, monitoring, configuration, and management, which are identified by the numbers 0, 1, 2, and 3, respectively.

- Configure the password-based login mode.

```
[Huawei] user-interface vty 0 4
```

```
[Huawei-ui-vty0-4] set authentication password cipher information
```

- This user-interface vty command displays the virtual type terminal (VTY) user interface view, and the set authentication password command configures the password authentication mode. The system supports the console user interface and VTY user interface. The console user interface is used for local login, and the VTY user interface is used for remote login. By default, a device supports a maximum of 15 concurrent VTY-based user accesses.

- Configure user interface parameters.

```
[Huawei] idle-timeout minutes [ seconds ]
```

- This command sets a timeout period to disconnect from the user interface. If no command is entered within the specified period, the system tears down the current connection. The default timeout period is 10 minutes.

- Each type of user interface has a corresponding user interface view. A user interface view is a command line view provided by the system for you to configure and manage all physical and logical interfaces working in asynchronous interaction mode, implementing unified management of different user interfaces. Before accessing a device, you need to set user interface parameters. The system supports console and VTY user interfaces. The console port is a serial port provided by the main control board of a device. A VTY is a virtual line port. A VTY connection is set up after a Telnet or SSH connection is established between a user terminal and a device, allowing the user to access the device in VTY mode. Generally, a maximum of 15 users can log in to a device through VTY at the same time. You can run the user-interface maximum-vty number command to set the maximum number of users that can concurrently access a device in VTY mode. If the maximum number of login users is set to 0, no user can log in to the device through Telnet or SSH. The display user-interface command displays information about a user interface.
- The maximum number of VTY interfaces may vary according to the device type and used VRP version.

Basic Configuration Commands (3/4)

- Configure an IP address for an interface.

```
[Huawei] interface interface-number  
[Huawei-interface-number]ip address ip address
```

▫ This command configures an IP address for a physical or logical interface on a device.

- Display currently effective configurations.

```
<Huawei> display current-configuration
```

- Save a configuration file.

```
<Huawei> save
```

- Check saved configurations.

```
<Huawei> display saved-configuration
```

- To run the IP service on an interface, you must configure an IP address for the interface. Generally, an interface requires only one IP address. For the same interface, a newly configured primary IP address replaces the original primary IP address.
- You can run the `ip address { mask | mask-length }` command to configure an IP address for an interface. In this command, `mask` indicates a 32-bit subnet mask, for example, `255.255.255.0`; `mask-length` indicates a mask length, for example, `24`. Specify either of them when configuring an IP address.
- A loopback interface is a logical interface that can be used to simulate a network or an IP host. The loopback interface is stable and reliable, and can also be used as the management interface if multiple protocols are deployed.
- When configuring an IP address for a physical interface, check the physical status of the interface. By default, interfaces are up on Huawei routers and switches. If an interface is manually disabled, run the `undo shutdown` command to enable the interface after configuring an IP address for it.

Basic Configuration Commands (4/4)

- Clear saved configurations.

```
<Huawei> reset saved-configuration
```

- Check system startup configuration parameters.

```
<Huawei> display startup
```

▫ This command displays the system software for the current and next startup, backup system software, configuration file, license file, and patch file, as well as voice file.

- Configure the configuration file for next startup.

```
<Huawei> startup saved-configuration configuration-file
```

▫ During a device upgrade, you can run this command to configure the device to load the specified configuration file for the next startup.

- Restart a device.

```
<Huawei> reboot
```

- The reset saved-configuration command deletes the configurations saved in a configuration file or the configuration file. After this command is run, if you do not run the startup saved-configuration command to specify the configuration file for the next startup or the save command to save current configurations, the device uses the default parameter settings during system initialization when it restarts.
- The display startup command displays the system software for the current and next startup, backup system software, configuration file, license file, and patch file, as well as voice file.
- The startup saved-configuration configuration-file command configures the configuration file for the next startup. The configuration-file parameter specifies the name of the configuration file for the next startup.
- The reboot command restarts a device. Before the device reboots, you are prompted to save configurations.

Contents

1. Huawei VRP Overview
2. **Command Line Basics**
 - CLI Overview
 - Basic Configuration Commands
 - Case Analysis
3. WLAN Device Upgrade
4. Fat AP Configuration

VRP Basic Configuration Commands

- As shown in the figure, an engineer needs to configure an AC. The requirements are as follows:
 - Connect the AC and PC. Assign the IP addresses shown in the figure to the AC and PC.
 - Allow other employees of the company to use the password huawei123 to remotely log in to the AC through the PC. Allow them to view configurations but disable them from modifying configurations.
 - Save current configurations and name the configuration file huawei.zip. Configure this file as the configuration file for the next startup.



Configuration Procedure (1/1)



Configure an interface IP address

```
<Huawei>system-view  
[Huawei]sysname AC  
[AC]interface Vlanif 1  
[AC-Vlanif1]ip address 192.168.1.1 24  
[AC-Vlanif1]quit
```

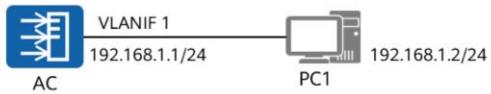
Configure a user level and a user authentication mode

```
[AC]user-interface vty 0 4  
[Huawei-ui-vty0-4]authentication-mode password cipher  
New Password: huawei123  
[AC-ui-vty0-4]user privilege level 1  
[AC-ui-vty0-4]quit
```

The password configuration command may vary according to devices. For details, see the product documentation.

- For some devices, after the authentication-mode password command is entered, the password setting page will be displayed automatically. You can then enter the password at the page that is displayed. For some devices, you need to run the set authentication-mode password command to set a password.

Configuration Procedure (1/2)



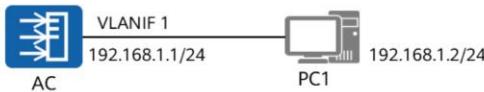
Specify the configuration file for next startup

```
<AC>save huawei.zip
Are you sure to save the configuration to huawei.zip? (y/n)[n]y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
<AC>startup saved-configuration huawei.zip
```

By default, configurations are saved in the **vrpcfg.cfg** file. You can also create a file for saving the configurations.

- To save configurations, run the `save` command. By default, configurations are saved in the `vrpcfg.cfg` file. You can also create a file for saving the configurations. In VRPv5, the configuration file is stored in the `flash:` directory by default.

Checking the Configuration



```
<AC>display startup
MainBoard:
  Startup system software:          null
  Next startup system software:     null
  Backup system software for next startup: null
  Startup saved-configuration file: flash:/vrpcfg.zip
  Next startup saved-configuration file: flash:/huawei.zip
  Startup license file:             null
  Next startup license file:        null
  Startup patch package:           null
  Next startup patch package:      null
  Startup voice-files:              null
  Next startup voice-files:         null
```

- The display startup command displays the system software for the current and next startup, backup system software, configuration file, license file, and patch file, as well as voice file.
 - Startup system software indicates the VRP file used for the current startup.
 - Next startup system software indicates the VRP file to be used for the next startup.
 - Startup saved-configuration file indicates the configuration file used for the current system startup.
 - Next startup saved-configuration file indicates the configuration file to be used for the next startup.
 - When a device starts, it loads the configuration file from the storage medium and initializes the configuration file. If no configuration file exists in the storage medium, the device uses the default parameter settings for initialization.
- The startup saved-configuration [configuration-file] command sets the configuration file for the next startup, where the configuration-file parameter specifies the name of the configuration file.

Contents

1. Huawei VRP Overview
2. Command Line Basics
- 3. WLAN Device Upgrade**
 - AC Upgrade
 - AP Upgrade
4. Fat AP Configuration

Why Is Device Upgrade Required?

- For a running network system, any operation that affects the running of services on the live network, such as hardware replacement, version upgrade, and configuration change, is called migration. Version upgrade is the most common task.
- Version upgrade brings the following benefits.



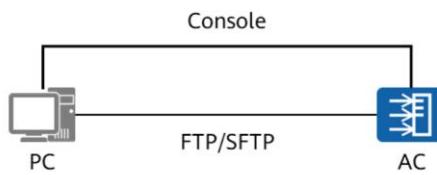
Fix system vulnerabilities

Optimize system resources

Add new functions

- Fix system vulnerabilities: Enhance system stability and security, and improve the resistance to viruses and Trojan horses.
- Optimize system resources: The hardware performance of the device can be fully used to improve the system smoothness.
- Add new functions: Provide customers with required product features to improve user experience.

AC Upgrade



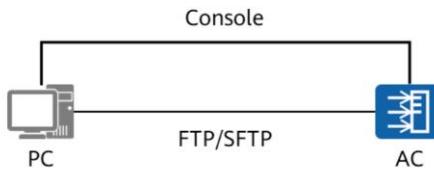
- Download the system software to be upgraded to the local PC.
- Download the system software to the AC through FTP or SFTP.
- Load the system software for the next startup.
- Restart the device.

Preparing for an Upgrade

Checking the system software version

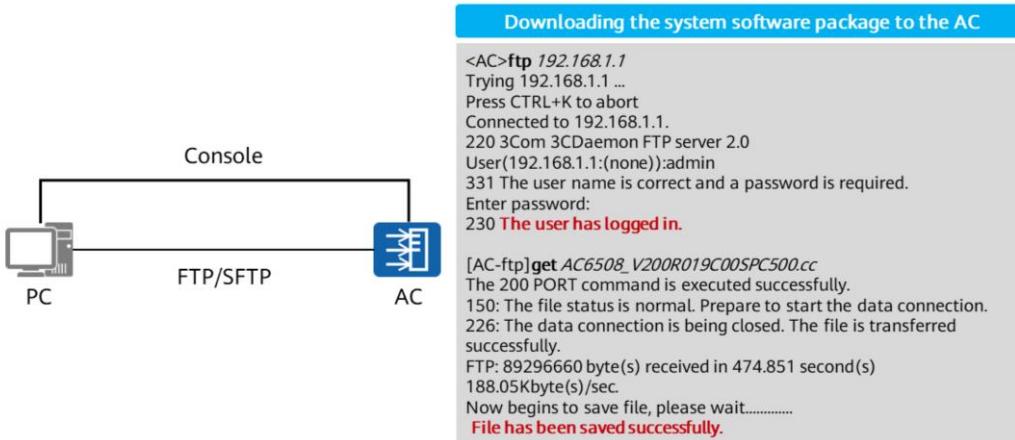
```
<AC>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (AC6508V200R007C10SPC100)
Copyright (C) 2011-2016 HUAWEI TECH CO., LTD
Huawei AC6508-8-PWR Router uptime is 0 week, 0 day, 0 hour, 17
minutes

MPU 0(Master) : uptime is 0 week, 0 day, 0 hour, 17 minutes
SDRAM Memory Size : 2048 M bytes
Flash Memory Size : 16 M bytes
SD Card Memory Size : 1838 M bytes
MPU version information:
1. PCB Version : H85D2H08M100 VER.A
2. MAB Version : 0
3. Board Type : AC6508-8-PWR
4. CPLD0 Version : 0
5. BootROM Version : 418
```



- You can download the required system software from Huawei official website.

Downloading the System Software

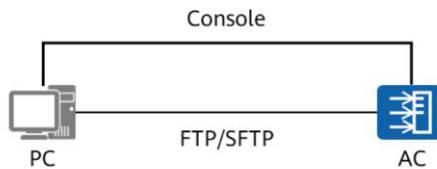


298 Huawei Confidential

 HUAWEI

- Before using FTP to download files, ensure that the AC can communicate with the FTP server and set up an FTP connection.

Loading the System Software

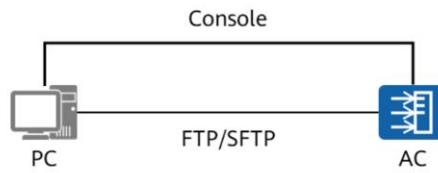


Specifying the system software for next startup

```
<AC>startup system-software AC6508_V200R019C00SPC500.cc
Info: Verifying the file, please wait...

<AC>display startup
Configured startup system software:          sdcard:/AC6508V200R007C10SPC100.cc
Startup system software:                      sdcard:/AC6508V200R007C10SPC100.cc
Next startup system software:               sdcard:/AC6508_V200R019C00SPC500.cc
Startup saved-configuration file:             sdcard:/vrpcfg.zip
Next startup saved-configuration file:        sdcard:/vrpcfg.zip
Startup patch package:                       NULL
Next startup patch package:                  sdcard:/AC6508V200R005C10SPH301.pat
```

Restarting the AC



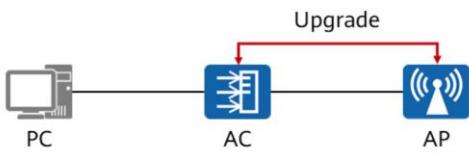
Restarting the AC

```
<AC>reboot fast
Warning: System will reboot! Continue ? [y/n]:y
Warning: do not power-off!
Info: system is sync data now ,please wait...
Info: system is rebooting ,please wait...
```

Contents

1. Huawei VRP Overview
2. Command Line Basics
- 3. WLAN Device Upgrade**
 - AC Upgrade
 - AP Upgrade
4. Fat AP Configuration

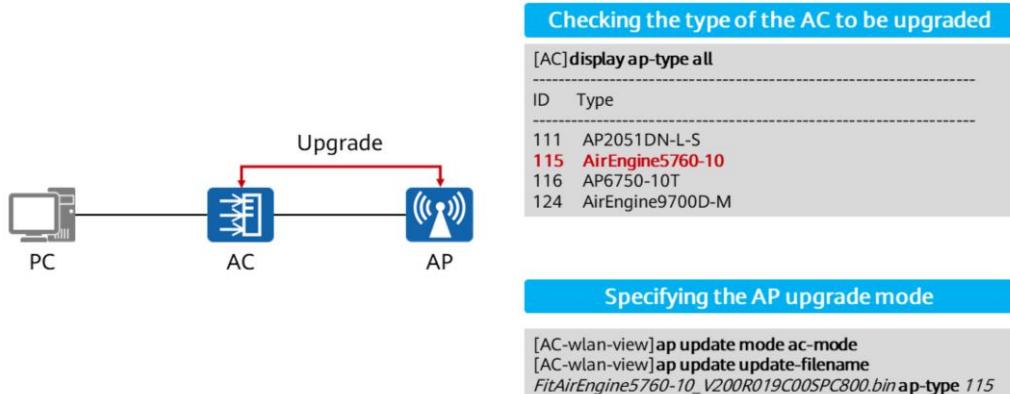
AP Upgrade



- Download the system software to be upgraded to the local PC.
- Download the system software to the AC through FTP or SFTP.
- Set the AP upgrade mode to AC mode.
- Configure the AP upgrade version file name and AP type.

- To upgrade the functions or versions of an existing WLAN, perform an in-service upgrade for APs or load patches on the WLAN.
- In an in-service upgrade, an AP is in normal or ver-mismatch state. If the AP finds that its version is different from the version of the AP upgrade file specified on the AC, the AP starts to upgrade its version.
- In an in-service upgrade, APs support several upgrade modes, including single AP upgrade, AP type-based upgrade, and AP group-based upgrade.
 - Upgrade of a single AP: allows you to upgrade a single AP to check whether the upgrade version can function properly. If the upgrade is successful, upgrade other APs in batches.
 - AP type-based upgrade: allows you to upgrade APs of the same type.
 - AP group-based upgrade: allows you to upgrade APs in the same AP group.
- Similar to the in-service upgrade, in-service patch loading allows you to load the patch for a single AP, APs of a specified type, or APs in a specified AP group.
- Three AP upgrade modes are supported. Run the following commands as required.
 - Run the `ap-update mode ac-mode` command to set AP upgrade to AC mode. By default, the AC mode is used.
 - Run the `ap update mode ftp-mode` command to set AP upgrade to FTP mode.
 - Run the `ap update mode sftp-mode` command to set AP upgrade to SFTP mode.

AP Upgrade in AC Mode



303 Huawei Confidential



- Before upgrading an AP through an AC, ensure that the AP can go online on the AC and the AP upgrade file is saved in the root directory of the AC.

Checking AP Online Information

- Run the “display ap all” command to check AP online information.

```
<AC6508>display ap all
Total AP information:
dload: download      [1]
ExtraInfo : Extra information
P   : insufficient power supply
```

| ID | MAC | Name | Group | IP | Type | State | STA | Uptime | ExtraInfo |
|----|----------------|------|---------|-------------|------------------|-------|-----|--------|-----------|
| 0 | b4fb-f9b7-de40 | AP1 | default | 10.1.10.231 | AirEngine5760-10 | dload | 0 | - | - |

Total: 1

Checking the AP Upgrade Status

- Run the “**display ap update status all**” command to check the AP upgrade status.

```
<AC6508>display ap update status all
FT : File Type
-----
ID  Name AP Type AP Group AP MAC      FT      Update Version  Last Update Time    Update Status
-----
0   AP1  AP4050DN default  b4fb-f9b7-de40 FIT    V200R019C00SPC800 2020-05-29/09:53:09  downloading(progress: 100%/47%)
-----
Total: 1
```

Checking the AP Online Status

- Wait for a period of time and query the AP online status again.

```
<AC6508>display ap all
Total AP information:
dload: download [1]
ExtraInfo : Extra information
P   : insufficient power supply
-----
ID      MAC        Name Group    IP          Type           State STA Uptime ExtraInfo
----- 
0      b4fb-f9b7-de40  AP1  default  10.1.10.231 AirEngine5760-10 nor 0 - 
-----
Total: 1
```

Restarting APs

- Restart an AP.

```
[AC6508-wlan-view]ap-reset ap-id 0
```

- Restart APs of the same type.

```
[AC6508-wlan-view]ap-reset ap-type type-id 75
```

- Restart a group of APs.

```
[AC6508-wlan-view]ap-reset ap-group default
```

- Restart all APs.

```
[AC6508-wlan-view]ap-reset all
```

- If the AP is in vmiss state and cannot be upgraded for a long time, you can run the restart command to restart the AP.

Contents

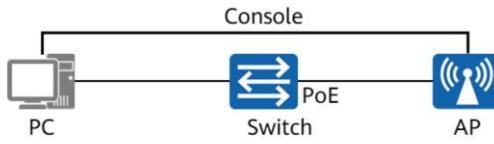
1. Huawei VRP Overview
2. Command Line Basics
3. WLAN Device Upgrade
- 4. Fat AP Configuration**

Huawei AP Working Modes - Fit AP and Fat AP

- Huawei APs can work as Fat or Fit APs and switch flexibly between the two working modes based on the network plan.
- When the wireless network scale is small, customers need to purchase only APs and configure the APs to work as Fat APs. As the network scale expands, tens of or hundreds of APs exist on the network. To simplify network management, customers are advised to purchase ACs to perform centralized management on the APs and set the APs to work as Fit APs.



Procedure for Switching the Working Mode of an AP



- Prepare the environment.
- Check AP information.
- Switch the working mode of the AP.
- Verify the switching.

- 1. Prepare the environment: Configure the IP address and FTP server software on the PC. Download the Fat AP software package of the target version to the FTP server. Check network connectivity and the indicator states of the AP.
- 2. Check AP information: On the PC, log in to the AP through the console port to check the version and working mode of the AP.
- 3. Start switching: Run the `ap-mode-switch fat ftp filename server-ip-address user-name password [port]` command in the system view. Then restart the AP.
- 4. Verify the switching: Log in to the AP again and check the working mode of the AP.

Switching the Working Mode of an AP

- After all preparations are complete, run the ap-mode-switch fat command to switch the working mode of the AP.

```
[Huawei]ap-mode-switch fat ftp Fat&CloudAirEngine5760-10_V200R019C00SPC800.bin 169.254.1.100 admin huawei
Warning: The system will reboot and start in fat mode of V200R019C00SPC800. Continue? (y/n)[n]:y
Warning: Do Not Power-off!
```

```
.....
Info: system is rebooting ,please wait...
```

- The default IP address of the AP is 169.254.1.1/24, the user name is admin, and the password is admin@Huawei.com.

Verify the Switching

- After the upgrade is complete, the AP automatically restarts. After the AP restarts, run the “display version” command to check whether the upgrade is successful.

```
<Huawei>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AirEngine5760-10 FAT V200R019C00SPC800)
Copyright (C) 2011-2020 HUAWEI TECH CO., LTD
Huawei AP4050DN Router uptime is 0 week, 0 day, 0 hour, 0 minute

MPU 0(Master) : uptime is 0 week, 0 day, 0 hour, 0 minute
SDRAM Memory Size   : 256   M bytes
NOR FLASH Memory Size: 64    M bytes
MPU version information:
1. PCB    Version : H84D2TD1D505 VER.A
2. MAB    Version : 0
3. Board   Type   : AP4050DN
4. CPLD0  Version : 0
5. BootROM Version : 627
```

Fat AP Configuration (1/2)

- Configure a country code.
[AP] **wlan**
[AP-wlan-view]
[AP-wlan-view] country-code country-code
- Create a VAP profile or enter an existing VAP profile view.
[AP-wlan-view] **vap-profile name** *profile-name*
[AP-wlan-vap-prof-profile-name]
- Configure a service VLAN for a VAP.
[AP-wlan-vap-prof-profile-name] **service-vlan vlan-id** *vlan-id*
- Configure the security profile.
[AP-wlan-view] **security-profile name** *profile-name*
[AP-wlan-sec-prof-profile-name]
- Bind the security profile to the VAP profile.
[AP-wlan-view] **vap-profile name** *profile-name*
[AP-wlan-vap-prof-profile-name] **security-profile** *profile-name*

- Command: **country-code 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
 - ...

Fat AP Configuration (2/2)

- Configure an SSID profile.

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

- An SSID profile is created and the SSID profile view is displayed, or the view of an existing SSID profile is displayed.
- By default, the system provides the SSID profile default.

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

- An SSID is configured for the SSID profile.

- Bind the SSID profile to the VAP profile.

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

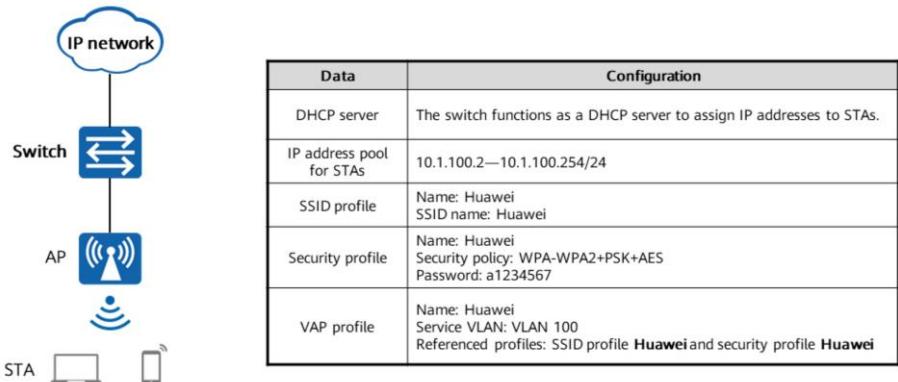
- Bind the specified VAP profile to radios on a radio interface.

```
[AP] interface Wlan-Radio 0/0/0  
[AP-Wlan-Radio0/0/0] vap-profile profile-name wlan wlan-id
```

- Command: `ssid ssid`

- `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.

Case: Layer 2 Networking of a Fat AP

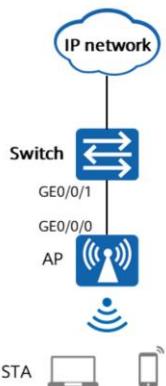


315 Huawei Confidential

 HUAWEI

- Service Requirements
 - An enterprise wants to enable users to access the Internet through a WLAN, meeting the basic mobile office requirements.
- Networking Requirements
 - DHCP deployment mode:
 - Configure the switch as a DHCP server to allocate IP addresses to STAs.
- Configuration roadmap:
 - Configure network connectivity between the AP and other network devices.
 - Configure WLAN service parameters for STAs to access the WLAN.

Configuring Network Connectivity



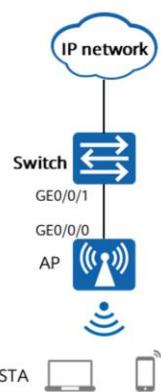
- Create VLANs and interfaces on the switch and AP.
- Configure the DHCP server to allocate IP addresses to STAs.

Configure VLANIF 100 on the switch to allocate an IP address to the AP.

```
[SW]dhcp enable  
[SW]interface vlanif 100  
[SW-Vlanif100]ip address 10.1.100.1 24  
[SW-Vlanif100]dhcp select interface  
[SW-Vlanif100]quit
```

- 1. Create VLANs and interfaces on S1, S2, and AC.
 - Switch configuration:
 - [SW]vlan batch 100
 - [SW] interface GigabitEthernet 0/0/1
 - [SW-GigabitEthernet0/0/1]port link-type trunk
 - [SW-GigabitEthernet0/0/1]port trunk pvid vlan 100
 - [SW-GigabitEthernet0/0/1]port trunk allow-pass vlan 100
 - [SW-GigabitEthernet0/0/1]quit
 - AP configuration:
 - [AP]interface GigabitEthernet 0/0/0
 - [AP-GigabitEthernet0/0/0]port link-type trunk
 - [AP-GigabitEthernet0/0/0]port trunk pvid vlan 100
 - [AP-GigabitEthernet0/0/0]port trunk allow-pass vlan 100
 - [AP-GigabitEthernet0/0/0]quit

Configuring WLAN Service Parameters (1/1)



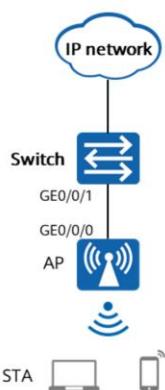
- Create a security profile named **Huawei** and configure a security policy.

```
[AP-wlan-view]security-profile name Huawei  
[AP-wlan-sec-prof-Huawei]security wpa-wpa2 psk pass-phrase  
a1234567aes  
[AP-wlan-sec-prof-Huawei]quit
```

- Create an SSID profile named **Huawei** and set the SSID name to **Huawei**.

```
[AP]wlan  
[AP-wlan-view]ssid-profile name Huawei  
[AP-wlan-ssid-prof-Huawei]ssid Huawei  
[AP-wlan-ssid-prof-Huawei]quit
```

Configuring WLAN Service Parameters (1/2)



- Create a VAP profile named **Huawei**, set the service VLAN, and apply the security profile and SSID profile to the VAP profile.

```
[AP-wlan-view]vap-profile name Huawei  
[AP-wlan-vap-prof-Huawei]ssid-profile Huawei  
[AP-wlan-vap-prof-Huawei]security-profile Huawei  
[AP-wlan-vap-prof-Huawei]service-vlan vlan-id 100  
[AP-wlan-vap-prof-Huawei]quit
```

- Enter the AP radio interface view and bind the VAP profile **Huawei** to the radio interface.

```
[AP]interface Wlan-Radio 0/0/0  
[AP-Wlan-Radio0/0/0]vap-profile Huawei/wlan 2  
[AP-Wlan-Radio0/0/0]quit  
[AP]interface Wlan-Radio 0/0/1  
[AP-Wlan-Radio0/0/1]vap-profile Huawei/wlan 2  
[AP-Wlan-Radio0/0/1]quit
```

Checking STA Connection Information

- Connect STAs to the WLAN with SSID Huawei and enter the password a1234567. Run the display station all command on the AP. The command output shows that the STAs are connected to the WLAN Huawei.

```
[AP]display station all
```

Rf/WLAN: Radio ID/WLAN ID

Rx/Tx: link receive rate/link transmit rate(Mbps)

| STA MAC | Ap name | Rf/WLAN | Band | Type | Rx/Tx | RSSI | VLAN | IP address | SSID |
|------------------------|----------------|---------|------|------|---------|------|------|----------------|--------|
| 3853-9c76-9fc4 | b4fb-f9b7-de40 | 1/2 | 5G | 11ac | 156/115 | -39 | 10 | 192.168.10.251 | Huawei |
| Total: 1 2.4G: 0 5G: 1 | | | | | | | | | |

Quiz

1. (Multiple-Answer Question) Which of the following are reasons for device software upgrade?
 - A. Fixing system vulnerabilities
 - B. Optimizing system resources
 - C. Adding new functions
 - D. Enhancing forwarding performance

- 1. ABC

Summary

- VRP is a Huawei proprietary network OS that can run on various hardware platforms. VRP has unified network, user, and management interfaces. To efficiently manage Huawei devices, you need to be familiar with VRP commands and configurations.
- Network engineers must master device upgrade skills. Network rectification often requires device upgrade.
- This course describes how to upgrade ACs and APs on a WLAN and how to configure Fat APs.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



WLAN Security



Foreword

- Due to the open transmission medium in wireless communications, the security of a WLAN becomes the main focus of concern. As 802.11 provides increasing wireless access bandwidth, more and more users start to use WLANs. Users also require high security of WLAN access. It has attracted more and more attention from users and enterprises on how to protect user access security and data transmission security.
- This course describes WLAN access security, data security, and security configuration.

Objectives

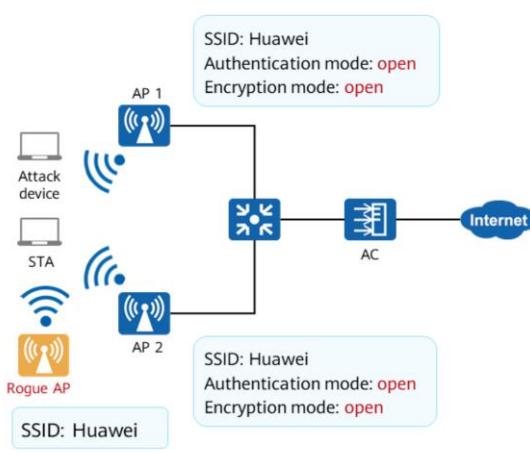
Upon completion of this course, you will be able to:

- Describe WLAN security threats.
- Describe WLAN security defense mechanisms.
- List common WLAN access authentication modes.

Contents

- 1. WLAN Security Threats and Defense**
2. WLAN Access Security
3. WLAN Data Security
4. WLAN Network Access Control
5. WLAN Security Configuration

Common WLAN Security Threats



- **No authentication:** Attackers can connect to a Wi-Fi network randomly to intrude into the network.
- **Non-encrypted wireless data:** Attackers can intercept and tamper with service data transmitted over wireless channels by capturing packets over the air interface.
- **Perimeter threat:** If a rogue AP publishes the same SSID as authorized APs, STAs may connect to the rogue AP. As a result, STA data is intercepted.

328 Huawei Confidential

 HUAWEI

- 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. Configuring WLAN security can protect WLANs against attacks and secure information and services of authorized users..
- WLAN security involves the following aspects:
 - Perimeter security: An 802.11 network is subject to threats from unauthorized APs and users, ad-hoc networks, and denial-of-service (DoS) attacks. A wireless intrusion detection system (WIDS) can detect unauthorized users and APs. A wireless intrusion prevention system (WIPS) can protect enterprise networks and users against access from unauthorized devices.
 - User access security: Link authentication and access authentication are used to ensure validity and security of user access on wireless networks.
 - Service security: Protects service data of authorized users from being intercepted by unauthorized users during transmission.

WLAN Security Defense

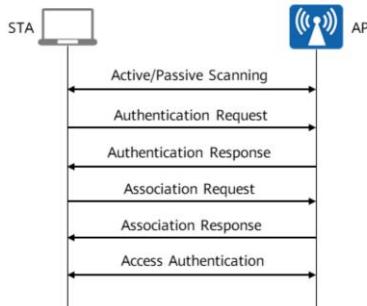
- Security authentication
 - Only authorized users are allowed to access and use the network.
 - Two-way authentication available: The client and server can authenticate each other.
- Data encryption and integrity
 - The confidentiality of data transmitted through transmission media is ensured.
 - Hash, message integrity check (MIC), and cyclic redundancy check (CRC) guarantee data integrity.
- Perimeter security (not described in this chapter)
 - The Wireless Intrusion Detection System (WIDS) monitors the running status of networks and systems in accordance with given security policies, analyzes user activities, and determines the type of intrusion events to detect unauthorized networks.
 - The Wireless Intrusion Prevention System (WIPS) monitors wireless networks in real time to detect intrusion events and provide active defense against and warning of attack behaviors.

Contents

1. WLAN Security Threats and Defense
- 2. WLAN Access Security**
3. WLAN Data Security
4. WLAN Network Access Control
5. WLAN Security Configuration

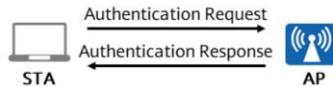
WLAN Access Process

- A STA discovers surrounding wireless networks in active/pассиве scanning mode. After link authentication, association, and access authentication are complete, the STA can connect to an AP and access wireless services.



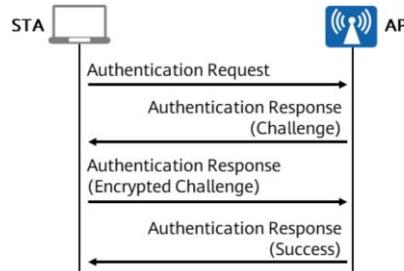
Link Authentication: Open System Authentication

- To ensure wireless link security, an AP needs to authenticate STAs that attempt to access the AP. IEEE 802.11 defines two link authentication modes: open system authentication and shared key authentication.
- Open system authentication requires no authentication. In this authentication mode, an AP responds to the authentication request from any STA with a message indicating that the STA passes the authentication.
- If you want to connect to an SSID that uses open system authentication, no authentication credential is required, and the system displays a message indicating that you have been associated with the WLAN.



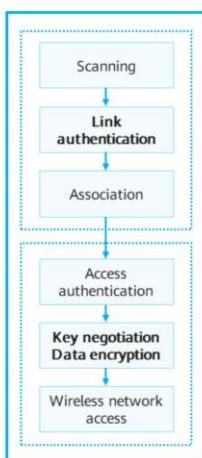
Link Authentication: Shared Key Authentication

- Shared key authentication requires that a STA and an AP have the same key preconfigured. In this authentication mode, the AP checks whether its key is the same as that on the STA during link authentication. If so, the authentication is successful. Otherwise, the STA fails the authentication.



- The STA sends an authentication request to the AP.
- The AP generates a random challenge and sends it to the STA.
- The STA uses the preset key to encrypt the challenge and sends the encrypted challenge to the AP.
- The AP receives the encrypted challenge, decrypts it by using a preset key, and then compares the decrypted challenge with the one previously sent to the STA. If they are the same, the authentication is successful. Otherwise, the authentication fails.

User Access Security Overview



- Link authentication: open system authentication
- Link authentication: shared key authentication

Access authentication security policy: Open

- Link authentication: open system authentication
- Access authentication: N/A
- Data encryption: no encryption

Access authentication security policy: WEP

- Link authentication: shared key authentication or open system authentication
- Data encryption: RC4

Access authentication security policy: WPA/WPA2

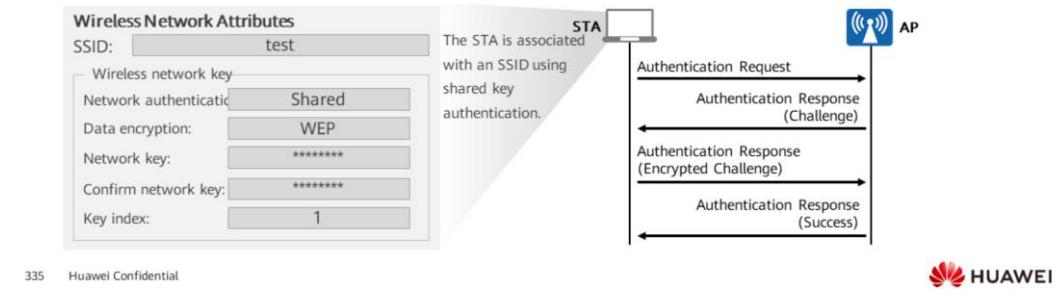
- Link authentication: open system authentication
- Access authentication: PSK, PPSK, or 802.1X
- Key negotiation: PTK/GTK
- Data encryption: TKIP or CCMP

To ensure secure access of wireless users on a WLAN, access security measures need to be taken, for example, establish security associations through authentication to ensure the validity of identities of all communication entities.



Access Authentication Security Policy: WEP

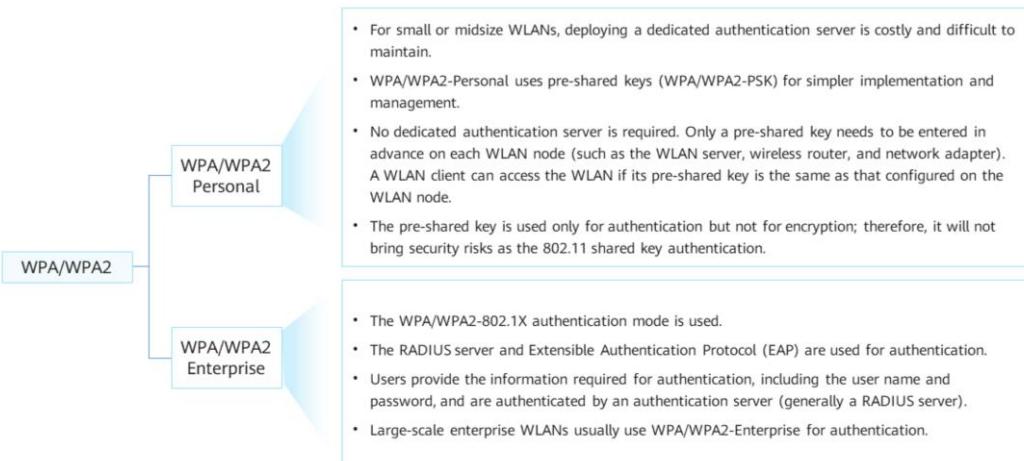
- Wired Equivalent Privacy (WEP) is a security mechanism defined in IEEE 802.11 to prevent the interception of data transmitted by authorized users on a WLAN.
- WEP uses the Rivest Cipher 4 (RC4) algorithm and a static key to encrypt data. All STAs associated with the same SSID use the same key to join a WLAN.
- Shared key authentication is supported only by WEP and requires that the same shared key be configured on a STA and the AP with which the STA attempts to associate.
- The WEP key is exchanged in clear text, which is insecure. Therefore, WEP is not recommended.



335 Huawei Confidential

- WEP uses the RC4 algorithm to encrypt data through a 64-bit, 128-bit, or 152-bit encryption 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 key. All STAs associated with the same SSID use the same key to join a WLAN.
- A WEP security policy defines a link authentication mechanism and a data encryption mechanism.
 - If open system authentication is used, WEP encryption is not required during link authentication. After a user goes online, service data can be encrypted by WEP or not, depending on the configuration.
 - If shared key authentication is used, key negotiation is complete during link authentication. After a user goes online, service data is encrypted using the negotiated key.

Access Authentication Security Policy: WPA/WPA2

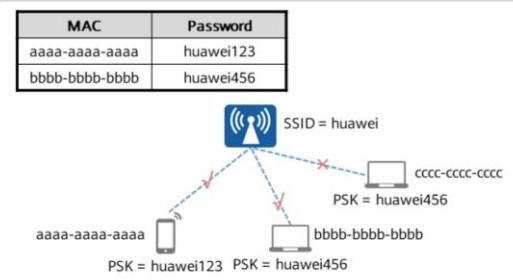


336 Huawei Confidential



- WEP shared key authentication uses the 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 solve the problems with WEP, Wi-Fi Alliance introduced the Wi-Fi Protected Access (WPA). 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.
- Subsequent to WPA, IEEE 802.11i defined WPA2, which uses a more secure encryption algorithm: Counter Mode with CBC-MAC Protocol (CCMP).
- For the sake of better compatibility, both WPA and WPA2 can use 802.1X access authentication and the TKIP or CCMP encryption algorithm. With almost the same security level, WPA and WPA2 mainly differ in the protocol packet format.
- To sum up, the WPA or WPA2 security policy involves four phases: link authentication, access authentication, key negotiation, and data encryption.

PSK and PPSK Authentication

| PSK | PPSK | | | | | | |
|---|--|-----|----------|----------------|-----------|----------------|-----------|
|  <p>SSID = huawei PSK = huawei123</p> <ul style="list-style-type: none"> WPA/WPA2-PSK authentication requires that the same pre-shared key be configured on a wireless client and a wireless server (such as an AP). All clients connected to a specified SSID use the same key, which may bring security risks. | <table border="1"> <thead> <tr> <th>MAC</th><th>Password</th></tr> </thead> <tbody> <tr> <td>aaaa-aaaa-aaaa</td><td>huawei123</td></tr> <tr> <td>bbbb-bbbb-bbbb</td><td>huawei456</td></tr> </tbody> </table>  <p>SSID = huawei PSK = huawei123 PSK = huawei456 PSK = cccc-cccc-cccc</p> <ul style="list-style-type: none"> WPA/WPA2-PPSK authentication inherits the advantages of WPA/WPA2-PSK authentication and is easy to deploy. In addition, WPA/WPA2-PPSK authentication provides different pre-shared keys for different clients, improving network security. Users connected to the same SSID can have different keys. | MAC | Password | aaaa-aaaa-aaaa | huawei123 | bbbb-bbbb-bbbb | huawei456 |
| MAC | Password | | | | | | |
| aaaa-aaaa-aaaa | huawei123 | | | | | | |
| bbbb-bbbb-bbbb | huawei456 | | | | | | |

337 Huawei Confidential



- In PSK authentication, a key must be configured on a STA. Then an AP negotiates with the STA through four-way handshake to validate the STA's key. The WPA-PSK mode can be used on networks with low security requirements.
- PSK authentication requires that a WLAN client and a WLAN server be configured with the same pre-shared key. A client and a server authenticate each other through key negotiation. During key negotiation, the client and server use their pre-shared keys to decrypt the messages sent from each other. If the messages are successfully decrypted, the client and server have the same pre-shared key.
- When PSK authentication is used in WPA/WPA2, only one pre-shared key needs to be entered in advance on each WLAN node. Although the deployment is simple, the pre-shared key is the same for all clients that connect to the same WLAN, which results in the key being shared to unauthorized users.
- As shown in the figures, in WPA/WPA2-PSK authentication, all clients connected to the specified SSID use the same key, which may bring security risks. In WPA/WPA2-PPSK authentication, users connected to the same SSID can have different keys and be authorized with different permissions. If a user has multiple client devices, these client devices can connect to a WLAN using the same PPSK user account.
- WPA/WPA2-PPSK authentication has the following characteristics:
 - Users connected to the same SSID can have different keys.
 - This authentication mode is easy to configure and deploy.
 - If a user has multiple client devices, these client devices can access a WLAN by using the same PPSK user account.
 - A PPSK user is bound to a user group or an authorized VLAN. Therefore, different PPSK users can be authorized with different permissions.

Contents

1. WLAN Security Threats and Defense
2. WLAN Access Security
- 3. WLAN Data Security**
4. WLAN Network Access Control
5. WLAN Security Configuration

WLAN Security Encryption

- After a WLAN user is authenticated and authorized to access a WLAN, the WLAN must use a mechanism to protect data of the user against tampering and eavesdropping. Encryption is the most commonly used mechanism. Encryption algorithms ensure that only devices with correct keys can decrypt received packets.
- WLAN encryption modes:
 - Temporal Key Integrity Protocol (TKIP)
 - Counter Mode with CBC-MAC Protocol (CCMP)
- WPA uses the TKIP encryption algorithm to provide a key reset mechanism and enhance the valid length of the key, alleviating the WEP key flaw.
- WPA2 uses the CCMP encryption mechanism, which adopts the Advanced Encryption Standard (AES) encryption algorithm. This algorithm is a symmetric block encryption technology and makes the key more difficult to crack than the TKIP encryption algorithm.
- Both WPA and WPA2 can use the TKIP or AES encryption algorithm for better compatibility. TKIP and AES provide almost the same security level.

- As WLANs use open transmission media, data is facing great risks if no encryption mechanism is used on transmission links. Anyone with an appropriate tool can intercept unprotected data transmitted on open transmission medium.
- Major objectives of communication security are confidentiality, integrity, and authentication. When data is transmitted on a network, data protection protocols must help network administrators achieve these objectives.
 - Confidentiality means that data will not be intercepted by unauthorized parties.
 - Integrity means that data is not being tampered with during transmission.
 - Authentication is the basis for all security policies. Data validity partially depends on reliability of the data source, so the data receiver must verify correctness of the data source. A system must protect data through authentication. Authorization and access control are both based on data authenticity. Before allowing a user to access any data, the system must verify the user's identity.
- Authentication has been described in the preceding slides. Therefore, WLAN encryption is to ensure data confidentiality and integrity.

WLAN Security Policy Comparison

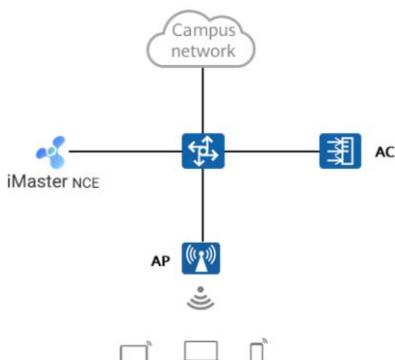
| Security Policy | Link Authentication | Access Authentication | Encryption Algorithm | Recommended Application Scenario | Description |
|-----------------|----------------------------|--|----------------------|--|--|
| Open | Open system authentication | N/A | No encryption | Networks with low security requirements | Wireless devices can connect to a WLAN without authentication. |
| WEP-open | Open system authentication | No access authentication is provided. This security policy can be used together with Portal or MAC address authentication. | No encryption/RC4 | Public places with high user mobility, such as airports, stations, business centers, and conference venues | It is insecure when used independently, because any wireless clients can access the WLAN without authentication. You are advised to configure this security policy together with Portal or MAC address authentication. |
| WEP-share-key | Shared key authentication | N/A | RC4 | Networks with low security requirements | This security policy is not recommended due to its low security. |
| WPA/WPA2-PSK | Open system authentication | PSK authentication | TKIP/AES | Home users or small/midsize enterprise networks | This security policy has higher security than WEP shared key authentication. Additionally, no third-party server is required and the cost is low. |
| WPA/WPA2-802.1X | Open system authentication | 802.1X authentication | TKIP/AES | Large-scale enterprise networks with high security requirements | This security policy provides high security and requires a third-party server, resulting in high costs. |

Contents

1. WLAN Security Threats and Defense
2. WLAN Access Security
3. WLAN Data Security
- 4. WLAN Network Access Control**
5. WLAN Security Configuration

NAC

- Network Access Control (NAC) is an end-to-end security technology that authenticates access clients and users to ensure network security.

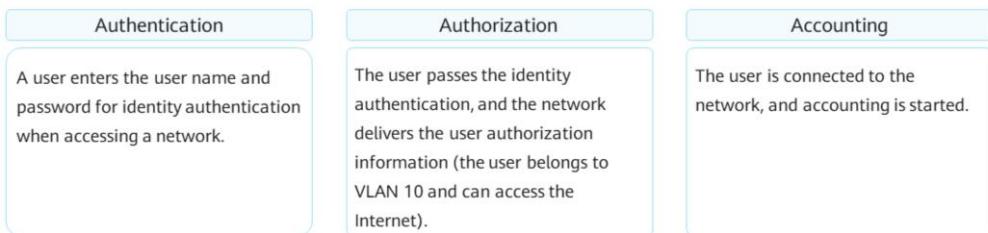


NAC works together with the authentication, authorization, and accounting (AAA) server to implement access authentication.

- NAC:
 - Is used for interaction between users and access devices.
 - Controls the user access mode (802.1X, MAC, or portal authentication) as well as parameters and timers during user access.
 - Ensures secure, stable connections between authorized users and access devices.
- AAA:
 - Is used for interaction between access devices and the AAA server.
 - The AAA server controls the access rights of access users by authenticating, authorizing, and accounting for them.

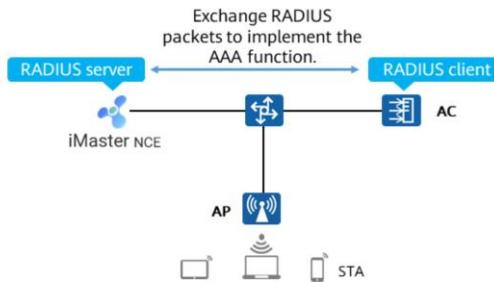
AAA

- Authentication, authorization, and accounting (AAA) provides a management mechanism for network security.
 - Authentication: verifies whether users are permitted to access the network.
 - Authorization: allows users to use particular services.
 - Accounting: records the network resources used by users.



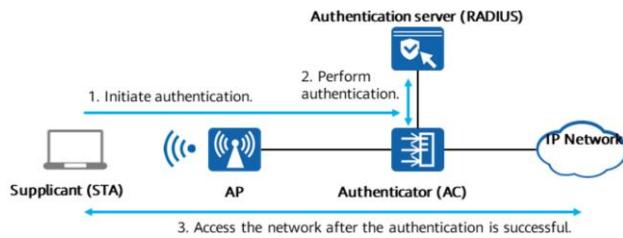
RADIUS

- AAA can be implemented using multiple protocols. RADIUS is most frequently used in actual scenarios.
- RADIUS is a protocol that uses the client/server model in distributed mode and protects a network from unauthorized access. It is often used in network environments that require high security and allow remote user access.
- It defines the UDP-based RADIUS packet format and transmission mechanism, and specifies UDP ports 1812 and 1813 respectively for authentication and accounting.
- RADIUS has the following characteristics:
 - Client/Server model
 - Secure message exchange mechanism
 - Fine scalability



802.1X Authentication

- IEEE 802.1X is an IEEE standard for port-based network access control. It is mainly used for authentication and security on the Ethernet.
- 802.1X authentication uses the typical client/server model and consists of three entities: supplicant, authenticator, and authentication server.
- The authentication server is usually a RADIUS server, which is used to perform authentication, authorization, and accounting for supplicants.
- 802.1X authentication is recommended for employees of midsize to large enterprises.



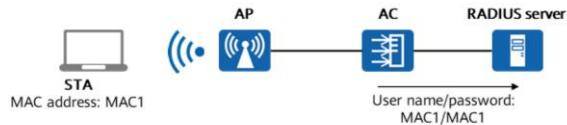
345 Huawei Confidential

 HUAWEI

- The 802.1X authentication system uses the Extensible Authentication Protocol (EAP) to implement information exchange between the supplicant, authenticator, and authentication server. Common 802.1X authentication protocols include Protected Extensible Authentication Protocol (PEAP) and Transport Layer Security (TLS). Their differences are as follows:
 - PEAP: The administrator assigns a user name and password to the user. The user enters the user name and password for authentication when accessing a WLAN.
 - TLS: Users use certificates for authentication. This authentication mode is usually used together with enterprise apps, such as Huawei AnyOffice.
- 802.1X authentication is recommended for employees of midsize to large enterprises.

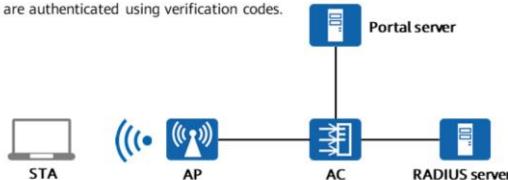
MAC Address Authentication

- MAC address authentication controls a user's network access rights based on the user's MAC address. In this authentication mode, the user does not need to install any client software.
- The access device whose interface has MAC address authentication enabled starts authenticating a user when detecting the user's MAC address for the first time.
- During the authentication process, the user does not need to enter a user name or password.
- MAC address authentication is usually used for dumb terminals (such as printers) to access the network. It also can be used with an authentication server to implement MAC address-prioritized portal authentication: After a user passes the authentication for the first time, the user can access the network again without authentication within a specified period of time.



Portal Authentication

- Portal authentication is also called web authentication. In this authentication mode, a browser is used as the authentication client, and no independent authentication client needs to be installed, as shown in the following figure.
- Before a user can access the Internet, the user must be authenticated on the portal page. The user can access network resources only after passing the authentication. In addition, the service provider can expand their business on the portal page, for example, displaying merchant advertisements.
- Portal authentication is recommended for guests, business exhibitions, and public places of large or midsize enterprises.
- Common portal authentication modes include:
 - User name and password authentication: The administrator registers a temporary account for guests. The guests use this temporary account for authentication.
 - SMS authentication: Guests are authenticated using verification codes.



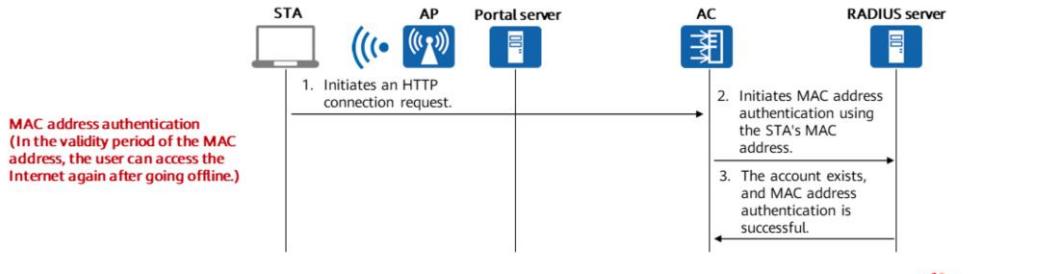
347 Huawei Confidential

 HUAWEI

- Definition:
 - Portal authentication is also called web authentication. Generally, portal authentication websites are referred to as web portals. When a user accesses the Internet, the user must be authenticated on the web portal. If the user fails to be authenticated, the user can access only specified network resources. The user can access other network resources only after passing the authentication.
- Advantages:
 - Ease of use: In most cases, portal authentication does not require the client to have additional software installed and allows the client to be directly authenticated on a web page.
 - Convenient operations: Portal authentication achieves business expansion on the portal page, including advertisement push and enterprise publicity.
 - Mature technology: Portal authentication has been widely used in networks of carriers, fast food chains, hotels, and schools.
 - Flexible deployment: Portal authentication implements access control at the access layer or at the ingress of key data.
 - Flexible user management: Portal authentication can be performed on users based on the combination of the user name and the VLAN, IP address, or MAC address.

MAC Address-Prioritized Portal Authentication

- MAC address-prioritized portal authentication allows disconnected users who have passed portal authentication to access the network again within a certain period of time, without entering the user name and password, as long as they pass MAC address authentication.
- After a user passes portal authentication, the user can access the network again through MAC address authentication within the validity period of the MAC address.
- MAC address-prioritized portal authentication saves the time for users to obtain SMS messages or follow official accounts when being authenticated each time.



348 Huawei Confidential

- To use this function, you need to configure mixed authentication (MAC + Portal) on the device, enable MAC address-prioritized portal authentication on the authentication server (RADIUS server), and set the MAC address validity period.
- If a STA's MAC address is stored on the RADIUS server, the RADIUS server checks the user name and password (both are the MAC address) and directly authorizes the STA. Then the STA can access the network without entering the user name and password.
- If the STA's MAC address expires on the RADIUS server, the RADIUS server deletes the STA's MAC address. MAC address authentication fails and the access device pushes the portal authentication page to the STA. In this case, the user needs to enter the user name and password for identity authentication.

Authentication Mode Comparison

- NAC provides three authentication modes: 802.1X authentication, MAC address authentication, and portal authentication. The three authentication modes are implemented differently and are applicable to different scenarios. In practice, you can use a proper authentication mode or multiple authentication modes (mixed authentication) based on scenarios. The combination of authentication modes depends on device specifications.

| Item | 802.1X Authentication | MAC Address Authentication | Portal Authentication |
|----------------------|--|--|--|
| Application scenario | New network with concentrated users and high requirements for security | Authentication of dumb terminals such as printers and fax machines | Scenario where users are sparsely distributed or move freely |
| Client | Required | Not required | Not required |
| Advantage | High security | No client required | Flexible deployment |
| Disadvantage | Inflexible deployment | MAC address registration required, making management complex | Low security |

Contents

1. WLAN Security Threats and Defense
2. WLAN Access Security
3. WLAN Data Security
4. WLAN Network Access Control
5. **WLAN Security Configuration**

Configuring Open Authentication

- Create a security profile.

```
[AC] wlan  
[AC-wlan-view] security-profile name profile-name
```

- Create a security profile and enter the security profile view. By default, security profiles default, default-wds, and default-mesh are created.

- Set the security policy to open authentication.

```
[AC-wlan-sec-prof-wlan] security open
```

- Set the security policy to open authentication. By default, the security policy is open.

- Command: security open
 - Sets the WEP authentication mode to open.

Configuring a WEP Security Policy

- Create a security profile.

```
[AC] wlan
```

```
[AC-wlan-view] security-profile name profile-name
```

- Set the security policy to WEP.

```
[AC-wlan-sec-prof-wlan] security wep share-key
```

- Configure a WEP shared key.

```
[AC-wlan-sec-prof-wlan] wep key key-id{ wep-40 | wep-104 | wep-128 } { pass-phrase | hex } key-value
```

- Configure a shared key and a key index for static WEP.

- Command: **security wep [share-key | dynamic]**
 - **security wep:** sets the WEP authentication mode to shared key.
 - **security wep share-key:** When the WEP authentication mode is set to shared key:
 - If this parameter is specified, the shared key is used to authenticate STAs and encrypt service packets
 - If this parameter is not specified, the shared key is used only to encrypt service packets.
 - A shared key is configured on STAs regardless of whether this parameter is specified.
 - **security wep dynamic:** Sets the WEP authentication mode to dynamic WEP.
- Command: **wep key key-id { wep-40 | wep-104 | wep-128 } { pass-phrase | hex } key-value**
 - **key-id:** key index.
 - **wep-40:** WEP-40 authentication.
 - **wep-104:** WEP-104 authentication.
 - **wep-128:** WEP-128 authentication.
 - **pass-phrase:** key phrase.
 - **hex:** hexadecimal number.
 - **key-value:** displays the user password in cipher text.

Configuring WPA/WPA2-PSK Authentication

- Create a security profile.

```
[AC] wlan  
[AC-wlan-view] security-profile name profile-name
```

- Set the security policy to WPA/WPA2-PSK.

```
[AC-wlan-sec-prof-wlan] security { wpa | wpa2 | wpa-wpa2 } psk { pass-phrase | hex } key-value{ aes | tkip | aes-tkip }
```

- Command: `security { wpa | wpa2 | wpa-wpa2 } psk { pass-phrase | hex } key-value { aes | tkip | aes-tkip }`
 - `wpa`: configures WPA authentication.
 - `wpa2`: configures WPA2 authentication.
 - `wpa-wpa2`: configures WPA + WPA2 mixed authentication. STAs can be authenticated using WPA or WPA2.
 - `psk`: configures PSK authentication.
 - `pass-phrase`: key phrase.
 - `hex`: hexadecimal number.
 - `key-value`: user password.
 - `aes`: uses AES to encrypt data.
 - `tkip`: uses TKIP to encrypt data.
 - `aes-tkip`: configures AES + TKIP mixed encryption. After the authentication is successful, STAs that support AES or TKIP can use the supported encryption algorithm to encrypt data.

Configuring WPA/WPA2-PPSK Authentication

- Create a security profile.

```
[AC] wlan  
[AC-wlan-view] security-profile name profile-name
```

- Set the security policy to WPA/WPA2-PPSK.

```
[AC-wlan-sec-prof-wlan] security { wpa | wpa2 | wpa-wpa2 } ppsk{ aes | tkip | aes-tkip }
```

- Set key PPSK parameters.

```
[AC-wlan-view] ppsk-user psk { pass-phrase | hex } key-value [ user-name user-name | user-group user-group | vlan vlan-id ]  
expire-date expire-date [ expire-hour expire-hour ] | max-device max-device-number | branch-group branch-group | mac-address  
mac-address]* ssid ssid
```

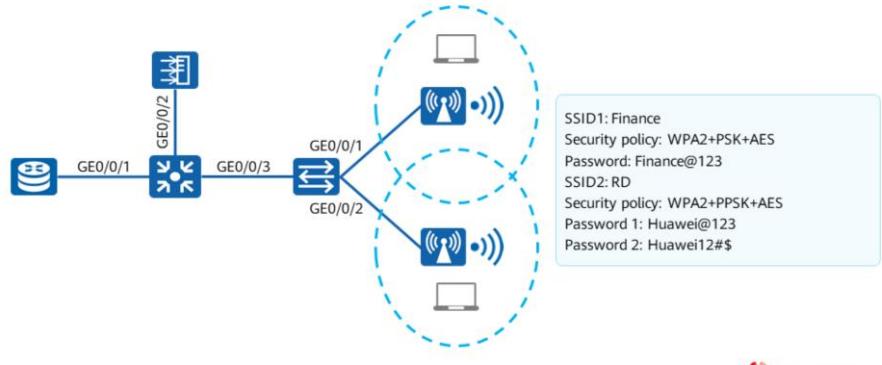
- Create a PPSK user, and configure the password, user name, user group, authorized VLAN, expiration time, maximum number of access users, branch group, MAC address, and SSID for the PPSK user.

- Command: security { wpa | wpa2 | wpa-wpa2 } psk { pass-phrase | hex } key-value { aes | tkip | aes-tkip }
 - ppsk: configures PPSK authentication.
- Command: ppsk-user psk { pass-phrase | hex } key-value [user-name user-name | user-group user-group | vlan vlan-id | expire-date expire-date [expire-hour expire-hour] | max-device max-device-number | branch-group branch-group | mac-address mac-address]* ssid ssid
 - pass-phrase: key phrase.
 - hex: hexadecimal number.
 - key-value: displays the user password in cipher text.
 - user-name user-name: specifies the name of a PPSK user.
 - If you do not specify user-name when creating a PPSK user, the system automatically generates the user name ppsk_auto_user_xxx, where xxx indicates a number. If user-name is specified, the user name must be unique.
 - user-group user-group: specifies the user group to which the PPSK user is bound.
 - vlan vlan-id: specifies the authorized VLAN bound to the PPSK user.
 - expire-date expire-date [expire-hour expire-hour]: specifies the expiration date of the PPSK user. The user cannot access the network after the specified date. If this parameter is not specified, the validity period of the PPSK user expires on December 31, 2099.
 - branch-group branch-group: specifies the branch AP group to which the PPSK user belongs.
 - mac-address mac-address: specifies the MAC address bound to the PPSK user.

- **ssid** **ssid:** specifies the SSID of the PPSK user.

Case: PSK and PPSK

- As shown in the figure, the customer requires that the WLAN be able to provide network services for both the R&D department and finance department. For employees in the finance department, the unified password authentication mode with high password security is needed. For employees in the R&D department, each employee requires one password for authentication.



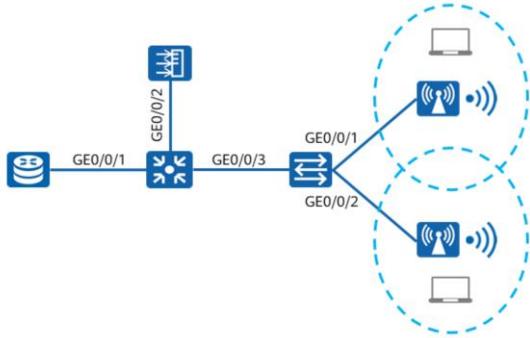
355 Huawei Confidential

 HUAWEI

- The WLAN has been deployed and WLAN signals have been released.
- Configuration roadmap:
 - Create two security profiles: Finance and RD.
 - Bind the two security profiles to the corresponding VAP profiles.

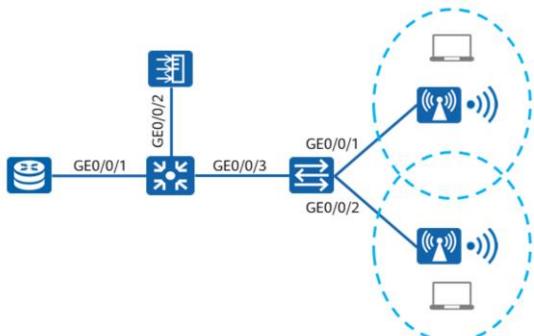
Creating Security Profiles

- Create security profiles **Finance** and **RD**, and set corresponding security policies.



```
[AC-wlan-view] security-profile name Finance
[AC-wlan-sec-prof-Finance] security wpa2 psk pass-phrase
Finance@123aes
[AC-wlan-sec-prof-Finance] quit
[AC-wlan-view] security-profile name Employee
[AC-wlan-sec-prof-RD] security wpa2 ppsk aes
[AC-wlan-sec-prof-RD] quit
[AC-wlan-view] ppsk-user psk pass-phrase Huawei@123 max-device
1 ssid RD
[AC-wlan-view] ppsk-user psk pass-phrase Huawei12#$max-device
1 ssid RD
```

Binding Profiles



- Bind the two security profiles to the corresponding VAP profiles.

```
[AC-wlan-view] vap-profile name Finance  
[AC-wlan-vap-prof-Finance] security-profile Finance  
[AC-wlan-vap-prof-Finance] quit  
[AC-wlan-view] vap-profile name RD  
[AC-wlan-vap-prof-RD] security-profile Guest  
[AC-wlan-vap-prof-RD] quit
```

Viewing AP Signal Information

- WLAN service configurations are automatically delivered to APs. After the configurations are complete, run the “**display vap ssid RD**” command to check the authentication type (Auth type).

```
[AC-wlan-view]display vap ssid RD
```

Info: This operation may take a few seconds, please wait.

WID : WLAN ID

| AP ID | AP name | RfID | WID | BSSID | Status | Auth type | STA | SSID |
|-------|---------|------|-----|----------------|--------|---------------|-----|------|
| 0 | AP1 | 0 | 1 | 00E0-FC41-6340 | ON | WPA/WPA2-PPSK | 0 | RD |
| 0 | AP1 | 1 | 1 | 00E0-FC41-6350 | ON | WPA/WPA2-PPSK | 0 | RD |
| 1 | AP2 | 0 | 1 | 00E0-FCA2-5970 | ON | WPA/WPA2-PPSK | 0 | RD |
| 1 | AP2 | 1 | 1 | 00E0-FCA2-5980 | ON | WPA/WPA2-PPSK | 0 | RD |

Quiz

1. (Multi-Answer Question) Which of the following belong to link authentication?
()
 - A. Open system authentication
 - B. Shared key authentication
 - C. WPA/WPA2 PSK
 - D. WPA/WPA2 PPSK

- 1. AB

Summary

- WLAN uses radio waves instead of network cables to transmit data. Compared with a wired network, a WLAN is easier to deploy. However, due to the particularity of transmission media, WLAN security issues are prominent.
- This course describes the security threats facing the WLAN and details common security mechanisms for reducing such threats.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



WLAN Service Configuration (Web)



Foreword

- An AC has a built-in web server to allow access through a web browser, facilitating its maintenance and use.
- This course will instruct you to configure WLAN services using the web system.

Objectives

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

- Understand the WLAN service configuration procedure.
- Configure basic WLAN services.

Contents

- 1. Web System Overview**
2. WLAN Service Configuration Procedure
3. WLAN Configuration Application

Web System Login



- The prerequisites for logging in to the web system are as follows:
 - An IP address has been configured for the access interface on the AC.
 - A PC can communicate with the device.
 - The device is running properly, and the HTTP and HTTPS services have been correctly configured.
 - The browser software has been installed on the PC.

- Open a browser, enter `http://IP address` or `https://IP address` in the address box, for example, `http://169.254.1.1` or `https://169.254.1.1`, and press Enter. (169.254.1.1 is used as an example here. Enter the actual IP address of the access interface.) The web platform login page is displayed.
- Enter login information.
 - Select a language.
 - The web system supports English and Chinese and automatically adapts to the language used by the web browser.
 - Enter the user name and password.
 - The default user name and password are `admin` and `admin@huawei.com`, respectively.
 - Click **Login**. The operation page is displayed.
 - To ensure security of the web system, you are prompted to change the password upon the first login, and log in again.
- Click the logout icon on the upper right of the page to return to the login page.
- After you successfully log in to the system, if no operation is performed in a specified period (default: 10 minutes), the system automatically logs out. Click **OK** to return to the login page.

Introduction to the Web System (1/3)

The screenshot shows the 'AP Going Online' section of the configuration interface. At the top, there are tabs for 'Monitoring', 'Configuration', 'Diagnosis', and 'Maintenance'. The 'Configuration' tab is selected. In the center, there's a table titled 'AP State Table' with two rows of data:

| AP ID | AP Name | MAC Address | Type | Version | Serial Number | Longitude, Latitude | Operat... |
|-------|---------|----------------|------|------------------|---------------|-----------------------|-----------|
| 0 | AP1 | f4de-af36-ad60 | -- | AirEngine5760-10 | -- | 2102352UBR10L60012... | id... |
| 1 | AP2 | f4de-af36-acc0 | -- | AirEngine5760-10 | -- | 2102352UBR10L60012... | id... |

At the bottom right of the table, there are navigation buttons: '<', '1', and '>'. A red box highlights the top right corner of the interface, which contains the 'Auto-save: Scheduled save' button, 'Save' button, 'CLI' button, help icon, and log out icon.

- Operation buttons: allow you to quickly save the current configuration, obtain help, and log out of the system.

Introduction to the Web System (2/3)

The screenshot shows the 'AP State Table' section of the 'AP Going Online' configuration page. On the left, a navigation tree includes 'Config Wizard', 'AC', 'AP Going Online' (which is highlighted), 'Wireless Service', 'Mesh', 'AC Config', 'AP Config', 'Security', 'Other Services', and 'Reliability'. The main area displays the following information:

- AC version number: V200R019C00SPC300
- AP authentication mode: Non-authentication (with a note: "After the AP authentication mode is modified, the states of APs will change. Manually update the AP state table later.")
- Total number of APs: 2
- Number of online APs: 2 (unauthorized: 0, verMismatch: 0, idle: 2, nameConflicted: 0)
- Table headers: AP ID, AP Name, MAC Address, IP Address, Type, Version, Serial Number, Longitude, Latitude, Operat...
- Data rows:

| AP ID | AP Name | MAC Address | IP Address | Type | Version | Serial Number | Longitude, Latitude | Operat... |
|-------|---------|----------------|------------|------------------|---------|-----------------------|---------------------|-----------|
| 0 | AP1 | f4de-af36-ad60 | -- | AirEngine5760-10 | -- | 2102352UBR10L60012... | id... | edit... |
| 1 | AP2 | f4de-af36-acc0 | -- | AirEngine5760-10 | -- | 2102352UBR10L60012... | id... | edit... |
- Total record(s): 2

- Menu navigation: displays the function categories on each tab page in navigation tree mode. The level-1 menu stays on the upper left area of the page, and the level-2 menu stays on the left area of the page.

Introduction to the Web System (3/3)

The screenshot shows the 'AP Going Online' configuration page. The top navigation bar includes tabs for Monitoring, Configuration, Diagnosis, Maintenance, and CLI. The left sidebar lists sections: Config Wizard, AC, AP Going Online (selected), Wireless Service, Mesh, AC Config, AP Config, Security, Other Services, and Reliability. The main content area has three tabs: 1. APs Go Online, 2. Group APs, and 3. Confirm Configurations. Tab 1 is selected. It displays the 'AP State Table' with the following details:

- AC version number: V200R019C00SPC300
- AP authentication mode: Non-authentication (with a note: "After the AP authentication mode is modified, the states of APs will change. Manually update the AP state table later.")
- Total number of APs: 2
- Number of online APs: 2 (unauthorized: 0, verMismatch: 0, idle: 2, nameConflicted: 0)

The table lists two APs:

| ID | AP Name | MAC Address | Type | Version | Serial Number | Longitude, Latitude | Operat... |
|----|---------|----------------|------------------|---------|-----------------------|---------------------|-----------|
| 0 | AP1 | f4de-af36-ad60 | AirEngine5760-10 | -- | 2102352UBR10L60012... | id... | edit |
| 1 | AP2 | f4de-af36-acc0 | AirEngine5760-10 | -- | 2102352UBR10L60012... | id... | edit |

Bottom right of the table: AP ID dropdown, search input, and navigation buttons (first, last, previous, next).

- Operation area: allows you to configure specific functions or view the function status.

Contents

1. Web System Overview
2. **WLAN Service Configuration Procedure**
3. WLAN Configuration Application

WLAN Basic Service Configuration Procedure

Configuring APs to go online

- Creating an AP group
- Configuring network connectivity
- Configuring system parameters for the AC

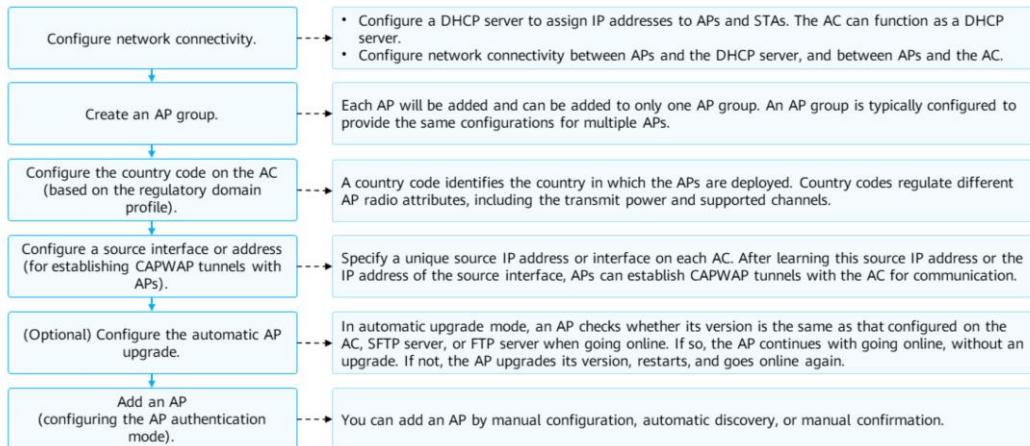
Configuring profiles

- Configuring an SSID profile
- Configuring a security profile
- Configuring a VAP profile

Binding profiles

- Binding profiles to a VAP profile
- Binding the VAP profile to an AP or AP group

Configuring an AP to Go Online

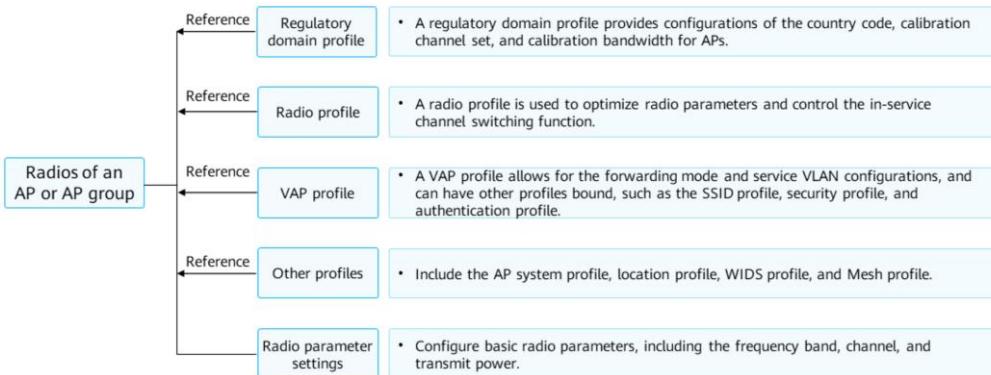


- Regulatory domain profile:
 - A regulatory domain profile provides configurations of the country code, calibration channel set, and calibration bandwidth for APs.
 - A country code identifies the country in which the APs are deployed. Country codes regulate different AP radio attributes, including 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 on the AC.
 - Specify a unique IP address, VLANIF interface, or loopback interface for each AC. In this manner, APs connected to an AC can learn the specified IP address or the IP address of the specified interface to establish CAPWAP tunnels with the AC for communication. This specified IP address or interface is called the source address or interface.
 - APs can establish CAPWAP tunnels with the AC only after the AC's source interface or address is specified.
 - A VLANIF or loopback interface can be configured as the AC's source interface so that the IP address of the source interface is used as the source address.
- Add APs: Configure the AP authentication mode and enable APs to go online.
 - You can add APs by manual configuration, automatic discovery, and manual confirmation, that is, importing APs before they go online, configuring the AC to automatically discover APs, and manually confirming APs in the unauthenticated AP

list.

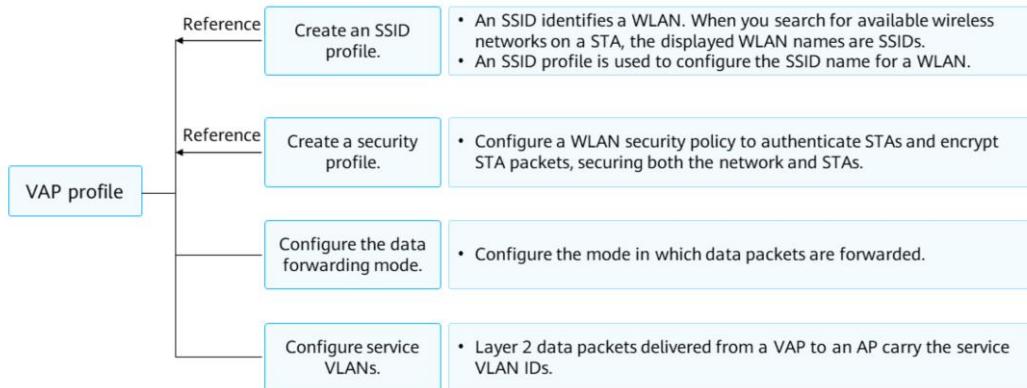
Configuring and Binding Profiles

- Various WLAN profiles are designed based on different WLAN functions and features to help you configure and maintain WLAN functions.



- There are a large number of APs on a WLAN, among which many require the same configurations. To simplify AP configurations, add these APs to an AP group and perform configurations uniformly in the AP group. However, APs may have different configurations. These configurations cannot be uniformly performed but can be directly performed on each AP. Each AP will be added and can be added to only 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.
- The following profiles can be bound to an AP group and AP: regulatory domain profile, AP system profile, radio profile, and VAP profile. 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. Correct country code configuration ensures that radio attributes of APs comply with local laws and regulations.
 - A calibration channel set limits the dynamic adjustment range for AP channels when the radio calibration function is configured. Exclude radar channels and the channels that are not supported by STAs from the calibration channel set.
- 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. After parameters in a radio profile are delivered to an AP, only the parameters supported by the AP can take effect.
 - Configurable parameters include the radio type, radio rate, multicast rate of radio packets, and interval at which an AP sends Beacon frames.

VAP Profile

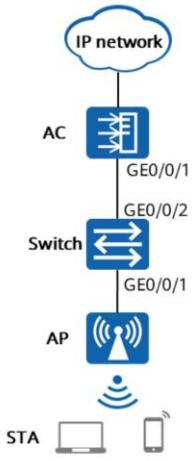


- SSID profile: allows you to configure an SSID name for a WLAN and other functions, including:
 - SSID hiding: When creating a WLAN, configure an AP to hide the SSID name to ensure WLAN security. In this manner, only the STAs that know the SSID can connect to the WLAN.
 - Maximum number of STAs on a VAP: More access STAs on a VAP indicate less network resources that are available to each STA. To ensure Internet access experience, you can configure a proper maximum number of access STAs on a VAP based on site requirements.
 - SSID hiding when the number of STAs reaches the maximum: With this function, when the number of access STAs on a WLAN reaches the maximum, the SSID of the WLAN is hidden so that new STAs cannot find the SSID.
- Security profile: allows you to configure a WLAN security policy to authenticate STAs and encrypt STA packets, securing both the WLAN and STAs.
 - A security profile supports various WLAN security policies including open-system authentication, WEP, WPA/WPA2-PSK, and WPA/WPA2-802.1X.

Contents

1. Web System Overview
2. WLAN Service Configuration Procedure
- 3. WLAN Configuration Application**

Topology Design



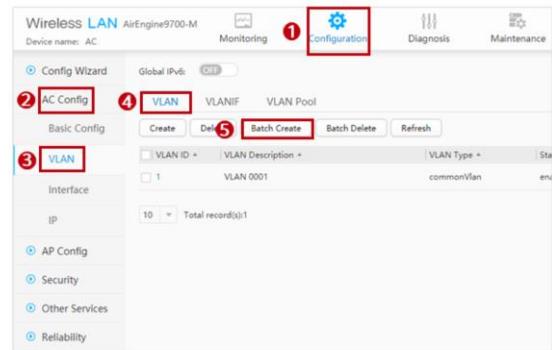
- This topology is a Layer 2 network where the AC is deployed in in-path mode, and applies to small-scale enterprises.
- The AC functions as the gateway for both APs and STAs.
 - APs' gateway address: 10.1.100.1/24
 - STAs' gateway address: 10.1.101.1/24
- All traffic from STAs reaches the AC and then is forwarded by the AC to the upper-layer network.

WLAN Data Planning

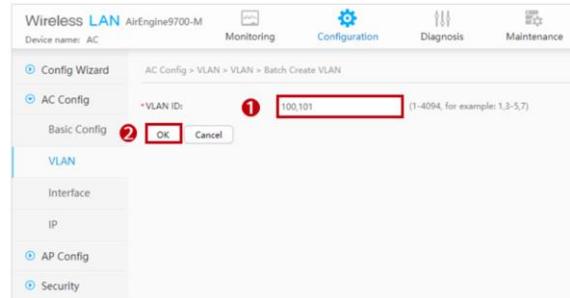
| Data | Configuration |
|---|--|
| DHCP server | The AC functions as a DHCP server to assign IP addresses to APs and STAs, and also serves as the gateway for APs and STAs. |
| IP address pool for APs | VLAN 100: 10.1.100.2-10.1.100.254/24 |
| IP address pool for STAs | VLAN 101: 10.1.101.2-10.1.101.254/24 |
| IP address of the AC's source interface | VLANIF 100: 10.1.100.1/24 |
| AP group | Name: ap-group1 Referenced profiles: VAP profile and regulatory domain profile |
| Regulatory domain profile | Name: domain Country code: CN |
| SSID profile | Name: employee SSID name: employee |
| Security profile | Name: employee Security policy: WPA-WPA2+PSK+AES-TKIP Password: a1234567 |
| VAP profile | Name: employee Forwarding mode: tunnel forwarding Service VLAN: VLAN 102 Referenced profiles: SSID profile employee and security profile employee |

Configuring Network Connectivity: Creating a VLAN (1/2)

- Choose **Configuration > AC Config > VLAN > VLAN**. The **VLAN** page is displayed.
- Click **Batch Create**. On the **Batch Create VLAN** page that is displayed, set parameters.



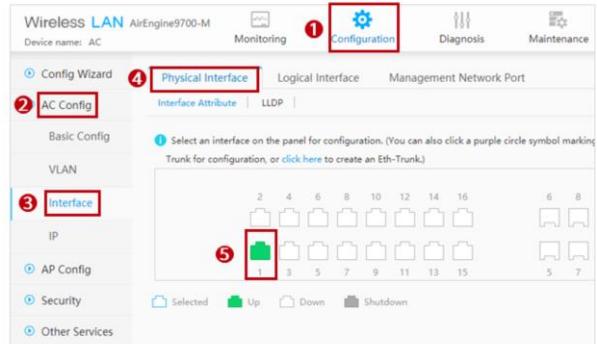
Configuring Network Connectivity: Creating a VLAN (2/2)



- Create VLAN 100 and VLAN 101 on the AC according to the WLAN data planning.
- Click OK. VLANs are created.

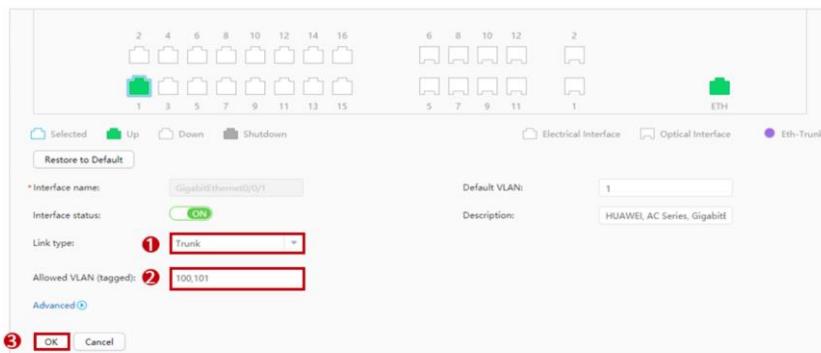
Configuring Network Connectivity: Configuring Ethernet Interfaces (1/2)

- Choose Configuration > AC Config > Interface > Physical Interface. The Physical Interface page is displayed.
- Click interface 1 as an example. In the expanded interface configuration area, set parameters.



Configuring Network Connectivity: Configuring Ethernet Interfaces (2/2)

- Set **Link type** to **Trunk** and **Allowed VLAN (tagged)** to VLANs 100 and 101.
- Click **OK**. The Ethernet interface is configured.



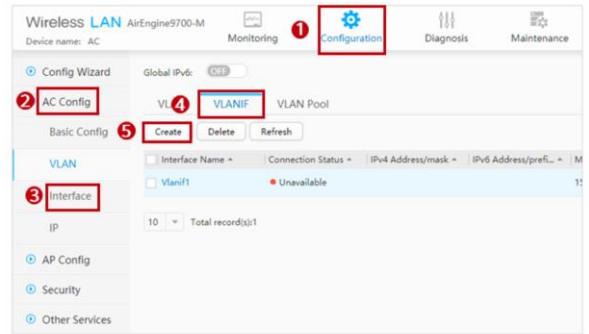
384 Huawei Confidential

HUAWEI

- Switch configuration:
 - [SW] vlan batch 100 101
 - [SW] interface gigabitethernet 0/0/1
 - [SW-GigabitEthernet0/0/1] port link-type access
 - [SW-GigabitEthernet0/0/1] port default vlan 100
 - [SW-GigabitEthernet0/0/1] quit
 - [SW] interface gigabitethernet 0/0/2
 - [SW-GigabitEthernet0/0/2] port link-type trunk
 - [SW-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 101
 - [SW-GigabitEthernet0/0/2] quit

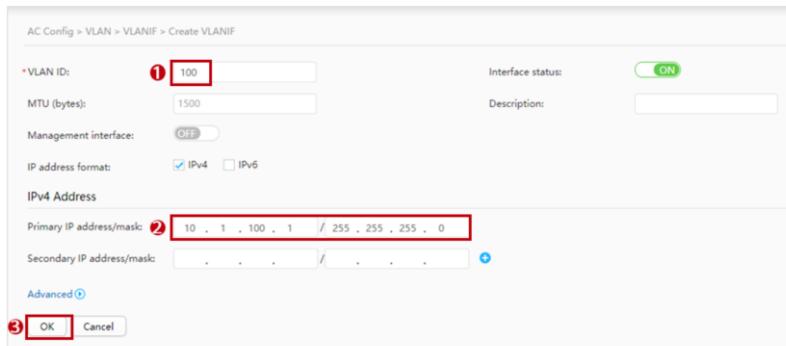
Configuring Network Connectivity: Configuring Virtual Interfaces (1/2)

- Choose **Configuration > AC Config > VLAN > VLANIF**. The **VLANIF** page is displayed.
- Click **Create**. On the **Create VLANIF** page that is displayed, set parameters.



Configuring Network Connectivity: Configuring Virtual Interfaces (2/2)

- Configure an IP address for VLANIF 100 as required. (The configuration is the same for VLANIF 101.)
- Click **OK**. The virtual interfaces are configured.



AC Config > VLAN > VLANIF > Create VLANIF

* VLAN ID: **100** MTU (bytes): 1500 Interface status: **ON**

Management interface: **Off** Description:

IP address format: IPv4 IPv6

IPv4 Address

Primary IP address/mask: **10 . 1 . 100 . 1 / 255 . 255 . 255 . 0**

Secondary IP address/mask: . . . / . . . +

Advanced **③**

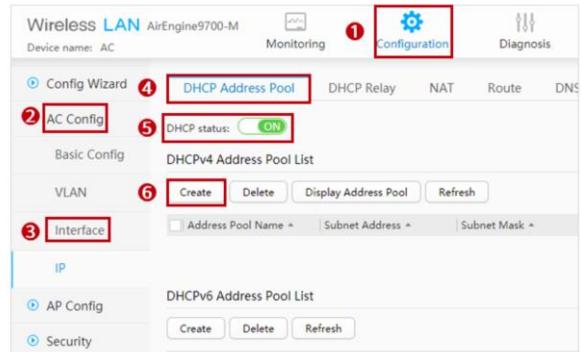
③ OK Cancel

386 Huawei Confidential



Configuring Network Connectivity: Configuring DHCP (1/2)

- Choose Configuration > AC Config > IP > DHCP Address Pool. The DHCP Address Pool page is displayed.
- Enable DHCP. In the DHCPv4 Address Pool List area, click Create. On the Create DHCPv4 Address Pool page that is displayed, set parameters.



Configuring Network Connectivity: Configuring DHCP (2/2)

- Configure an interface address pool for VLANIF 100 as required. (The configuration is the same for VLANIF 101.)
- Click **OK**. The DHCP configuration is completed.

AC Config > IP > DHCP Address Pool > Create DHCPv4 Address Pool

* Address pool type: Global address pool Interface address pool **①**

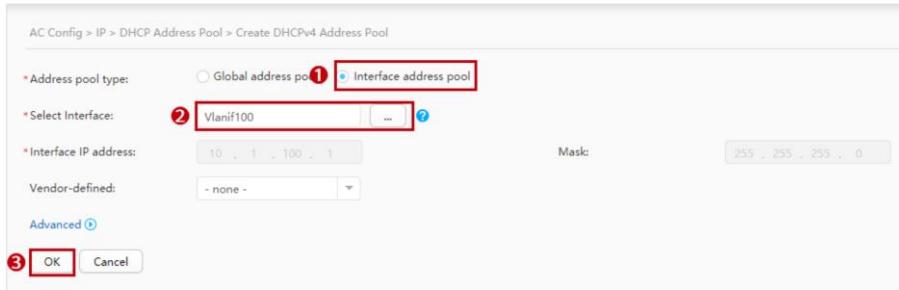
* Select Interface: **②**

* Interface IP address: Mask:

Vendor-defined:

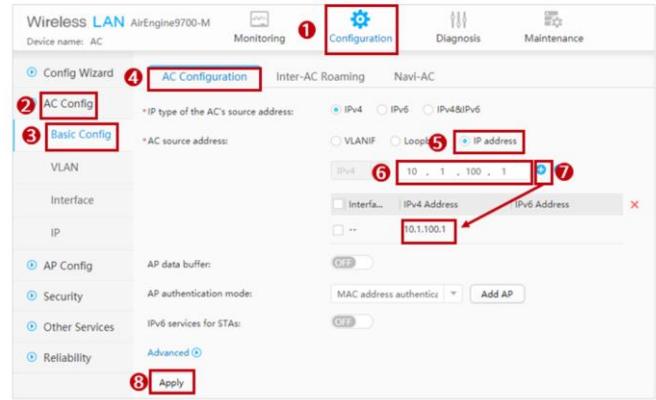
Advanced

③



Configuring APs to Go Online: Configuring the AC's Source Address

- Choose Configuration > AC Config > Basic Config > AC Configuration. The AC Configuration page is displayed.
- Set AC source address to 10.1.100.1.
- Click **Apply**. The AC's source address is configured.



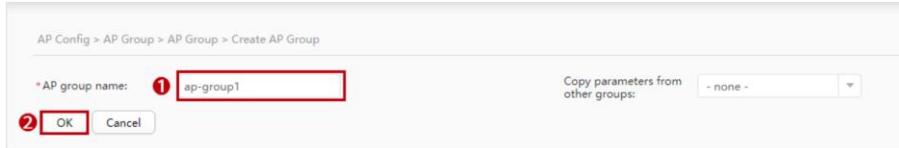
Configuring APs to Go Online: Creating an AP Group (1/2)

- Choose **Configuration > AP Config > AP Group > AP Group**. The AP Group page is displayed.
- Click **Create**. On the Create AP Group page that is displayed, set parameters.

The screenshot shows the 'AP Group' page under the 'Configuration' tab of the 'Wireless LAN' section. The top navigation bar includes 'Monitoring', 'Configuration' (with a red box around it), and 'Diagnosis'. Below the navigation is a table header with columns: 'Group Name', 'VAP Profile', 'Radio 0 Profile', and 'Radio 1 Profile'. A single row is visible with the value 'default' in the 'Group Name' column. To the right of the table are buttons for 'Create', 'Delete', and 'Refresh'. The left sidebar has tabs for 'AP Config' (highlighted with a red box) and 'AP Group' (also highlighted with a red box). Other tabs include 'Profile' and 'Security'. At the bottom left of the page is a note: '20 Total record(s):1'.

Configuring APs to Go Online: Creating an AP Group (2/2)

- Create an AP group as required.
- Click **OK**. The AP group is configured.



Configuring APs to Go Online: Adding an AP (1/2)

- Choose Configuration > AP Config > AP Info. The AP Info page is displayed.
- In the AP List area, click Add. On the Add AP page that is displayed, set parameters.

The screenshot shows the AP Info page with several UI elements highlighted by red boxes and numbers:

- 1**: A red box highlights the "Configuration" tab in the top navigation bar.
- 2**: A red box highlights the "AP Config" item in the left sidebar.
- 3**: A red box highlights the "AP Config" item in the left sidebar under "AP Group".
- 4**: A red box highlights the "AP Info" tab in the top navigation bar.
- 5**: A red box highlights the "Add" button in the toolbar below the AP List table.

The AP List table has the following columns: AP ID, AP MAC, AP Name, Group, IP Address, Type, and Ver. The table displays the message "No data".

Configuring APs to Go Online: Adding an AP (2/2)

- Add the recorded MAC address of the AP and name it **AP1**.
- Click **OK**. The AP is added.

The screenshot shows the 'AP Config > AP Config > AP Info > Add AP' interface. It has two tabs: 'Manually add' (selected) and 'Batch import'. Under 'Adding mode', 'AP MAC' is selected. In the 'AP MAC' field, the value 'f4de - af36 - ad60' is entered. The 'AP name' field contains 'AP1'. The 'OK' button at the bottom left is highlighted with a red border and the number '3' above it. A small blue '+' icon is located in the top right corner of the form area.

Configuring APs to Go Online: Adding an AP to an AP Group (1/2)

- Choose Configuration > AP Config > AP Config > AP Info. The AP Info page is displayed.
- In the AP List area, select an AP and click Modify AP Configuration. On the Modify AP page that is displayed, modify parameters as required.

Configuring APs to Go Online: Adding an AP to an AP Group (2/2)

- Change AP group to ap-group1.
- Click OK. The AP is added to the AP group.

AP Config > AP Config > AP Info > Modify AP

AP group: ① ap-group1

Branch AP group: - none -

AC IP address list:

Selected AP List

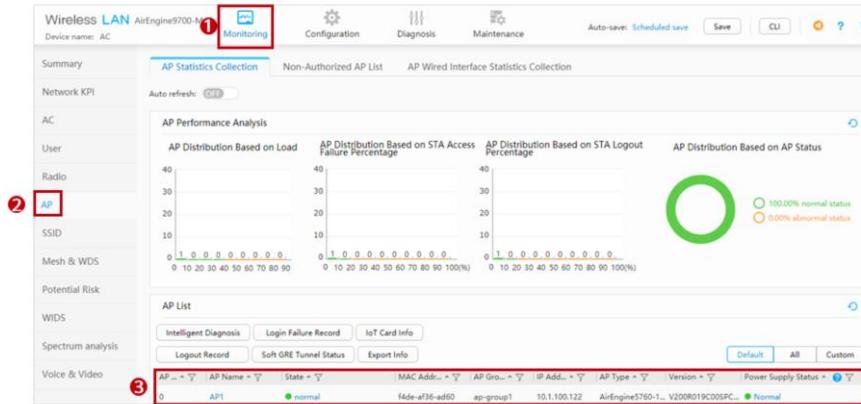
| AP... | AP... | AP Name | AP Group | IP Obtaining Mod... | IP Address | Mask | Gateway |
|-------|---------|---------|----------|---------------------|------------|------|---------|
| 0 | f4de... | AP1 | default | - none - | -- | -- | -- |

10 Total record(s):

② OK Cancel

Configuring APs to Go Online: Checking AP Onboarding Information

- Choose **Monitoring > AP**. The **AP Statistics Collection** page is displayed.
- Check AP onboarding information.



396 Huawei Confidential

HUAWEI

Configuring Profiles: SSID Profile (1/2)

- Choose Configuration > AP Config > Profile > Wireless Service > SSID Profile. The SSID Profile List page is displayed.
- Click Create. On the Create SSID Profile page that is displayed, set parameters.

The screenshot shows the 'Configuration' tab selected in the top navigation bar. The left sidebar has 'Profile' highlighted with a red box. The main area shows 'Profile Management' with 'SSID Profile' selected (also highlighted with a red box). A list of profiles is shown on the right, with 'default' selected. Buttons for 'Create', 'Delete', 'Clear', and 'Display Reference' are visible. A note at the bottom says 'Total record(s):1'. Red numbers 1 through 6 are overlaid on the interface to indicate specific steps: 1 points to the Configuration tab, 2 points to the AP Config item in the sidebar, 3 points to the Profile item in the sidebar, 4 points to the Wireless Service item in the Profile Management list, 5 points to the SSID Profile item in the list, and 6 points to the Create button.

Configuring Profiles: SSID Profile (2/2)

- Set **Profile name** to **employee** and click **OK**. The SSID profile **employee** is created.
- On the page that is displayed, set **SSID** to **employee**.
- Click **Apply**. The SSID profile is configured.

The screenshot shows two pages of a network configuration interface. The top part is a 'Create SSID Profile' dialog with fields for 'Profile name' (set to 'employee') and 'SSID' (set to 'employee'). The bottom part is the 'SSID Profile' configuration page for the 'employee' profile, showing the 'Basic Configuration' tab selected. It displays the 'SSID' ('employee'), 'Maximum number of STAs' (set to '64'), and an 'Action upon reaching the maximum' dropdown set to 'Reject new STA access'. A note at the top of this page states: 'Profile Description: SSIDs identify different wireless networks. When you search for available wireless networks on your STA, the displayed'. The 'Basic Configuration' tab is highlighted in blue.

398 Huawei Confidential

 HUAWEI

Configuring Profiles: Security Profile (1/3)

- Choose Configuration > AP Config > Profile > Wireless Service > Security Profile. The Security Profile List page is displayed.
- Click Create. On the Create Security Profile page that is displayed, set parameters.

The screenshot shows the 'Configuration' tab selected in the top navigation bar. The left sidebar has 'Profile' highlighted. The main content area shows 'Profile Management' with 'Wireless Service' selected. Under 'Wireless Service', 'Security Profile' is highlighted and selected. A 'Create' button is visible in the top right of the profile list table. The table lists three security profiles: 'default', 'default-wds', and 'default-mesh'. The bottom right of the interface shows the HUAWEI logo.

Configuring Profiles: Security Profile (2/3)

- Set **Profile name** to **employee**.
- Click **OK**. The security profile **employee** is created.

The screenshot shows a 'Create Security Profile' dialog box. At the top left is the title 'Create Security Profile'. Below it is a field labeled 'Profile name:' with the value 'employee'. To the right of this field is a dropdown menu labeled 'Copy parameters from other profiles:' with the option '- none -'. At the bottom left of the dialog are two buttons: 'OK' (highlighted with a red box and the number '2') and 'Cancel'.

Configuring Profiles: Security Profile (3/3)

- Configure the security profile as required.
- Click **Apply**. The security profile is configured.

Security Profile: employee Display Reference

Profile Description: You can configure WLAN security policies to authenticate identities of wireless terminals and encrypt user packets.

Basic Configuration Advanced Configuration

Security policy: Open WEP WPA **WPA-1** **WPA-WPA2** WAPI

Authentication policy: **PSK** Dot1x PPSK

WPA encryption mode: AES TKIP **AES-TKIP**

WPA2 encryption mode: AES TKIP **AES-TKIP**

Key type: HEX **PASS-PHRASE**

* Key:

Apply

① Security policy: WPA-WPA2
② Authentication policy: PSK
③ WPA encryption mode: AES-TKIP
④ Key type: PASS-PHRASE
⑤ Key value: *****
⑥ Apply button

401 Huawei Confidential

 HUAWEI

Configuring Profiles: VAP Profile (1/3)

- Choose **Configuration > AP Config > Profile > Wireless Service > VAP Profile**. The **VAP Profile List** page is displayed.
- Click **Create**. On the **Create VAP Profile** page that is displayed, set parameters.

The screenshot shows the 'Profile Management' section of the configuration interface. The left sidebar has 'Profile' selected (step 3). The main area shows a list of profiles under 'Wireless Service' (step 4), with 'VAP Profile' selected (step 5). A 'Create' button is highlighted (step 6). The right side displays the 'VAP Profile List' with one entry named 'default'. The top navigation bar includes 'Configuration' (highlighted in red), 'Monitoring', 'Diagnosis', and 'Maintenance'.

Configuring Profiles: VAP Profile (2/3)

- Set **Profile name** to **employee**.
- Click **OK**. The VAP profile **employee** is created.

Create VAP Profile

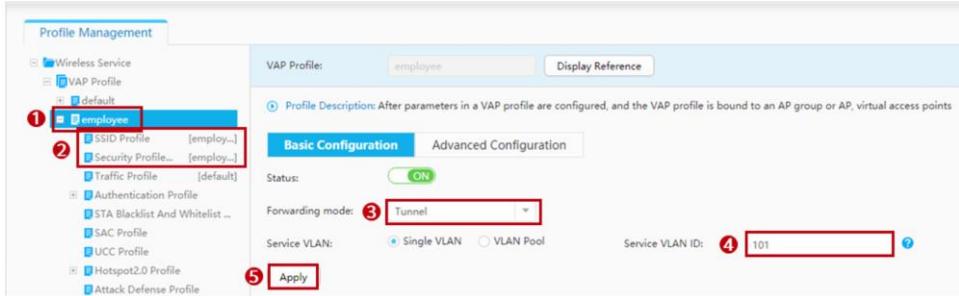
Profile name: **employee** ①

Copy parameters from other profiles: **- none -** ▼

② **OK** **Cancel**

Configuring Profiles: VAP Profile (3/3)

- Configure the VAP profile as required.
- Click **Apply**. The VAP profile is configured.



Binding Profiles: Binding Profiles to an AP Group (1/2)

- Choose Configuration > AP Config > AP Group > AP Group. The AP Group page is displayed.
- Click ap-group1. On the AP Group page that is displayed, set parameters.

| Group Name | VAP Profile | Radio 0 Profile | Radio 1 Profile | Radio 2 Profile |
|-------------|--------------|-----------------|-----------------|-----------------|
| default | 2.4G-default | 5G-default | 5G-default | 5G-default |
| 5 ap-group1 | 2.4G-default | 5G-default | 5G-default | 5G-default |

Binding Profiles: Binding Profiles to an AP Group (2/2)

- Click **VAP Configuration**. On the **VAP Profile List** page that is displayed, click **Add**. On the **Add VAP Profile** page that is displayed, select a VAP profile as required.
- Click **OK**. The VAP profile is bound to the AP group.

The screenshot shows the HUAWEI AP Config interface. At the top left, it says "AP Config > AP Group > AP Group". The main title is "AP group configuration: ap-group1". Below this, there's a "Members" section with a checkbox for "Display all profiles" and a link to "VAP Configuration". A red box labeled ① highlights this link. To the right is a "VAP Profile List" table with columns for "Profile Name", "SSID Profile", "Authentic.", and "Security Profile". There are "Create", "Add", "Remove", and "Display Reference" buttons. Below the table is a "Related Configuration" section with checkboxes for "Profile Name", "SSID Profile", "Authentic.", and "Security Profile". A red box labeled ② highlights the "Add" button. In the center, a modal window titled "Add VAP Profile" is open. It contains fields for "VAP profile name" (set to "employee", highlighted by a red box ③), "WLAN ID" (set to "1"), and "Radio" (set to "0,1,2"). Below these fields are "Advanced" and "OK" buttons. A red box labeled ④ highlights the "OK" button. At the bottom left of the main interface, it says "406 Huawei Confidential". At the bottom right, the HUAWEI logo is visible.

Checking STA Access Information

- Choose **Monitoring > User**. The **Online STA Statistics** page is displayed.
- Check STA access information.

The screenshot shows the 'Online STA Statistics' page for a device named 'AirEngine9700-0'. The 'Monitoring' tab is selected. The 'User' section is highlighted with a red box labeled ②. The 'User List' table at the bottom is also highlighted with a red box labeled ③. The table displays the following data:

| User Name | MAC Address | AP Name | IPv4 Address | Frequency | PHY Mode | Negotiation | RSSI (dBm) | SNR (dBm) | Air Interface |
|--------------|----------------|---------|--------------|-----------|--------------|-------------|------------|-----------|---------------|
| 38539c789fc4 | 3853-9c78-9fc4 | API | 10.1.101.84 | 2.4G | 11n HT 20MHz | 144/117 | -69 | 26.0 | 40 |

Quiz

1. (Multiple-Answer Question) Which of the following profiles can be bound to an AP group?
 - A. SSID profile
 - B. Security profile
 - C. Regulatory domain profile
 - D. VAP profile

- 1. CD

Summary

- In this course, we go through the WLAN service configuration procedure, including how an AP goes online and how to configure VAPs. WLAN service configurations help you understand the service relationships between WLAN profiles.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



WLAN Service Configuration



Foreword

- Various WLAN profiles are designed based on different WLAN functions and features to help you configure and maintain WLAN functions. These WLAN profiles have different referencing relationships, based on which you can easily grasp the configuration roadmap of WLAN profiles and complete required service configurations.
- This course will instruct you to configure WLAN services using the CLI.

Objectives

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

- Understand the WLAN service configuration procedure.
- Configure basic WLAN services.

Contents

- 1. WLAN Service Configuration Procedure**
2. WLAN Configuration Application

WLAN Basic Service Configuration Procedure

Configuring APs to go online

- Creating an AP group
- Configuring network connectivity
- Configuring system parameters for the AC

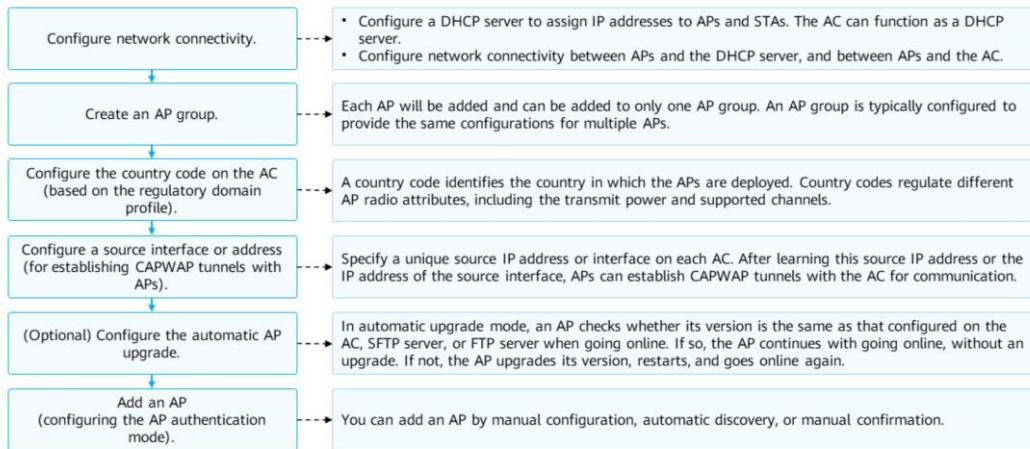
Configuring profiles

- Configuring an SSID profile
- Configuring a security profile
- Configuring a VAP profile

Binding profiles

- Binding profiles to a VAP profile
- Binding the VAP profile to an AP or AP group

Configuring an AP to Go Online

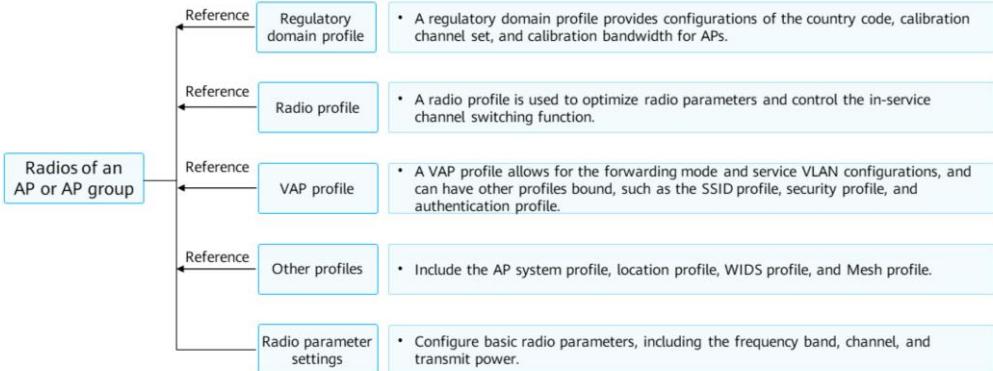


- Regulatory domain profile:
 - A regulatory domain profile provides configurations of the country code, calibration channel set, and calibration bandwidth for APs.
 - A country code identifies the country in which the APs are deployed. Country codes regulate different AP radio attributes, including 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 on the AC.
 - Specify a unique IP address, VLANIF interface, or loopback interface for each AC. In this manner, APs connected to an AC can learn the specified IP address or the IP address of the specified interface to establish CAPWAP tunnels with the AC for communication. This specified IP address or interface is called the source address or interface.
 - APs can establish CAPWAP tunnels with the AC only after the AC's source interface or address is specified.
 - A VLANIF or loopback interface can be configured as the AC's source interface so that the IP address of the source interface is used as the source address.
- Add APs: Configure the AP authentication mode and enable APs to go online.
 - You can add APs by manual configuration, automatic discovery, and manual confirmation, that is, importing APs before they go online, configuring the AC to automatically discover APs, and manually confirming APs in the unauthenticated AP

list.

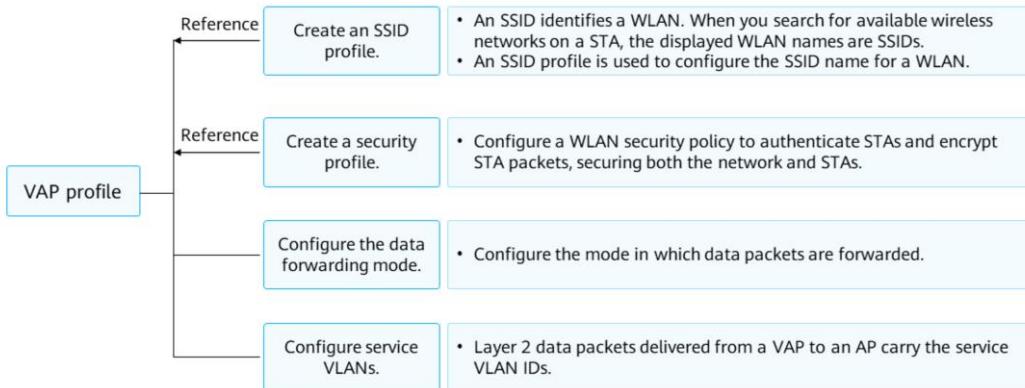
Configuring and Binding Profiles

- Various WLAN profiles are designed based on different WLAN functions and features to help you configure and maintain WLAN functions.



- There are a large number of APs on a WLAN, among which many require the same configurations. To simplify AP configurations, add these APs to an AP group and perform configurations uniformly in the AP group. However, APs may have different configurations. These configurations cannot be uniformly performed but can be directly performed on each AP. Each AP will be added and can be added to only 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.
- The following profiles can be bound to an AP group and AP: regulatory domain profile, AP system profile, radio profile, and VAP profile. 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. Correct country code configuration ensures that radio attributes of APs comply with local laws and regulations.
 - A calibration channel set limits the dynamic adjustment range for AP channels when the radio calibration function is configured. Exclude radar channels and the channels that are not supported by STAs from the calibration channel set.
- 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. After parameters in a radio profile are delivered to an AP, only the parameters supported by the AP can take effect.
 - Configurable parameters include the radio type, radio rate, multicast rate of radio packets, and interval at which an AP sends Beacon frames.

VAP Profile



420 Huawei Confidential



- SSID profile: allows you to configure an SSID name for a WLAN and other functions, including:
 - SSID hiding: When creating a WLAN, configure an AP to hide the SSID name to ensure WLAN security. In this manner, only the STAs that know the SSID can connect to the WLAN.
 - Maximum number of STAs on a VAP: More access STAs on a VAP indicate less network resources that are available to each STA. To ensure Internet access experience, you can configure a proper maximum number of access STAs on a VAP based on site requirements.
 - SSID hiding when the number of STAs reaches the maximum: With this function, when the number of access STAs on a WLAN reaches the maximum, the SSID of the WLAN is hidden so that new STAs cannot find the SSID.
- Security profile: allows you to configure a WLAN security policy to authenticate STAs and encrypt STA packets, securing both the WLAN and STAs.
 - A security profile supports various WLAN security policies including open-system authentication, WEP, WPA/WPA2-PSK, and WPA/WPA2-802.1X.

WLAN Service Configuration: Configuring an AP to Go Online (1/3)

- 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 }
 - The DHCP server is configured to assign the specified user-defined option to DHCP clients.
- Create a regulatory domain profile and configure the country code.

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

- A regulatory domain profile is created and its view is displayed, or the view of an existing regulatory domain profile is displayed.

- A country code is configured for the device.

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

- Command: **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 that ranges 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.
- Command: **regulatory-domain-profile** name profile-name
 - 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 (").
- Command: **country-code** 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
 - FR: France
 - US: United States
 - ...

WLAN Service Configuration: Configuring an AP to Go Online (2/3)

- Bind the regulatory domain profile.

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

- An AP group is created and its view is displayed, or the view of an existing AP group is displayed.

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

- The regulatory domain profile is bound to an AP or AP group.

- Configure a source interface or address.

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

- A source interface is specified on the AC for establishing CAPWAP tunnels with APs.

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

- The AC's source IP address is configured.

- Command: ap-group name group-name

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

WLAN Service Configuration: Configuring an AP to Go Online (3/3)

- Add an AP.

```
[AC-wlan-view] ap auth-mode { mac-auth | sn-auth | no-auth }
```

- The AP authentication mode is set to MAC address or SN authentication. The default mode is MAC address authentication.

```
[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
```

- An AP is added or the AP view is displayed, and the AP name is configured.

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

- The AP is added to an AP group.

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

- Check AP information.

- Command: 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 }]
 - ap-id: specifies the ID of an AP. The value is an integer that ranges from 0 to 8191.
 - type-id type-id: specifies the ID of an AP type. The value is an integer that ranges from 0 to 255.
 - ap-type ap-type: specifies the type of an AP. The value is a string of 1 to 31 characters.
 - ap-mac 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.
 - ap-sn 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.

Basic WLAN Service Configuration: Configuring VAPs (1/4)

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

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

- Configure the direct or tunnel data forwarding mode in the VAP profile.

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

- Configure service VLANs for the VAP.

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

Basic WLAN Service Configuration: Configuring VAPs (2/4)

- Configure a security profile.
 - A security profile is created and the security profile view is displayed.
[AC-wlan-view] **security-profile name** *profile-name*
[AC-wlan-sec-prof-profile-name]
 - By default, the system has security profiles default, default-wds, and default-mesh.
 - The security profile is bound to the VAP profile.
[AC-wlan-view] **vap-profile name** *profile-name*
[AC-wlan-vap-prof-profile-name] **security-profile** *profile-name*

Basic WLAN Service Configuration: Configuring VAPs (3/4)

- Configure an SSID profile.
 - An SSID profile is created and the SSID profile view is displayed, or the view of an existing SSID profile is displayed.

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

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

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

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

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

- The SSID profile is bound to the VAP profile.

- Command: **ssid ssid**

- 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.

Basic WLAN Service Configuration: Configuring VAPs (4/4)

- Bind the VAP profile to radios in the AP group.

```
[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 } ]
```

- Display information about service VAPs.

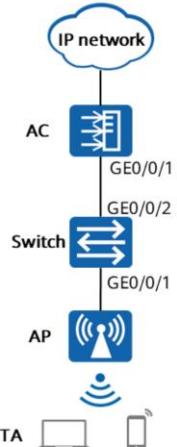
```
[AC] display vap { ap-group ap-group-name | { ap-name ap-name| ap-id ap-id } [ radio radio-id ] } [ ssid ssid ]  
[AC] display vap { all | ssid ssid }
```

- Command: `display vap { ap-group ap-group-name | { ap-name ap-name | ap-id ap-id } [radio radio-id] } [ssid ssid]`
 - ap-group ap-group-name: displays information about all service VAPs in a specified AP group. The AP group must exist.
 - ap-name ap-name: displays information about service VAPs on the AP with a specified name. The AP name must exist.
 - ap-id ap-id: displays information about service VAPs on the AP with a specified ID. The AP ID must exist.
 - radio radio-id: displays information about service VAPs of a specified radio. The value is an integer that ranges from 0 to 2.
 - ssid ssid: displays information about service VAPs of a specified SSID. The SSID must exist.
- Command: `display vap { all | ssid ssid }`
 - all: displays information about all service VAPs.

Contents

1. WLAN Service Configuration Procedure
2. **WLAN Configuration Application**

Topology Design

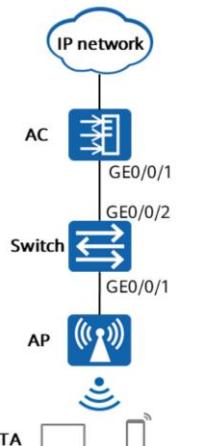


- This topology is a Layer 2 network where the AC is deployed in in-path mode, and applies to small-scale enterprises.
- The AC functions as the gateway for both APs and STAs.
 - APs' gateway address: 10.1.100.1/24
 - STAs' gateway address: 10.1.101.1/24
- All traffic from STAs reaches the AC and then is forwarded by the AC to the upper-layer network.

WLAN Data Planning

| Data | Configuration |
|---|--|
| DHCP server | The AC functions as a DHCP server to assign IP addresses to APs and STAs, and also serves as the gateway for APs and STAs. |
| IP address pool for APs | VLAN 100: 10.1.100.2-10.1.100.254/24 |
| IP address pool for STAs | VLAN 101: 10.1.101.2-10.1.101.254/24 |
| IP address of the AC's source interface | VLANIF 100: 10.1.100.1/24 |
| AP group | Name: ap-group1 Referenced profiles: VAP profile and regulatory domain profile |
| Regulatory domain profile | Name: domain Country code: CN |
| SSID profile | Name: employee SSID name: employee |
| Security profile | Name: employee Security policy: WPA-WPA2+PSK+AES Password: a1234567 |
| VAP profile | Name: employee Forwarding mode: tunnel forwarding Service VLAN: VLAN 101 Referenced profiles: SSID profile employee and security profile employee |

Configuring Network Connectivity



- Create VLANs and interfaces on the switch and AC.
- Configure a DHCP server to assign IP addresses to APs and STAs.

```
[AC]dhcp enable  
[AC]interface Vlanif 100  
[AC-Vlanif100]ip address 10.1.100.1 24  
[AC-Vlanif100]dhcp select interface  
[AC-Vlanif100]quit  
[AC]interface Vlanif 101  
[AC-Vlanif101]ip address 10.1.101.1 24  
[AC-Vlanif101]dhcp select interface  
[AC-Vlanif101]quit
```

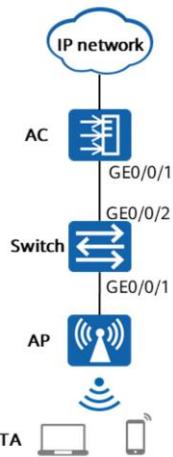
- Switch configuration:

- [SW] vlan batch 100 101
- [SW] interface gigabitethernet 0/0/1
- [SW-GigabitEthernet0/0/1] port link-type access
- [SW-GigabitEthernet0/0/1] port default vlan 100
- [SW-GigabitEthernet0/0/1] quit
- [SW] interface gigabitethernet 0/0/2
- [SW-GigabitEthernet0/0/2] port link-type trunk
- [SW-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 101
- [SW-GigabitEthernet0/0/2] 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 an AP to Go Online (1/2)



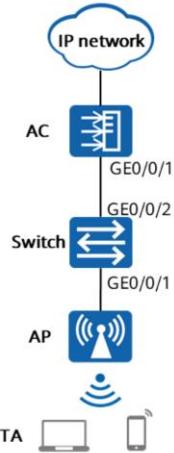
- Create an AP group.

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

Configuring an AP to Go Online (2/2)



- Configure the AC's source interface.

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

- Import an AP that is offline on the AC.

```
[AC]wlan
```

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

```
[AC-wlan-view]ap-id 0 ap-mac 00e0-fc44-4270
```

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

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

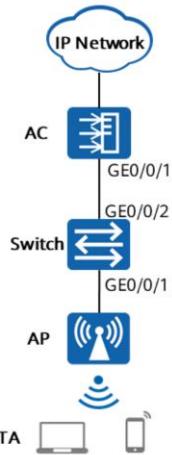
```
[AC-wlan-ap-0]quit
```

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]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   00e0-fc44-4270  ap1    ap-group1  10.1.100.254 AirEngine5760-10  nor    0   10S      -
-----
Total: 1
```

Configuring WLAN Service Parameters (1/2)



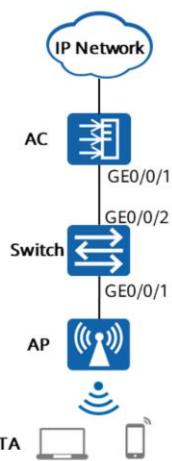
- Create security profile **employee** and configure a security policy.

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

- Create SSID profile **employee** and set the SSID name to **employee**.

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

Configuring WLAN Service Parameters (2/2)



- Create VAP profile **employee**, 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 employee  
[AC-wlan-vap-prof-employee]forward-mode tunnel  
[AC-wlan-vap-prof-employee]service-vlan vlan-id 101  
[AC-wlan-vap-prof-employee]security-profile employee  
[AC-wlan-vap-prof-employee]ssid-profile employee  
[AC-wlan-vap-prof-employee]quit
```

- Bind VAP profile **employee** to the AP group so that configurations in this VAP profile are applied to all radios on the AP.

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

Checking VAP Profile Information

- The WLAN service configuration is automatically delivered to the AP. After the service configuration is complete, run the `display vap ssid employee` command to check VAP profile information. If Status in the command output is displayed as ON, the VAPs have been successfully created for the corresponding AP radios.

```
[AC-wlan-view]display vap ssid employee
```

WID : WLAN ID

| AP ID | AP name | RfID | WID | BSSID | Status | Auth type | STA | SSID |
|-------|---------|------|-----|----------------|--------|--------------|-----|----------|
| 0 | ap1 | 0 | 1 | 00E0-FC44-4270 | ON | WPA/WPA2-PSK | 0 | employee |
| 0 | ap1 | 1 | 1 | 00E0-FC44-4280 | ON | WPA/WPA2-PSK | 0 | employee |

Total: 2

Quiz

1. (True or False) After a VAP profile is configured, it can be bound only to an AP group but not to a single AP.
 - A. True
 - B. False

- 1. B

Summary

- In this course, we go through the WLAN service configuration procedure, including how an AP goes online and how to configure VAPs. WLAN service configurations help you understand the service relationships between WLAN profiles.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



WLAN Troubleshooting Basics



Foreword

- Wired LANs are expensive and lack mobility. The increasing demand for portability and mobility requires WLAN technologies. As the most cost-efficient and convenient network access mode nowadays, WLAN allows users to freely move within the covered area.
- Common faults on a WLAN include AP join failures, STA access faults, and other faults caused by incorrect configurations. This course describes the basic WLAN troubleshooting process.

Objectives

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

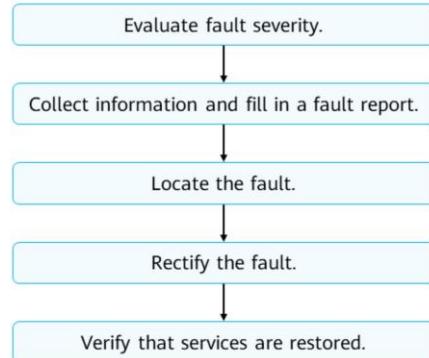
- Summarize common WLAN faults.
- Describe the WLAN troubleshooting process.
- Know common troubleshooting methods.

Contents

- 1. Overview of WLAN Troubleshooting**
 - General Troubleshooting Process
 - Common System Maintenance Methods
 - Common System Maintenance Commands
2. Troubleshooting APs' Failures to Go Online
3. Troubleshooting STAs' Failures to Go Online
4. Troubleshooting AP Signal Issues
5. Troubleshooting Slow Internet Access of STAs

General Troubleshooting Process

- The common troubleshooting process is as follows:



Evaluating Fault Severity

- Upon a fault, analyze the fault symptom and confirm the fault scope to determine how to process it further.
 - If all the users encounter a fault, check whether other users or devices connected to the same upper-layer device also encounter this fault.
 - If only certain users encounter the fault, perform the following operations:
 - Check the type of the faulty service to find out whether other services are faulty.
 - Check whether the AC port to which the faulty user is connected has normal users connected.
- Faults are classified into the following levels based on the fault severity:

| Critical | Major | Minor | Warning |
|--|--|--|---|
| An alarm severity that indicates a severe resource problem disrupting or severely impeding normal use. | An alarm severity that indicates the possibility of some service-related problems with the resource. The severity of the problem is relatively high and the normal use of the resource is likely to be impaired. | An alarm severity that indicates the problems without affecting services. The problems of this severity may result serious faults, and therefore you need to take some corrective actions. | An alarm severity that indicates a condition exists that could potentially cause a problem with the resource. |

Collecting Information

- After a fault occurs, collect detailed fault information immediately, helping locate the fault accurately. Collect the following information before troubleshooting a fault:

| No. | Item | Collection Method |
|-----|------------------------|--|
| 1 | Networking information | Draw a network diagram, showing upstream and downstream devices and interconnection interfaces. |
| 2 | Running status | Record the system running status before and after a fault as well as the generated log information. |
| 3 | Fault symptom | Record the fault time, fault symptom, and operations that may cause the fault. |
| 4 | Hardware status | Record the model, version, and running status of the faulty device. |
| 5 | System information | Collect system information by running the display current-configuration command in the system view. |

Common Methods for Collecting Information (1/3)

- Collect information by one click. This method is used to display or export diagnosis information during system running to a .txt file. The diagnosis information includes the startup configuration, current configuration, interface information, time, and system version.

```
<Huawei> display diagnostic-information dia-info.txt  
This operation will take several minutes, please wait.....
```

Info: The diagnostic information was saved to the device successfully.

▫ By default, diagnostic information is saved to the root directory of the default storage device (**flash:/** or **sdcard:/**). To verify that the file is correctly generated, run the **dir** command in the user view.

- Obtain logs (including user and diagnostic logs), which record user operations, system faults, and system security information.

```
<AC> save logfile  
<AC> system-view  
[AC] diagnose  
[AC-diagnose] save diag-logfile  
[AC-diagnose] return
```

▫ After the preceding commands are executed, user logs and diagnostic logs are saved in **log.log** and **log.dbg** files, which are saved in the log directory (for example, **flash:/logfile**).

Common Methods for Collecting Information (2/3)

- Query the interface status.

```
[Huawei] display interface brief
```

- Query the MAC address table.

```
[Huawei] display mac-address
```

- Query the ARP table.

```
[Huawei] display arp all
```

- Query the current configuration.

```
[Huawei] display current-configuration
```

- Query the device version.

```
[Huawei] display version
```

Common Methods for Collecting Information (3/3)

- Check AP online failure records.

```
<AC> display ap online-fail-record mac xxxx-xxxx-xxxx
```

- Check the AP status.

```
<AC> display ap all
```

- Check the IP address of the AP.

```
<AP> display ap-address-info
```

- Check the CAPWAP link status of the AP.

```
[AP-diagnose] display capwap link all
```

- Check the CAPWAP configuration on the AC.

```
[AC] display capwap configuration
```

Locating a Fault

- Locating a fault quickly and accurately is important for troubleshooting in the following ways:
 - Improves troubleshooting efficiency.
 - Effectively prevents the fault from occurring at other locations.
 - Provides guidance and reference for troubleshooting.
- Preliminarily locating faults

| Fault Symptom | Possible Cause |
|---|---|
| Services on a single AP are interrupted. | Faults of STAs, lines, switch ports, power supply, etc. |
| Services on all APs are interrupted. | Faults of the AC or lines, network attacks, etc. |
| Services on multiple devices are interrupted. | Faults of upper-layer devices, data configuration errors of devices, etc. |

Common Methods for Locating Faults

- Observation: Observe device alarms and indicator status.
- Exclusion: Disable a suspicious function or feature to eliminate its impact on the problem. For example, if the fault is rectified after encrypted authentication is disabled, the fault is caused by this function. If the fault persists, the problem is not caused by this function.
 - In terms of hardware, if a device may cause the fault, directly replace the device to check whether the fault is rectified.
- Comparison: Locate a fault by comparing the faulty component or fault symptom with a functional component or normal condition, respectively.
- Interchange: Locate a fault by interchanging a possibly faulty component with a functional component and comparing the running status before and after the interchange.

Rectifying a Fault

- Fault rectification is the procedure for restoring the system by taking proper measures. After locating the fault, rectify it as follows:
 - Isolate the fault to prevent it from occurring at other locations and reduce impact on services.
 - Troubleshoot the fault by checking and repairing lines, replacing components, or modifying configuration data.
 - For hardware faults: Reset or replace the faulty component.
 - For configuration faults: Modify configuration data or upgrade software.

Service Verification

- After rectifying a fault, verify that the affected services are restored.
 - Verify that the fault has been rectified and no new fault occurs.
 - After the fault is rectified, work out a troubleshooting report and summarize cases as soon as possible.

Contents

- 1. Overview of WLAN Troubleshooting**
 - General Troubleshooting Process
 - Common System Maintenance Methods
 - Common System Maintenance Commands
2. Troubleshooting APs' Failures to Go Online
3. Troubleshooting STAs' Failures to Go Online
4. Troubleshooting AP Signal Issues
5. Troubleshooting Slow Internet Access of STAs

Restoring Factory Defaults

- When a fault, such as a device login failure, occurs due to incorrect configurations, hold down the Default button to enable the device to restart using the factory defaults.
- To restore the factory defaults of the device, hold down the Default button for at least 3s after the device is started. The device then restarts and loads the factory defaults.
- Alternatively, run the reset factory-configuration command to restart the device and restore the factory defaults.
- After factory defaults are restored, the original configuration file still exists. To change the startup configuration file, run the startup saved-configuration command.

```
<Huawei> startup saved-configuration vrpcfg.cfg  
<Huawei> reboot fast
```

Restarting the Device

- When a network fault occurs, restarting the device may clear the fault.
- The following methods are available for restarting a device:

| Method | Description |
|------------------------------|---|
| Cold restart | To perform a cold restart, power off and then power on the device again, which is usually used by onsite maintenance personnel. Running configurations will not be saved during the cold restart. Therefore, save configurations before restarting the device. |
| Warm restart (using the CLI) | A warm restart is performed using the reboot command, which is usually used by maintenance personnel for remote device management. During the warm restart, the system displays a message, asking you whether to save the configurations. This prevents loss of configuration data. |

Transferring Files Using FTP/TFTP (1/3)

- The PC functions as an FTP server. In this mode, you must install the FTP server software on your PC. You only need to configure an IP address for the interface connecting the device to the PC, and then run the put or get command to upload or download files.



- Configure an IP address for the interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.0.1 24
[Huawei-GigabitEthernet0/0/0] ping 192.168.0.2
  PING 192.168.0.2: 56 data bytes, press CTRL_C to break
    Reply from 192.168.0.2: bytes=56 Sequence=1 ttl=128 time=4 ms
    Reply from 192.168.0.2: bytes=56 Sequence=2 ttl=128 time=3 ms
    Reply from 192.168.0.2: bytes=56 Sequence=1 ttl=128 time=4 ms
    Reply from 192.168.0.2: bytes=56 Sequence=2 ttl=128 time=3 ms
...
...
```

Transferring Files Using FTP/TFTP (2/3)

- Log in to the FTP server.

```
<Huawei> ftp 192.168.0.2
Trying 192.168.0.2 ...
Press CTRL+K to abort
Connected to 192.168.0.2.
220 FTP Server ready.
User(192.168.0.2:(none)):ftpuser
331 Password required for ftpuser.
Enter password:
230 User logged in.
```

- Upload files.

```
[Huawei-ftp] put vrpcfg.zip
```

- Download files.

```
[Huawei-ftp] binary
[Huawei-ftp] get devicesoft.cc
```

- The binary command sets the file transfer mode to binary on an FTP client.
- By default, the file transfer mode is ASCII.
- The ASCII mode is used to transfer plaintext files, and the binary mode is used to transfer application files, such as system software (with the file name extension of .cc or .pat), images, video files, compressed files, and database files.

Transferring Files Using FTP/TFTP (3/3)

- The device functions as an FTP server. In this mode, you must configure an IP address for the device and configure an FTP user, without the need to install the FTP server software on the device.
- When there are a large number of devices on a network, the PC is recommended as the FTP server.

```
<Huawei> system-view
[Huawei] ftp server enable
[Huawei] aaa
[Huawei-aaa] local-user huawei password irreversible-cipher huawei@123
[Huawei-aaa] local-user huawei service-type ftp
[Huawei-aaa] local-user huawei ftp-directory flash:
[Huawei-aaa] local-user huawei privilege level 15
[Huawei-aaa] quit
[Huawei] quit
```

Contents

- 1. Overview of WLAN Troubleshooting**
 - General Troubleshooting Process
 - Common System Maintenance Methods
 - Common System Maintenance Commands
2. Troubleshooting APs' Failures to Go Online
3. Troubleshooting STAs' Failures to Go Online
4. Troubleshooting AP Signal Issues
5. Troubleshooting Slow Internet Access of STAs

display Commands

- The display commands are essential fault locating tools, so it is important that maintenance engineers master these commands. The display commands can be executed in any view and show the following information:
 - Current device status
 - Neighboring device information
 - Overall network information
 - Network fault location

Common display Commands (1/2)

| Item | Command | Description |
|------------------------------|--------------------------------|---|
| Basic information | display diagnostic-information | Displays basic system information, integrating the outputs of multiple common display commands, such as display version and display current-configuration . |
| Device information | display device | Displays the device status. If the status of a device is displayed as Abnormal , the device is faulty. |
| Interface information | display interface | Displays various interface information to help analyze the cause of interface interconnection failures and check statistics on lost packets. |
| Version information | display version | Displays versions of the system software, BootROM, MPUs, and fan modules, as well as sizes of storage devices. |
| Patch information | display patch-information | Displays current patch information, including the patch package version and name. |
| Electronic label information | display elabel | Displays electronic label information. Electronic labels identify information about hardware components of a device. |
| Device state information | display health | Displays the temperature, power supply, fan, power, CPU usage, memory usage, and storage medium usage of a device. |

Common display Commands (2/2)

| Item | Command | Description |
|------------------------------|---|---|
| Current system configuration | display current-configuration | Displays all configuration information on a device. You can specify a regular expression to obtain the required configuration information. |
| Saved configuration | display saved-configuration | Displays the startup configuration of a device. • To check the system configuration saved last time, run the display saved-configuration last command. • To check the last time when the system configuration is saved, run the display saved-configuration time command. |
| Time information | display clock | Displays the current system date and clock setting. |
| User log information | display logfile buffer (diagnostic view) | Displays user logs saved in the log buffer. |
| Diagnostic log information | display diag-logfile buffer (diagnostic view) | Displays diagnostic logs saved in the log buffer. |
| Alarm information | display trapbuffer | Displays information recorded in the trap buffer of the information center. |
| Memory usage | display memory-usage | Displays the memory usage of a device. |
| CPU usage | display cpu-usage | Displays the CPU usage of a device. |
| Running status of an AP | display ap run-info | Displays the running status of an AP. |
| AP status | display ap all | Displays the AP status. |
| Access user information | display access-user display station | Displays information about access users. |

reset Commands

- When you use the ping command to test link connectivity, you also need to run the display interface or display ip interface command to check whether packets are correctly sent and received on interfaces and whether there are CRC errors. Then you can locate the interface if a fault occurs. The display command output shows packet statistics generated after the device starts or the counter is reset; therefore, the packet statistics may contain unnecessary information that interferes with fault location.
- In this case, run the reset command to clear the statistics as required.
 - The display interface command shows counters to collect statistics about transmitted and received Layer 2 packets. The reset counters interface command resets these counters.
 - The display ip interface command shows counters to collect statistics on sent and received Layer 3 packets. The reset ip statistics command resets these counters.

Ping & Tracert

- The ping command is used to test network connectivity and device reachability.

```
ping [-a source-ip-address] [-c count] [-f] [-s packet-size] [-t timeout] host
```

- The tracert command is used to detect the gateways that packets pass through from the source to the destination, helping you check network connectivity and locate faulty nodes.

```
tracert [-a source-ip-address] [-f first-ttl] [-m max-ttl] [-q nqueries] [-w timeout] host
```

- During routine system maintenance, you can run the ping command to check network connectivity. If the ping operation fails, run the tracert command to locate the fault on the network.

- Parameter description of the ping command

- a: specifies the source IP address of the ICMP Echo Request message. If the source IP address is not specified, the IP address of the outbound interface is used as the source IP address of the ICMP Echo Request message.
- c: specifies the number of times for sending ICMP Echo Request messages. The default value is 5. If the network quality is poor, you can increase the parameter value to determine the network quality based on the packet loss rate.
- f: indicates that packets are not fragmented when they are sent. The device discards the packets if the packet size exceeds the MTU.
- s: specifies the length of an ICMP Echo Request message, excluding the IP header and ICMP header.
- t: specifies the timeout interval of ICMP Echo Reply messages. You can set a larger timeout interval if the network is unstable. The default value is 2 seconds. If the device receives no Echo Response message within 2 seconds, it determines that the destination is unreachable.
- host: specifies the domain name or IP address of the destination host.

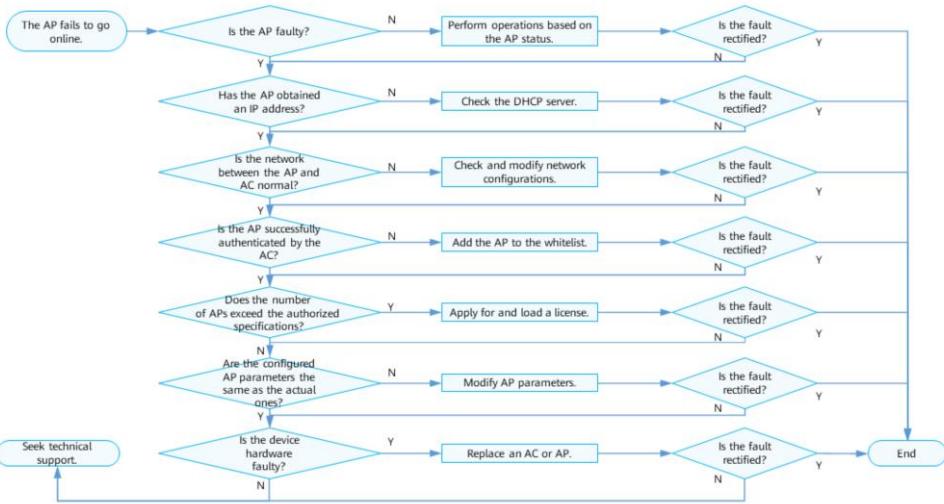
Contents

1. Overview of WLAN Troubleshooting
2. **Troubleshooting APs' Failures to Go Online**
3. Troubleshooting STAs' Failures to Go Online
4. Troubleshooting AP Signal Issues
5. Troubleshooting Slow Internet Access of STAs

Common Causes for an AP's Failure to Go Online

- The AP fails to obtain an IP address or obtains an incorrect IP address.
- The network between the AP and AC fails.
- The AP fails to be authenticated.
- The number of APs on an AC exceeds the AC's specifications.
- The AP is faulty.

Troubleshooting Process



Checking the AP Status

- Log in to the AC and run the display ap all command to check the AP status.

| <AC> display ap all | | | | | | | | |
|-----------------------|----------------|----------------|-------|-------------------------|----------|-------|-----|---------------|
| Total AP information: | | | | | | | | |
| ID | MAC | Name | Group | IP | Type | State | STA | Uptime |
| 0 | 60de-4476-e360 | L1_003 | | default 192.168.109.254 | AP7060DN | nor | 0 | 2D:5H:48M:44S |
| 1 | dcd2-fc04-b500 | dcd2-fc04-b500 | | default - | AP7060DN | idle | 0 | - |

Total: 2

- normal:** An AP is working properly.
- standby:** An AP is in normal state on the standby AC.
- idle:** It is the initialization state of an AP before it establishes a link with the AC for the first time.
- download:** An AP is in upgrade state.
- fault:** An AP fails to go online.

- commit-failed:** WLAN service configurations fail to be delivered to an AP after it goes online on an AC.
- config-failed:** WLAN service configurations fail to be delivered to the AP when the AP is going online on an AC.
- name-conflicted:** The name of an AP conflicts with that of an existing AP.
- xxx-mismatch:** The xxx parameter of an AP does not match that on the AC.
- unauth:** An AP fails to be authenticated.

- Common states of an AP include:

- normal: The AP has successfully registered with the AC.
- fault: The AP fails to register with the AC. If an AP is in fault state, go to the next check step.
- download: The AP is loading the system software during the upgrade. Wait until the AP upgrade is complete and check the AP status again.
- committing: The AC is delivering services to the AP.
- config-failed: The AP fails to initialize the configuration. If an AP is in config-failed state, check the network connectivity. Configure the AP and AC to ping each other. Check whether packet loss occurs and whether the MTU value is small on the intermediate network. If NAT traversal is configured on the intermediate network, check whether NAT communication is normal. Run the display cpu-defend statistics wired command to check the discarded CAPWAP packets in the statistics on packets sent to the CPU. If a large number of packets are lost, check whether the threshold is set properly. If the fault persists for a long time, collect related information and contact technical support.
- name-conflicted: The name of the AP conflicts with that of another AP. If an AP is in name-conflicted state, run the ap-rename ap-id ap-id new-name ap-name command in the WLAN view to change the AP name.
- ver-mismatch: The AP version does not match the AC version. If an AP is in ver-mismatch state, run the display ap version all command to check the AP version, and run the display version command to check the AC version. Check whether the AC version matches the AP version.
- standby: AP status on the standby AC.
- idle: After an AP is added offline, it is in idle state. If an AP is in this state, check

whether the AP is properly connected to the network.

Checking Whether the AP Is Faulty

- Observe the AP. Check whether the AP indicator blinks normally. If not, check whether the power cable and network cable are connected properly. If so, replace the AP.

| Information Type | Color | Indicator Status | Description |
|-------------------------------|-------|----------------------------------|--|
| Default status after power-on | Green | Steady on | The AP is just powered on and the software is not started yet. |
| Software startup status | Green | Steady on after blinking once | After the system is reset and starts uploading the software, the indicator blinks green once. Until the software is uploaded and started, the indicator remains steady green. |
| Running | Green | Blinking once every 2s (0.5 Hz) | <ul style="list-style-type: none">• The system is running properly, the Ethernet connection is normal, and STAs are associated with the AP.• The system enters the Uboot CLI. |
| | | Blinking once every 5s (0.2 Hz) | The system is running properly, the Ethernet connection is normal, and no STA is associated with the AP. The system is in low power consumption state. |
| Alarm | Green | Blinking once every 0.25s (4 Hz) | <ul style="list-style-type: none">• The software is being upgraded.• After the software is loaded and started, the AP requests to go online if it works in Fit AP mode (until the AP successfully goes online and a CAPWAP link is set up).• The AP works in Fit AP mode and fails to go online (CAPWAP link disconnection). |
| Fault | Red | Steady on | A fault that affects services has occurred, such as a DRAM detection failure or system software loading failure. The fault cannot be automatically rectified and must be rectified manually. |

Checking Whether the AP Has Obtained an IP Address (1/2)

- On the DHCP server, run commands to check whether the AP is assigned an IP address.
- Assuming that the AC serves as a DHCP server, run the `display ip pool` command to check allocated IP addresses. Determine whether the AP has obtained an IP address based on its MAC address. If so, ping the IP address.

```
<AC> display ip pool interface Vlanif1219 used | include dcd2-fc22-d880
Pool-name      : Vlanif1219
Pool-No       : 4
Lease        : 1 Days 0 Hours 0 Minutes
...
Network section :
-----
Index      IP          MAC        Lease   Status
-----
4090    10.1.15.251  dcd2-fc22-d880    9368  Used
-----
```

Checking Whether the AP Has Obtained an IP Address (2/2)

- If another device functions as a DHCP server, check whether the AP has obtained an IP address on the DHCP server.
- If the AP does not obtain an IP address, check whether the DHCP server and related device interfaces are correctly configured.
- If the AP fails to obtain an IP address, check whether:
 - The link between the AP and AC is properly connected.
 - The management VLAN is created on intermediate devices between the AP and AC.
 - All the interfaces between the AP and AC are correctly configured and allow packets of the management VLAN to pass through.
 - The Option 43 or Option 15 is configured in the IP address pool when the AP and AC are connected through a Layer 3 network.
 - The AP is powered on properly.

Checking Whether the AP Is Authenticated by the AC

- Run the `display ap global configuration` command on the AC to check the AP authentication mode.
- If MAC address or SN authentication is used, run the `display ap unauthorized record` command to check whether any AP fails to be authenticated.

```
<AC> display ap unauthorized record
```

Unauthorized AP record:

AP type: AP7110DN-AGN

AP SN: 210235555310D1000067

AP MAC address: **dcd2-fc22-d880** //The AP with MAC address dcd2-fc22-d880 is in the unauthorized AP list.

AP IP address: 10.1.7.251

Record time: 2019-11-17 10:36:43

Total number: 1

Run the `ap-confirm mac dcd2-fc22-d880` command to confirm unauthenticated APs.

Alternatively, run the `ap whitelist mac dcd2-fc22-d880` command to add the AP's MAC address to the whitelist.

Checking Whether the Number of AP Connections Exceeds the Threshold

- Run the `display license resource usage` command to check the current service capability set based on the keyword `resource usage`. If the number of normal APs reaches the capability set, new APs cannot go online. In this case, purchase a new license.

```
<AC> display license resource usage
Activated License: -
FeatureName | ConfigureItemName | ResourceUsage
CRFEA1      LH85WLANAP00      4/4
```

- The number of APs that can be connected to an AC depends on the following factors:
 - License resource items: The total number of common APs and central APs cannot exceed the number of license resource items. RUs do not occupy license resources.
 - Maximum number of APs that can be managed by an AC:
 - The total number of common APs and RUs cannot exceed the maximum number that can be managed by an AC.
 - The total number of central APs does not exceed the maximum number that can be managed by an AC.

Checking CAPWAP Link Information

- Log in to the AP and run the display capwap link all command in the diagnostic view.

```
[AP-diagnose] display capwap link all
```

Info: This operation may take a few seconds. Please wait for a moment.done.

| ID | MAC | CPort | DPort | Type | State | Role | VPN | DstAddr | SrcAddr |
|----|----------------|-------|-------|-------|-------|----------|----------|-------------|--------------|
| 0 | 7079-90ba-8ea0 | 5246 | 5247 | AC | RUN | Client - | | 120.120.1.1 | 120.120.5.60 |
| 1 | 7079-90ba-8ea0 | 5246 | 5247 | AC | RUN | Client - | | 120.120.1.2 | 120.120.5.60 |
| 2 | 4cfa-caff-f560 | | 55450 | 65535 | INAP | RUN | Server - | 120.120.7.6 | 120.120.5.60 |

- Pay attention to the link whose DstAddr is the CAPWAP source address of the destination AC.

- If information about the CAPWAP link to the destination AC does not exist, check the status of other links whose Type is AC.
- If there is such a link and the status is RUN, the AP goes online on another AC. You can locate the AC based on DstAddr.

Common Causes for APs to Go Offline

- A common cause for an AP to go offline is heartbeat timeout. To find out the specific cause, run the display ap offline-record command or collect AC logs.
- The method for locating this fault is the same as that for locating the cause for an AP's failure to go online.

```
<AC> display ap offline-record all
```

| MAC | Last offline time | Reason |
|----------------|---------------------|-----------------------------------|
| 0023-0024-0080 | 2015-01-31/16:21:50 | Reboot by ap-reset command |
| 60de-4476-e360 | 2015-01-31/14:02:35 | Reboot by ap update reset command |
| 1047-80b1-56a0 | 2015-01-31/13:52:35 | Echo timeout |

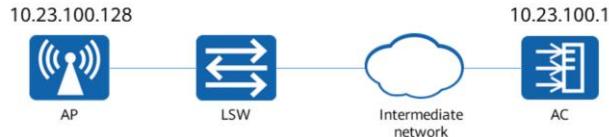
Total records: 3

Common heartbeat timeout causes are as follows:

- The AP is powered off, which can be found in the AP restart reason.
- The network between the AP and AC is unstable or a loop occurs. (For example, the AP goes offline and online repeatedly.)
- The AP is faulty and does not send packets, and the switch cannot learn the AP's MAC address.
- The power supply of the AP is insufficient, and the negotiated rate of the peer port is incorrect.

Case: An Exception on the Intermediate Network Leads to an Abnormal AP Status (1/2)

- Networking information



- Symptom

- The AP and AC can ping each other.
 - The AP status is cfg-failed or cmt-failed in the display ap all command output.

Case: An Exception on the Intermediate Network Leads to an Abnormal AP Status (2/2)

- Troubleshooting procedure

- Run the display ap all command to query the AP status. If the AP status is cfg-failed or cmt-failed, the AP fails to go online. config-failed indicates that the AP initialization configuration fails, and commit-failed indicates that the service configuration fails to be committed. In this case, check network connectivity between the AP and AC.
- Ping the IP address of the AP from the AC. The ping operation succeeds. However, the ping with large packets fails.

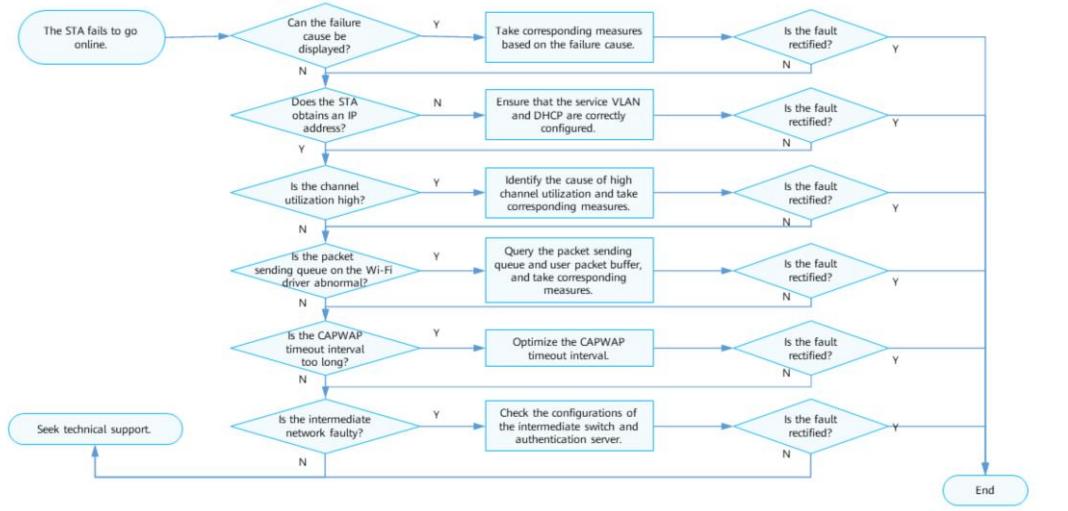
```
<AC> ping -s 1500 10.23.100.128
```
- Perform a ping test segment by segment using the dichotomy to check whether an intermediate node fails to be pinged. The recommended method is to check whether MTU discarding is configured on an intermediate node. If so, check whether the intermediate network can allow packets whose length exceeds the MTU to pass through.
- The customer cannot change the MTU of an intermediate node. Therefore, change the MTU to a smaller value on the AC's CAPWAP interface.

```
[AC-Vlanif110] mtu 1000 //Changing the MTU value does not affect services on the live network.
```

Contents

1. Overview of WLAN Troubleshooting
2. Troubleshooting APs' Failures to Go Online
- 3. Troubleshooting STAs' Failures to Go Online**
4. Troubleshooting AP Signal Issues
5. Troubleshooting Slow Internet Access of STAs

Troubleshooting Process



Checking Causes for a STA's Failure to Go Online (1/2)

- Run the display station online-fail-record sta-mac sta-mac command to check causes for the STA's failure to go online.

```
[AC-wlan-view] display station online-fail-record sta-mac f06b-ca63-313d
```

| STA MAC | AP ID | Ap name | Rf/WLAN | Last record time | Reason |
|----------------|-------|---------|---------|---------------------|------------------------------------|
| f06b-ca63-313d | 2 | ap-10 | 0/1 | 2020-07-03/19:05:12 | The STA is in the VAP's blacklist. |

Total stations: 1 Total records: 1

- Rectify the fault based on the specific cause.

Common Causes for a STA's Failure to Go Online

| Cause | Handling Suggestion |
|---|--|
| The STA is in the global blacklist. | <ul style="list-style-type: none">Run the display sta-blacklist-profile command to check information about STAs in the blacklist.Run the undo sta-mac mac-address command to delete the STA from the blacklist. |
| The STA is in the dynamic blacklist. | Run the display wlan ids dynamic-blacklist all command to view attack records and check whether the STA initiates attacks. |
| Access from legacy STAs is denied. | Run the undo legacy-station disable command in the SSID profile view. |
| The STA uses a static IP address. | Check whether the STA uses a static IP address. Unless otherwise specified, configure the STA to obtain an IP address dynamically. |
| Authentication fails. | Enter the correct WLAN key on the STA and attempt to access the WLAN again. |
| The number of STAs exceeds the physical specifications allowed by the AP. | Expand the network capacity or retain the current configuration as required. |
| The STA associates with a heavily loaded radio. | <ul style="list-style-type: none">Run the display sta-load-balance static-group command to check load balancing information.In static load balancing profile mode, run the gap-threshold command to adjust the load balancing threshold.Alternatively, run the undo sta-load-balance static-group command to disable the load balancing function. |

Checking Causes for a STA's Failure to Go Online (2/2)

- If the fault cause cannot be located, perform the following steps to rectify the fault:
 - If the STA fails to obtain an IP address, check the IP address, VLAN, and DHCP configurations, and the link between the STA and the DHCP server.
 - Run the `display vap` command to check whether the SSID of the VAP contains special characters.
 - Run the `display radio ap-id 0` command to check whether the AP radio channel utilization is high.

Case: STAs Fail to Associate with an AP Because the Number of STAs Associated with the AP Reaches the Upper Limit (1/3)

- Symptom
 - A STA cannot go online.
 - According to the display station online-fail-record command output, the cause is The number of STAs exceeds the maximum allowed in the VAP reported by the AP.
- Fault analysis
 - The number of STAs associated with the target VAP has reached the upper limit, and new STAs cannot be associated with the VAP.
 - More STAs associated with a VAP or AP indicate fewer network resources available to each STA. To ensure Internet access experience for users, set a proper maximum number of STAs that can be associated with a VAP or AP. When the number of STAs associated with a VAP or AP reaches the maximum, new STAs cannot connect to the network.

Case: STAs Fail to Associate with an AP Because the Number of STAs Associated with the AP Reaches the Upper Limit (2/3)

- Troubleshooting procedure

- Check the number of associated STAs.

```
<huawei> display station ap-id 0
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-----
STA MAC      Rf/WLAN  Band Type Rx/Tx  RSSI VLAN IP address   SSID
-----
14cf-9208-9abf    0/2       2.4G 11n  3/8   -70  10      10.10.10.253  tap1
...
Total: 32 2.4G: 20 5G: 12 //A total of 32 STAs are associated with AP 0.
```

- Check the maximum number of STAs supported by the AP in the product description of the corresponding AP model. Check whether the actual number of STAs connected to the AP reaches the maximum value. If so, expand the network capacity.

Case: STAs Fail to Associate with an AP Because the Number of STAs Associated with the AP Reaches the Upper Limit (3/3)

- If not, adjust the maximum number of STAs that can be associated with the VAP.

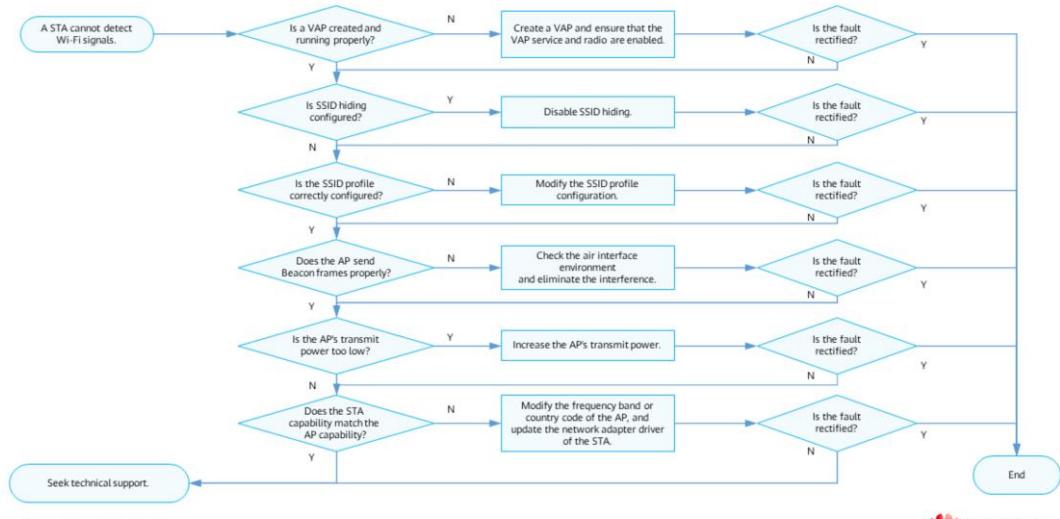
```
<huawei> display ssid-profile name ssid-0
...
SSID hide : disable
Association timeout(min) : 5
Max STA number : 32 //A maximum of 32 STAs can associate with a VAP.
Reach max STA SSID hide : enable
Legacy station : disable
...
<huawei> system-view
[huawei] wlan
[huawei-wlan-view] ssid-profile name ssid-0
[huawei-wlan-ssid-prof-ssid-0]max-sta-number 70 //Set the maximum number of STAs associated with a VAP to 70.
```

- To ensure proper service running, it is recommended that a maximum of 30 STAs associate with a single-band AP, and a maximum of 50 STAs associate with a dual-band AP.

Contents

1. Overview of WLAN Troubleshooting
2. Troubleshooting APs' Failures to Go Online
3. Troubleshooting STAs' Failures to Go Online
- 4. Troubleshooting AP Signal Issues**
 - No Signal for STAs
 - Weak Signals for STAs
5. Troubleshooting Slow Internet Access of STAs

Troubleshooting Process



492 Huawei Confidential

 HUAWEI

Checking Whether the VAP Status Is Normal

- Ensure that the AP is online and run the display vap command to check the VAP status.

```
[AC-wlan-view] display vap ap-id 4 radio 0
WID : WLAN ID
-----
AP ID AP name      RfID WID   BSSID      Status Auth type STA   SSID
4    9c50-ee45-6cc0 0  1  9C50-EE45-6CC0 ON   Open    0   HUAWEI-WLAN
-----
Total: 1
```

- For a normally created VAP, the value of the BSSID field is not all 0s. For a working VAP, the value of the Status field is ON.
- If the VAP fails to be created, run the display vap create-fail-record all command to check the cause for the VAP creation failure and rectify the fault.
- If the VAP is correctly bound to the radio but the value of the BSSID field is all 0s, the configuration fails to be delivered.
- If the BSSID is displayed normally but the Status field displays OFF, the configuration may be incorrect. For example, the radio or the VAP is disabled.

Checking the SSID Hiding Configuration (1/2)

- If SSID hiding is configured, STAs cannot detect signals. The following methods can be used to hide SSIDs:

- Hide the SSID in a VAP.

```
<AC> display ssid-profile name default
```

```
-----  
Profile ID          : 0  
SSID               : HUAWEI-WLAN  
SSID hide          : disable  
Association timeout(min) : 5  
Max STA number    : 64  
Action upon reaching the max STA number: SSID hide
```

- Run the undo ssid-hide enable and reach-max-sta hide-ssid disable commands in the SSID profile view to disable SSID hiding and automatic SSID hiding when the number of access STAs reaches the maximum.

Checking the SSID Hiding Configuration (2/2)

- When the number of access STAs on a radio reaches the maximum, the SSID is automatically hidden. Check whether this configuration is enabled in the RRM profile of the radio.

```
<AC> display rrm-profile name default
```

```
.....  
UAC channel utilization access threshold(%) : 80  
UAC channel utilization roam threshold(%) : 80  
UAC hide SSID : enable  
.....
```

- Run the undo uac reach-access-threshold command in the RRM profile view to disable automatic SSID hiding when the number of access STAs on a radio reaches the configured threshold.

Checking the SSID Profile Configuration

- Check the SSID profile bound to the VAP profile.

```
<AC> display vap-profile name VAP-Profile-Name
```

```
.....  
SSID profile :guest  
.....
```

- Configure an SSID in the SSID profile.

```
[AC-wlan-view] ssid-profile name guest  
[AC-wlan-ssid-prof-ssid1] ssid mySSID  
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Checking Beacon Frames Sent by an AP

- SSID information contained in wireless signals is carried in Beacon frames sent by APs. If an AP does not send Beacon frames, STAs cannot detect the corresponding signals.

```
[AP-1-diagnose] display Wi-Fi radio-statistics radio 0
```

```
.....
```

```
[Beacon]
```

| | | |
|-------------|---|-------|
| Transmitted | : | 41663 |
| Missed | : | 13427 |

```
.....
```

- If the number of Missed Beacon frames is greater than that of Transmitted Beacon frames, STAs cannot detect signals.
- Beacon frames are lost because the air interface is busy and the AP cannot compete for the time to send packets.
- Run the display ap traffic statistics wireless command to check the channel utilization and noise floor in the current environment.

Checking Interference in the Air Interface Environment (1/2)

- Channel utilization is a key factor representing the air interface status. If the service volume on an AP is small but the channel utilization is high, interference is severe on the air interface.
- Check the interference rate on the AP.

```
[AP-diagnose] display Wi-Fi base-info radio 0
```

```
.....
```

```
CoChanInterferenceRate(%) = 46
```

- Check whether other interference exists in the surrounding environment. In most cases, you need to use scanning software to scan the surrounding air interface environment. Common scanning tools include WirelessMon, inSSIDer, and Network Stumbler. The WiFi Analyzer software is available on Android phones.
- Based on the scanning result, other Wi-Fi signals on the working channel can be detected. If there are many such Wi-Fi signals, the working signal is interfered. In this case, change the working channel of the AP to one with less interference.

Checking Interference in the Air Interface Environment (2/2)

- In addition to the interference caused by other Wi-Fi devices, devices that work on the same or similar frequency band as the AP may cause non-Wi-Fi interference.
- APs can work on 2.4 GHz and 5 GHz frequency bands.
 - The 2.4 GHz frequency band is the Industrial, Scientific, and Medical (ISM) open frequency band. Interference sources on the 2.4 GHz frequency band include cordless phones, microwave ovens, wireless cameras, Bluetooth devices, infrared sensors, and fluorescent light ballasts.
 - The 5 GHz frequency band has fewer interference sources than the 2.4 GHz frequency band. More and more devices begin to work on the 5 GHz frequency band, such as cordless phones, radars, wireless sensors, and digital satellites.
- These non-Wi-Fi interference sources have great impact on AP services, and are difficult to identify. In most cases, spectrum analyzers and dedicated tools can be used to identify non-Wi-Fi interference sources.

Checking the AP's Transmit Power

- By default, automatic power calibration is enabled on an AP. To manually adjust the transmit power, disable this function.
- Set the transmit power to a small value that is enough for STAs to detect signals. This is because a high transmit power value may cause interference to other APs.

```
[AC-wlan-view] ap-id 1  
[AC-wlan-ap-1] radio 0  
[AC-wlan-radio-1/0] calibrate auto-tpower-select disable  
[AC-wlan-radio-1/0] eirp 127
```

- To check the AP's transmit power, run the display radio command.

```
<AC> display radio ap-id 1
```

| AP ID | Name | RfID | Band | Type | Status | CH/BW | CE/ME | STA | CU |
|-------|----------------|------|------|------|--------|-------|-------|-----|-----|
| 1 | 9c50-ee45-6dc0 | 0 | 2.4G | bgn | on | 6/20M | 11/32 | 0 | 39% |

Contents

1. Overview of WLAN Troubleshooting
2. Troubleshooting APs' Failures to Go Online
3. Troubleshooting STAs' Failures to Go Online
- 4. Troubleshooting AP Signal Issues**
 - No Signal for STAs
 - Weak Signals for STAs
5. Troubleshooting Slow Internet Access of STAs

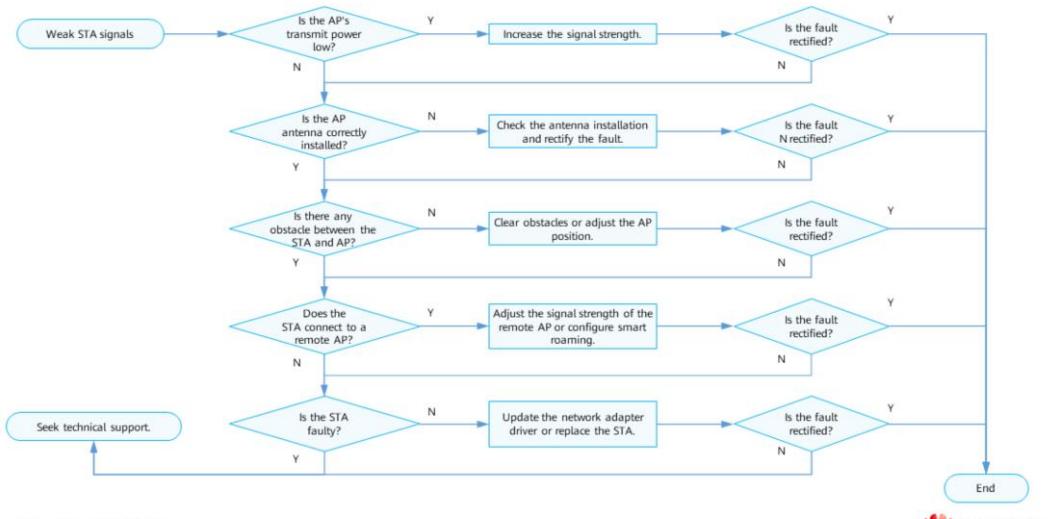
Common Causes for Weak Wi-Fi Signals

- The actual transmit power of an AP is low.
- The external antennas of an AP are not properly fastened or not installed.
- There are obstacles, such as walls and folding screens, between the STA and AP.
- The STA is connected to a remote AP.
- The STA is faulty.

Reference Signal Attenuation of Typical Obstacles

| Obstacle | Thickness (mm) | 2.4 GHz Signal Attenuation (dB) | 5 GHz Signal Attenuation (dB) |
|---------------------|----------------|---------------------------------|-------------------------------|
| Synthetic material | 20 | 2 | 3 |
| Asbestos | 8 | 3 | 4 |
| Wooden door | 40 | 3 | 4 |
| Glass window | 50 | 4 | 7 |
| Thick colored glass | 80 | 8 | 10 |
| Brick wall | 120 | 10 | 20 |
| Brick wall | 240 | 15 | 25 |
| Armored glass | 120 | 25 | 35 |
| Concrete wall | 240 | 25 | 30 |
| Metal | 80 | 30 | 35 |

Troubleshooting Process

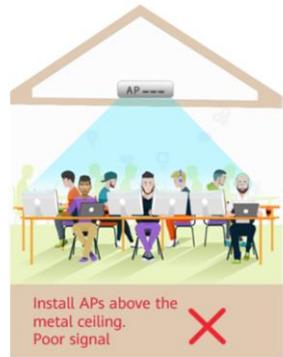


Weak AP Signals Caused by Obstacles in the Surrounding Environment

- Symptom
 - The AP antenna or STA is severely blocked by trees or walls.
 - Possible cause
 - The signal path loss is large due to obstacles such as trees and walls around the AP antenna.
 - There is interference from devices such as microwave ovens, wireless mouses, and wireless headsets around the STA, and the STA cannot directly "see" the AP antenna.
 - Troubleshooting procedure
 - Clean the obstacles around the AP antenna and properly place the AP antenna.
 - Check the interference and obstacles around the STA, and place the STA in an ideal position.

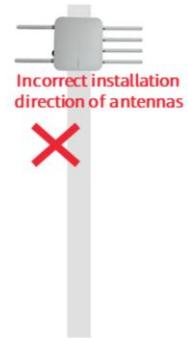
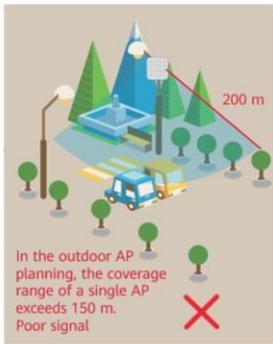
Common Installation Problems That Affect Wi-Fi Signals (Indoor)

- When installing an AP, try to reduce the number of obstacles (especially metal obstacles) that signals pass through.



Common Installation Problems That Affect Wi-Fi Signals (Outdoor)

- Deploy APs far away from interference sources and directly face the network coverage area to ensure that the signal strength in each area meets user requirements and to minimize co-channel interference between neighboring APs.



Weak AP Signals Due to Poor STA Performance

- Symptom
 - Some STAs receive weak AP signals, while other STAs do not have this problem.
 - Possible cause
 - STA performance is low.
 - Troubleshooting procedure
 - Compare the test results of the same STA under different antenna angles, for example, placing a laptop's front or rear facing the antenna, to find the optimal angle of the wireless network adapter antenna of the laptop.
 - Replace the laptop or use an external network adapter. Generally, the performance of the built-in network adapter on a laptop is poorer than that of an external network adapter, and varies greatly depending on laptop models. You are advised to use multiple laptops for comparison tests.

Contents

1. Overview of WLAN Troubleshooting
2. Troubleshooting APs' Failures to Go Online
3. Troubleshooting STAs' Failures to Go Online
4. Troubleshooting AP Signal Issues
- 5. Troubleshooting Slow Internet Access of STAs**

Troubleshooting Roadmap

- Check whether the fault occurs on the wired or wireless side.

| Wireless Side | Wired Side |
|---|---|
| Check whether VLANs are configured correctly. | Check whether ARP packets are lost on the intermediate network. |
| Check whether the AP's channel utilization is normal. | Check whether a loop occurs on the network. |
| Check whether the AP's packet buffer resources and packet sending queue are normal. | Check whether the AP's CPU usage is normal. |
| Check whether the signal strength of the AP is normal. | Check whether the AP's IP address conflicts. |
| Check whether packet loss occurs on the AP. | |
| Check whether there is heavy traffic of services from low-rate STAs. | |

Case: Slow Internet Access Due to Poor Signal Quality

- Symptom
 - The signal strength of the STA is lower than -65 dBm.
- Possible cause
 - The STA is far away from the AP.
 - Obstacles exist between the STA and AP antenna.
 - The AP antenna is not properly installed.
 - The AP's transmit power is not the maximum.
 - Troubleshooting procedure
 - Refer to the method for handling poor AP signals.

Case: Slow Internet Access Due to Co-Channel Interference

- Symptom
 - At a site, two APs work on the same channel, and the difference between their signal strengths is within 20 dBm.
- Possible cause
 - Services are performed concurrently on two APs working on the same channel, leading to co-channel interference. As a result, the service quality cannot be guaranteed.
- Troubleshooting procedure
 - Check the AP's channel to determine whether co-channel and adjacent-channel interference exists.
 - Check whether hidden nodes exist between APs.
 - Check whether other Wi-Fi interference exists.

512 Huawei Confidential



- As shown in the figure, two AP signals are found on channel 1 and have similar strengths. When the two APs have concurrent services, co-channel interference occurs, degrading service quality.

| SSID | SIGNAL ▼ | CHANNEL | SECURITY | MAC ADDRESS |
|------------|----------|---------|--------------|-------------------|
| ChinaNet | | 6 | Open | 06:1F:6F:32:0C:0F |
| | | 6 | WPA-Personal | 00:1F:6F:32:0C:0F |
| CMCC-EDU | | 1 | Open | 10:47:80:C6:70:F0 |
| ★ CMCC-EDU | | 1 | Open | 10:47:80:C6:08:A0 |
| CMCC-EDU | | 11 | Open | 10:47:80:C6:08:D0 |
| CMCC-EDU | | 6 | Open | 10:47:80:C6:08:E0 |
| CMCC-EDU | | 11 | Open | 10:47:80:C6:08:B0 |
| ChinaNet | | 1 | Open | 06:1F:6F:32:0C:37 |
| ChinaNet | | 1 | Open | 06:1F:6F:32:0B:12 |
| | | 1 | WPA-Personal | 00:1F:6F:32:0B:12 |
| CMCC-EDU | | 11 | Open | 10:47:80:C6:71:00 |

Quiz

1. (Single Choice) Which of the following commands is used to query the cause for a STA's failure to go online?
 - A. display ap online-fail-record
 - B. display vap create-fail-record
 - C. display station offline-record
 - D. display station online-fail-record

Quiz

2. (Multi-Answer Question) Which of the following symptoms may occur on an AP that is interfered by air interface signals?
 - A. Low transmit power
 - B. High channel utilization
 - C. High noise floor
 - D. A large number of Missed Beacon frames

- BCD

Summary

- This course describes the basic WLAN troubleshooting process and common troubleshooting commands.
- We also go through how to troubleshoot typical WLAN faults, such as APs' and STAs' failures to go online and signal interference issues.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



WLAN Antenna Technology



Foreword

- WLAN signals are transmitted in the air as radio waves. Antennas are used to transmit and receive radio waves and play an important role in WLAN.
- This course describes the fundamentals, typical parameters, and model selection of WLAN antennas.

Objectives

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

- Describe the definition, functions, and classification of antennas.
- Understand the fundamentals and key performance indicators of antennas.
- Distinguish parameters of different antennas.

Contents

- 1. Antenna Overview**
2. Concepts Related to Antennas
3. Antenna Selection
4. Traditional Indoor Distribution System

Antenna Overview

- An antenna is an essential component for all wireless devices, covering radiotelegram, broadcast, walkie-talkie, television, microwave, satellite communication, wireless communication, and so on.



Transceiver antenna



Radio antenna



TV antenna



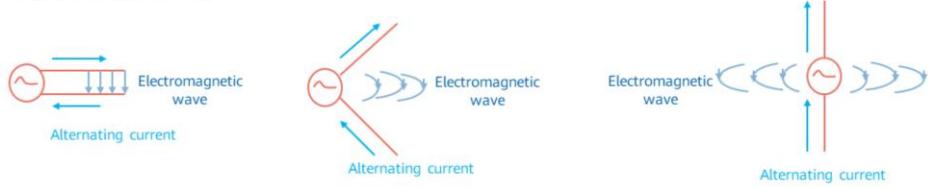
Yagi digital TV antenna



Satellite antenna

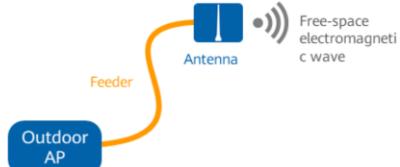
Basic Concepts of Wireless Communication Signals

- Wireless communication at anytime, anywhere requires a communication medium that is available at anytime, anywhere is required. Radio waves are electromagnetic waves that can be propagated in the space.
- Radio frequency (RF) signal is an electromagnetic wave that radiates through the space in the frequency range from 300 kHz to 300 GHz. The term microwave is applied to radiation of frequency from 300 MHz to 300 GHz. A wireless communications system uses RF transmission.
- When the two conducting wires are close to each other, the electric field is limited between them and the radiation is weak. When two conducting wires are far away from each other, the electric field is enlarged and the radiation is enhanced.



- Baseband signal is an original analog or digital signal that is sent from a signal source and has not been modulated. For example, sound waves emitted by people are analog baseband signals, and signals from computers to peripherals such as monitors and printers are baseband signals. The baseband signal has the following characteristics: 1. low frequency; 2. poor anti-interference performance; 3. suitable for short-distance transmission.
- Intermediate frequency (IF): In the traditional modulation and demodulation mode, baseband signals are converted into IF signals before being converted into RF signals, or received RF signals are also converted into IF signals before being converted into baseband (I, Q) signals.
- Zero-IF (ZIF) is a modulation and demodulation method of directly converting between RF signals and baseband signals without using IF signals.

Antenna Definition and Implementation

| Antenna definition | Antenna implementation |
|--|---|
| <p>An antenna is a transducer designed to radiate or receive electromagnetic waves in a specific direction. It is a component of a radio device to convert electrical power into electromagnetic waves and vice versa.</p>  | <ul style="list-style-type: none">• Antenna functions:<ul style="list-style-type: none">◦ Converts energy, that is, between guided waves and free-space waves, and between high-frequency current and electromagnetic waves.◦ Radiates and receives electromagnetic waves in certain directions.• An antenna converts between guided waves on transmission lines into electromagnetic waves propagated in unbounded media (free space in most cases), or vice versa.• Radio signals transmitted by an outdoor AP are received by the AP's antenna through a feeder (a type of RF cable) and then radiated by the antenna in the form of electromagnetic waves. Electromagnetic waves are received by the antenna of an AP and then sent to the AP through a feeder.• Generally, an antenna can be used for both transmitting and receiving electromagnetic waves.• Antenna reciprocity theorem: Reciprocity states that the receive and transmit properties of an antenna are identical. |

524 Huawei Confidential



- Guided waves refer to the electromagnetic waves transmitted along a transmission line in a certain direction. Typical guided waves are the waves transmitted along parallel lines or coaxial feeders, waves transmitted along waveguides, and waves transmitted along the ground from the transmitter to the receiver.
- Free-space waves refer to the electromagnetic waves transmitted in free space.

Antenna Classification

| Antenna classification |
|---|
| • By radiation direction: |
| ▫ Omnidirectional antenna, directional antenna, and smart antenna |
| • By polarization: |
| ▫ Single-polarized antenna and dual-polarized antenna |
| • By appearance: |
| ▫ Whip antenna and plate antenna |
| • By location: |
| ▫ External antenna and built-in antenna |



525 Huawei Confidential

 HUAWEI

- Omnidirectional antenna:
 - An omnidirectional antenna radiates equal energy in all directions on the horizontal plane and radiates different energy in different directions on the vertical plane.
 - The radiation pattern of an omnidirectional antenna is similar to that of an incandescent lamp, which radiates visible light in all directions on the horizontal plane.
- Directional antenna:
 - A directional antenna radiates energy more effectively in one direction than in others on the horizontal and vertical planes.
 - The radiation pattern of a directional antenna is similar to that of a flashlight, which radiates visible light towards a certain direction. With the same radio energy, a directional antenna provides a longer coverage distance than an omnidirectional antenna in a particular direction.
- Smart antenna:
 - A smart antenna is an array of low-gain antennas that have the same polarization and are arranged and activated in a certain order. Based on the wave interference theory, they provide radiation patterns with high directivity and form the beams in expected directions. A smart antenna has multiple directional radiation patterns and one omnidirectional radiation pattern on the horizontal plane.
 - A smart antenna receives signals from transmitters in the omnidirectional pattern. The smart antenna algorithm can determine the location of a transmitter based on the received signals, and control the CPU to send control signals to the transmitter in a directional radiation pattern with the direction of the maximum radiation.

Common WLAN Antennas

- Indoor ceiling-mount antennas are light, good-looking, and easy to install.



Ceiling-mount antenna

- Indoor wall-mount antennas have similar advantages to those of indoor ceiling-mount antennas.



Indoor directional antenna

- Outdoor antennas are the most important part in an outdoor WLAN project. Antenna types decide whether signals can be stably transmitted in a long distance.



2.4G&5G outdoor omnidirectional antenna



Outdoor backhaul antenna

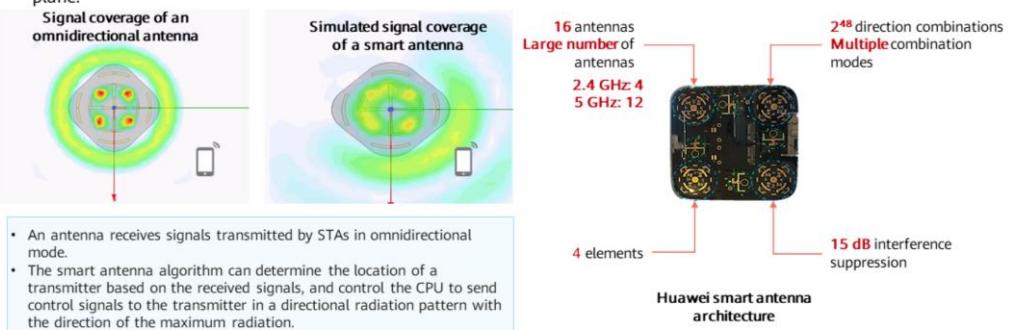


2.4G&5G outdoor directional antenna

- Indoor ceiling-mount antennas are light, good-looking, and easy to install, and have a low gain (about 2 to 5 dBi). Such antennas are usually deployed in an indoor distribution system. They are mounted on the ceiling or joists and connect to signal sources through feeders.
- Indoor wall-mount antennas have similar advantages to those of indoor ceiling-mount antenna, and have a gain of about 5 to 8 dBi. Such antennas are usually deployed in an indoor distribution system or directly connect to signal sources to provide directional coverage.
- Outdoor antennas are the most important part in an outdoor WLAN project. Antenna types decide whether signals can be stably transmitted in a long distance. When selecting antenna types, consider the antenna's coverage range and angle. For a short coverage range, low-gain omnidirectional or directional antennas are recommended. For a long coverage range, high-gain directional antennas are recommended. For outdoor long-distance point-to-point transmission, high-gain small-angle antennas are recommended.
- Directional antennas can provide a high gain. Generally, an antenna with a smaller angle provides a higher gain and therefore supports a longer signal transmission distance. However, such antennas are difficult to install and adjust. They must be properly aligned to each other on the transmitter and receiver to ensure efficient signal transmission. Therefore, such antennas are suitable for long-distance transmission but must be properly placed.

Smart Antenna

- A smart antenna is an array of low-gain antennas that have the same polarization and are arranged and activated in a certain order. Based on the wave interference theory, they provide radiation patterns with high directivity and form the beams in expected directions.
- A smart antenna has multiple directional radiation patterns and one omnidirectional radiation pattern on the horizontal plane.



528 Huawei Confidential

 HUAWEI

- Advantages of smart antennas:

- Large coverage area: Smart antennas bring centralized energy and high gain, providing a large coverage range. The coverage range of a smart omnidirectional antenna is equivalent to that of a directional antenna.
- High anti-interference capability: A smart antenna directs signals to a certain direction to form directional beams. The main lobe points to the direction of arrival (DOA) of usable signals, and side lobes and nulls point to the DOA of interference signals.
- Low pollution to the environment: A smart antenna provides satisfied power for STAs using low transmit power. This reduces the electromagnetic wave pollution to the environment.

Contents

1. Antenna Overview
- 2. Concepts Related to Antennas**
3. Antenna Selection
4. Traditional Indoor Distribution System

Concepts Related to Antennas

Antenna fundamentals

Half-wave dipole

Directivity

Polarization

Typical antenna parameters

Antenna gain

Transmit power

Beamwidth

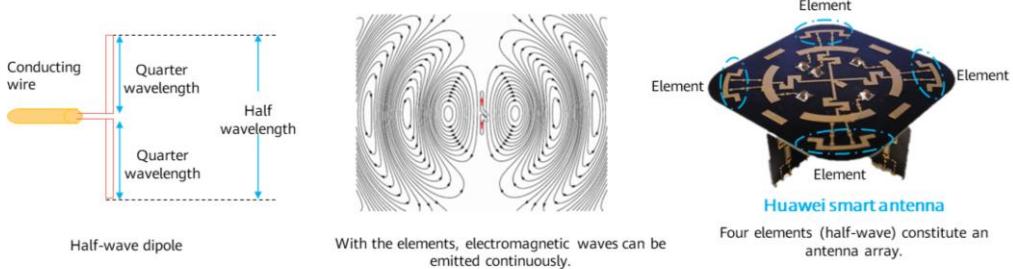
Front-to-back ratio (FBR) of a directional antenna

Downtilt

Operating frequency range (frequency bandwidth)

Half-Wave Dipole

- A half-wave dipole consists of two quarter-wavelength conductors placed end to end for a total length of approximately $L = \lambda/2$. Half-wave dipoles (or elements) are the basic units of an antenna.
- Electromagnetic waves are radiated by a conducting wire by transmitting alternating current. The radiation capability is determined by the length and shape of the conducting wire.
- A group of elements can constitute an antenna array. That is, a smart antenna is an array of elements.



531 Huawei Confidential

HUAWEI

- An element with the arms of the same length is called a symmetric element. A half-wave symmetric element has a length of $1/4$ wavelength and a full length of $1/2$ wavelength on each arm.
- Half-wave symmetric elements can be used independently or as the feed source of a parabolic antenna. In addition, multiple half-wave symmetric elements can constitute an antenna array.
- When the two conducting wires are close to each other, the electric field is limited between them and the radiation is weak. When two conducting wires are far away from each other, the electric field is enlarged and the radiation is enhanced.
- When the two conducting wires are too close to each other and form a straight line, they become an antenna.
- When the wire length is $1/4$ of the signal wavelength, the radiation is the maximum, which is called the basic element.
- When the two conducting wires are charged, an electric field is produced between the two poles. A magnetic field is produced when current flows between the metal bodies.
- When the two conducting wires are slightly farther from each other, an electric field and a magnetic field will be produced in the space around the metal bodies.
- If the conducting wires form a straight line, an electromagnetic field is produced outside the wires.
- When the length of a conducting wire (L) is far smaller than the wavelength (λ), the radiation is weak. When the conducting wire length is almost the same as the wavelength, current on the conducting wire greatly increases, producing strong radiation. Such straight conducting wire that can produce strong radiation is called element.

Antenna Directivity (1/3)

Antenna directivity

Antenna directivity indicates the capability of antennas radiating electromagnetic waves to a certain direction. For RX antennas, the directivity indicates the capability of receiving electromagnetic waves from different directions. An antenna can transmit waves to different directions or receive waves from different directions.



Directional antenna
(external)

- A directional antenna has one or more directions of maximum radiation on the horizontal plane.
- Directional antennas radiate or receive radio waves more effectively in certain directions. Therefore, they concentrate energy and are suitable for long-distance communication.
- Directional antennas have strong anti-interference capabilities.



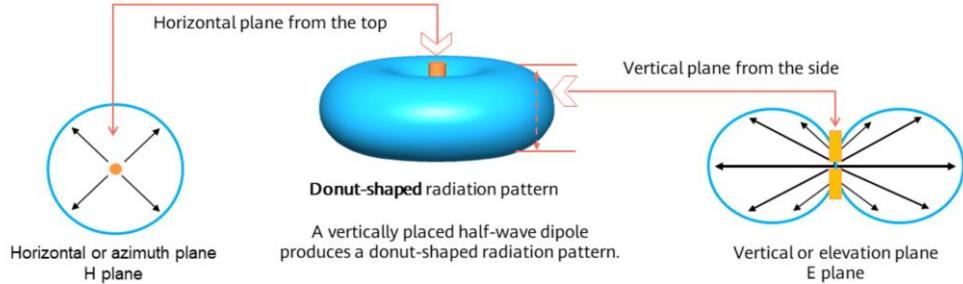
Omnidirectional
antenna (external)

- An omnidirectional antenna does not have the direction of maximum radiation on the horizontal plane.
- Omnidirectional antennas are undirectional, so they are usually used for point-to-multipoint communication.

Antenna Directivity (2/3)

Antenna radiation pattern

- A planar pattern shows an antenna's directivity on a specified plane.
- An antenna pattern shows the antenna's capability of radiating or receiving electromagnetic waves in each direction.
- The energy radiated in the axis direction of an element is zero, and the direction of maximum radiation is on the horizontal plane. An antenna has equal radiation in all directions on the horizontal plane.



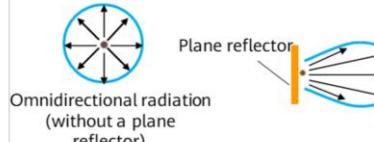
Antenna Directivity (3/3)

A flatter donut-shaped radiation pattern indicates higher-level signal concentration.



When the donut-shaped radiation pattern of an antenna becomes flatter, signals are more concentrated, the radiation capability in a specific direction becomes stronger, while the radiation capability in other directions gets weaker.

For a directional antenna, the reflector reflects electromagnetic waves to one side to enhance the gain.

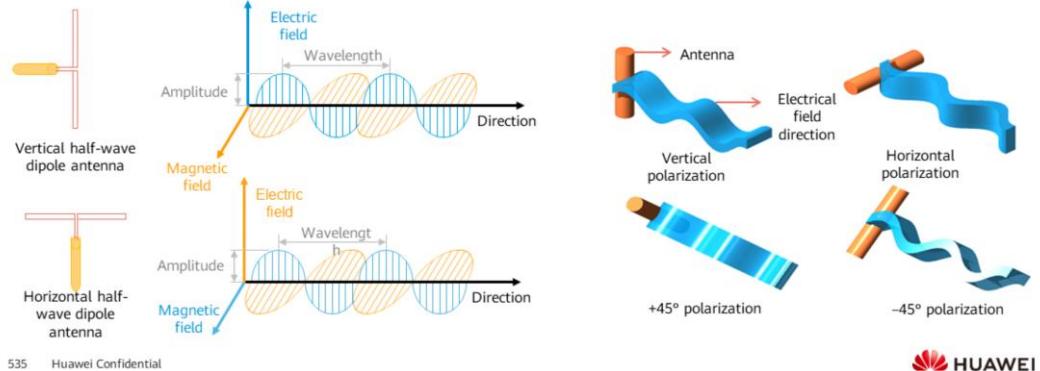


Plane reflector
Directional enhancement
(with a plane reflector)

- The reflector reflects power to one side, enhancing the gain.
- Parabolic reflectors are used to concentrate energy within a small solid angle to enhance the gain.
- A parabolic antenna consists of a paraboloid reflector and a radiation source placed in the focus of the parabola.

Antenna Polarization (1/3)

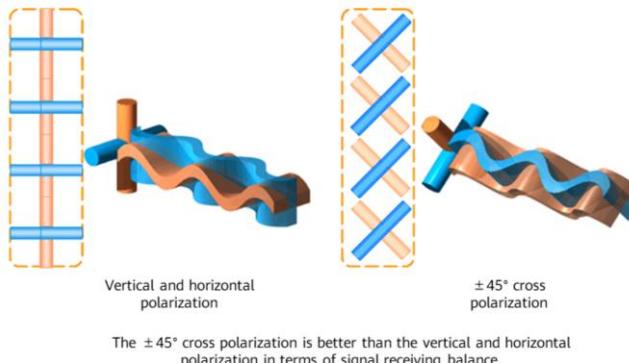
- Polarization is the radiation specification that describes the orientation of electromagnetic wave field. The electrical field and magnetic field have a fixed relationship, so the polarization direction of antennas is represented by the direction of the electrical field. It is the electrical field direction of the maximum radiation.



- Due to the characteristics of electrical waves, the horizontally polarized signals generate current when approaching to the ground. Polarized current generates heat due to ground impedance. As a result, electrical field signals are attenuated. The vertically polarized signals do not generate current, so energy will not be attenuated. Therefore, vertical polarization is widely used in mobile communication. For example, Huawei uses vertically polarized antennas or $\pm 45^\circ$ dual-polarized antennas in wireless communication systems.
- The polarization direction of the antenna is the electric field direction of the electromagnetic field of antenna radiation.
 - If the electric field of the radio wave is perpendicular to the ground, the radio wave is a vertical polarization wave.
 - If the electric field of the radio wave is parallel to the ground, the radio wave is a horizontal polarization wave.

Antenna Polarization (2/3)

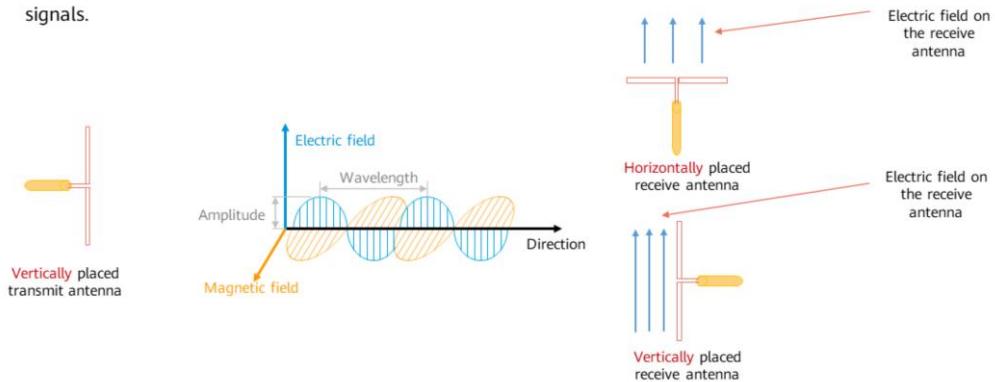
- Dual-polarized antenna: generates two polarized waves that are mutually orthogonal. Two antennas whose polarization directions are perpendicular to each other are integrated as a whole, which maximizes the diversity gains and saves the installation clearance.



- A dual-polarized antenna is a combination of vertically polarized antennas and horizontally polarized antennas, or a combination of $+45^\circ$ polarized antennas and -45° polarized antennas.
- With development of new technologies, dual-polarized antennas are widely used now. There are two polarization modes: vertical and horizontal polarization and $\pm 45^\circ$ polarization. The $\pm 45^\circ$ polarization mode has better performance than the vertical and horizontal polarization modes. Therefore, the $\pm 45^\circ$ polarization mode is used in most cases. A dual-polarized antenna combines two orthogonal antennas with polarization directions of $+45^\circ$ and -45° and works in duplex mode, which greatly reduces the number of antennas in each cell. In addition, the orthogonal polarization ($\pm 45^\circ$) ensures the good effect of receive diversity.
- Vertically and horizontally polarized waves are received by antennas with vertical and horizontally polarization characteristics, respectively. Right-handed and left-handed circular polarization waves are received using antennas with right-handed and left-handed circular polarization characteristics, respectively. If the polarization direction of the incoming waves is different from that of the receiving antenna, polarization loss occurs. For example, polarization loss occurs when a $+45^\circ$ polarization antenna is used to receive vertically or horizontally polarized waves, or when a vertically polarized antenna is used to receive $+45^\circ$ polarization or -45° polarization waves. Similarly, when the circular polarization antenna receives linear polarization waves or vice versa, signals are attenuated. The received signals may be only a half of the total signals.

Antenna Polarization (3/3)

- Antenna polarization is important because a receive antenna can receive signals only when the polarization direction of electromagnetic waves is consistent with that of the receive antenna. If the polarization direction of electromagnetic waves is perpendicular to that of the receive antenna, the receive antenna cannot receive signals.



537 Huawei Confidential

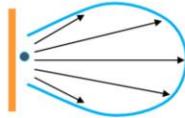
HUAWEI

- As shown in the preceding figure, when the transmit antenna is vertically placed and the receive antenna is horizontally placed, the receive antenna cannot receive signals from the transmit antenna. The electric field polarization direction of electromagnetic waves emitted by the transmit antenna is vertical. When the vertical electric field acts on the receive antenna, the electrons on the antenna conductor cannot move under the electric field. Therefore, the electric field cannot generate current.
- When both the transmit antenna and the receive antenna are placed vertically, the polarization direction of electromagnetic waves emitted by the transmit antenna is vertical. When the vertical electric field acts on the receive antenna, electrons on the antenna move vertically under the electric field. Therefore, the receive antenna generates current.

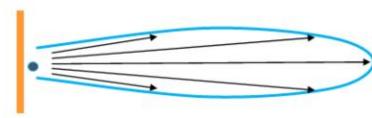
Antenna Gain (1/2)

Concept of gain

- Antennas are passive components, and they do not amplify electromagnetic signals.
- Gain is the ratio of the power of electromagnetic waves produced by an antenna to the power produced by a hypothetical reference antenna at the same spatial location under the same input power. It quantitatively describes a degree to which an antenna intensively radiates an input power.
- The gain of an antenna is related to the antenna model and can measure the antenna's capability of receiving and sending signals in a specific direction. It is also used for selecting a base station antenna.



Low gain

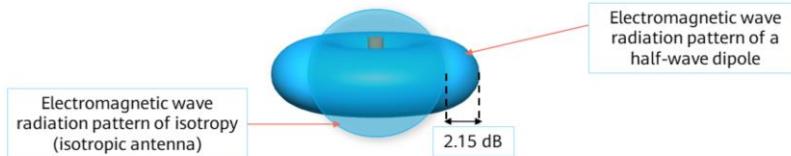


High gain

- A gain is the ratio of the signal output of a system to the signal input of the same system. Assume that the transmit antenna is an ideal unidirectional source and the input power is 100 W. If the transmit antenna is a directional antenna with a gain of 13 dB (20 times the original signal), only 5 W (100/20) of input power is required. That is, an antenna's gain is the amplifier of input power of the unidirectional ideal radiation source.
- If the antenna gain is measured based on half-wave symmetric elements, the gain unit is dBd.
- When selecting gain, ensure that the beam matches the coverage distance. If the coverage distance is small, select low-gain antennas with wide vertical lobes to ensure the coverage effect in the area near the antenna.
- Typical WLAN antenna gains are as follows:
 - Indoor and outdoor rod antenna: 2 to 3 dBi
 - Indoor built-in antenna: 3 to 5 dBi
 - Outdoor external omnidirectional antenna: 6 to 8 dBi
 - Outdoor built-in sector or directional antenna: 8 to 14 dBi

Antenna Gain (2/2)

| Parameter | Description | Calculation Formula |
|----------------------------------|---|----------------------|
| dB _i /dB _d | Describes the antenna gain, with the reference of an isotropic antenna for dB _i and the reference of dipole (half-wave dipole) for dB _d . | $dB_d = dB_i + 2.15$ |



- The antenna gain in dB_i is the ratio between the gain of an antenna relative to the gain of an isotropic antenna. An isotropic antenna radiates power uniformly in all directions.
- The antenna gain in dB_d refers to the gain of a directional antenna relative to a half-wave dipole antenna.
- That is, the gain 16 dB_d is equivalent to 18.14 dB_i, that is, 18 dB.

- Both dB_i and dB_d are relative values used to represent the antenna gain, with different references. The reference for dB_i is an isotropic antenna, and that of dB_d is a dipole. Therefore, the values of dB_i and dB_d are slightly different. The unit energy radiated uniformly by a wave source onto a sphere is smaller than the unit energy flattened on the surface of an ellipsoid with its maximum radius. Therefore, the ratio of the energy received at a point outside the space to the energy on the sphere is greater than that of the energy received at the point outside the space to the energy on the ellipsoid. The gain expressed in dB_i is 2.15 greater than that expressed in dB_d.

Transmit Power of an Antenna

| Parameter | Description | Calculation Formula |
|-----------|---|---|
| W | Describes the transmit power of a device. | Device nominal value |
| dBm | Calculates the wireless link. | $10 \times \log (\text{power value}/1 \text{ mW})$ |
| dB | Describes the relative value of the signal power. | $10 \times \lg (\text{power value A}/\text{power value B})$ |

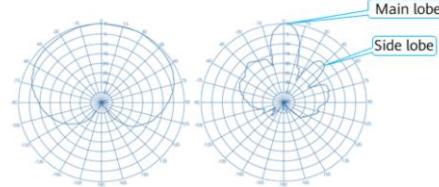
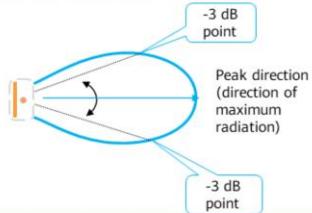
- dB is a unit of power gain. The formula $10 \times \lg(A/B)$ can be used to calculate the dB difference between the power of A and that of B. For example, if the power of A is twice that of B, $10 \times \lg(A/B) = 10\lg 2 = 3$ dB. That is, the power of A is 3 dB higher than that of B.
- dBm is a unit of signal strength. The calculation formula is as follows: $10 \times \log \text{power value}/1 \text{ mW}$. For example, if the transmit power is 1 mW, the value in the unit of dBm is: $10 \times \log(1 \text{ mW}/1 \text{ mW}) = 0$ dBm. For 40 W power, $10 \times \log (40 \text{ W}/1 \text{ mW}) = 46$ dBm.

- dBm: absolute power value. Typical values are as follows:
 - 0 dBm = 1 mW
 - 3 dBm = 2 mW
 - -3 dBm = 0.5 mW
 - 10 dBm = 10 mW
 - -10 dBm = 0.1 mW
- dB: relative power value
 - For example, if the power of A is twice that of B, $10 \times \lg(\text{power of A}/\text{power of B}) = 10 \times \lg 2 = 3$ dB. That is, the power of A is 3 dB higher than that of B.
 - When transmitting signals within 100 m on the 2.4 GHz frequency band, the power loss of a 1/2-inch feeder is about 12.1 dB.
 - If the power of A is 46 dBm and that of B is 40 dBm, the gain of A is 6 dB higher than that of B.
 - If the power of A is 12 dBd and that of B is 14 dBd, the gain of A is 2 dB lower than that of B.

Beamwidth

Beamwidth

- Beamwidth is the angle of the sector formed by radio waves. It is a key parameter for measuring the horizontal/vertical coverage width.
- The radiation pattern of an antenna usually has two or more lobes. The lobe with the maximum radiation is the main lobe, and the other lobes are back and side lobes.
- In the radiation pattern of an antenna, the beamwidth or half-power angle is the angle between the half-power (-3 dB) points of the main lobe, when referenced to the peak effective radiated power of the main lobe. Beamwidth falls into horizontal and vertical beamwidth.

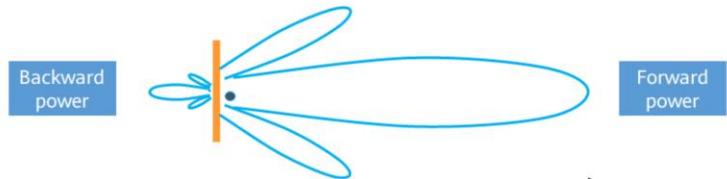


A smaller beamwidth indicates better directionality, longer radiation distance, and stronger anti-interference capabilities.

- Different antennas have different radiation patterns. Radiation patterns of some antennas have many lobes. The lobe with the maximum radiation is the main lobe, and the other lobes are back and side lobes. The areas between the main lobe and side lobes have weak radiation.
- At the two sides of the main lobe, the radiation is reduced by 3 dB (power density is reduced by half). The angle between the two sides is defined as beamwidth (also called main-lobe width or half-power angle). A smaller beamwidth indicates better directionality, larger coverage, and stronger anti-interference capabilities.
- When deploying antennas, note that side lobes will interfere with peripheral cells. Generally, the main-lobe radiation needs to be enhanced, and side-lobe radiation needs to be suppressed. However, in the areas near the antennas, we can enhance the side-lobe radiation to eliminate coverage holes.
- There is another beamwidth (10 dB). It is the angle between the points in the main lobe that are down from the maximum radiation by 10 dB (power density reduced to one tenth).

FBR of a Directional Antenna

- The FBR compares the power density in the direction of the main lobe with the strongest radiation to the power density in the direction of the back lobe with the strongest radiation. A large FBR indicates small backward radiation of antennas, which reflects backward radiation capabilities of antennas or antenna's leakage capabilities of signal power.
- Generally, the maximum gain within 180 degrees from the back of the main lobe is the back lobe gain. In mobile communications, a maximum gain within a range of +/-30 degrees in the back direction is typically used as the back lobe gain.
- In most cases, the FBR of an antenna must be greater than 18 dB.



542 Huawei Confidential

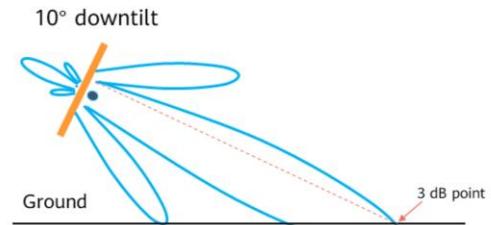
 HUAWEI

- The FBR is valid only for directional antennas. It refers to the ratio of the power density in the antenna forward maximum radiation direction to the power density in the backward maximum radiation direction within ± 30 -degree range. The FBR reflects the capability of an antenna to suppress backward interference.
- Typical FBR value in a WLAN scenario: outdoor sector antenna > 20 dB

Downtilt

- To direct the main lobe to the ground for effective coverage, you must adjust the downtilt of an antenna. A recommended method is to align the upper 3 dB point of the main lobe with the edge of the coverage area.

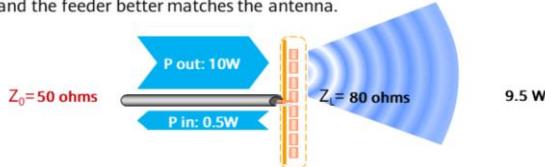
| Mechanical downtilt |
|--|
| Adjust the antenna installation angle to increase the downtilt. |
| Electrical downtilt |
| Adjust the phase of the antenna feed network to change the downtilt. |



- To control the coverage area of an antenna and reduce interference, you need to adjust the downtilt of the antenna.
- Two methods are available for adjusting the antenna downtilt:
 - Mechanical downtilt: Adjust the antenna installation angle to increase the downtilt.
 - When the mechanical downtilt exceeds the half-power beamwidth on the vertical plane, the horizontal beam coverage of the base station antenna will be deformed, which affects the coverage control of the sector. Therefore, the mechanical downtilt cannot exceed the half-power beamwidth on the vertical plane.
 - Electrical downtilt: Adjust the phase of the antenna feed network to change the downtilt. The electrical downtilt can be achieved in the following ways:
 - Electrical downtilt with fixed beam: When designing antennas, deviate the antenna main beam from the normal direction of the array antenna element at a certain angle (such as 3°, 6°, or 9°) by controlling the amplitude and phase of the radiating element. Along with the electrical downtilt, the adjustment range could be from 18° to 20°.
 - Continuous manual electrical tilt: When designing antennas, use adjustable phase shifters to continuously adjust the direction of the main beam. The adjustment range could be from 0° to 10°.
 - Wire remote electrical tilt from the angle of depression: When designing this type of base station, add a servomechanism. A precise motor is used to control the phase shifter so that the electrical tilt can be remotely controlled. However, due to the new active circuit, the reliability of the antenna decreases and the surge protection problem becomes complicated.

Operating Frequency Range (Frequency Bandwidth)

- The operating frequency band of WLAN antennas ranges from 2400 MHz to 2500 MHz.
- Input voltage standing wave ratio (VSWR): indicates the impedance matching at the antenna port. The better the impedance matching, the closer the VSWR value to 1, which indicates that more signal power in the feeder is transmitted to the antenna. On the contrary, the larger the VSWR is, the worse the impedance matching is, and the more the energy loss at the port is. A VSWR value close to 1 is recommended.
- The ratio of the reflected wave amplitude to the incident wave amplitude is the reflection coefficient, which is recorded as R.
- VSWR is the ratio of power of standing wave antinode and amplitude of wave node power. It is also called standing wave coefficient.
- If the antenna impedance Z_L is closer to the feeder characteristic impedance Z_0 , the reflection coefficient r is smaller, the VSWR is closer to 1, and the feeder better matches the antenna.



$$R = \frac{\text{Reflected wave amplitude}}{\text{Incident wave amplitude}} = \frac{(Z_L - Z_0)}{(Z_L + Z_0)}$$

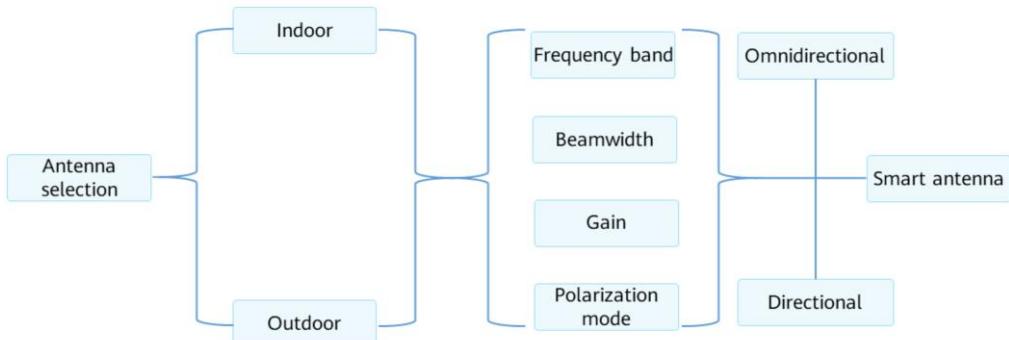
$$\text{VSWR} = \frac{\text{Amplitude of standing power antinode } V_{\max}}{\text{Amplitude of wave node power } V_{\min}} = \frac{(1+R)}{(1-R)}$$

- An antenna works on a certain frequency range (bandwidth) in both the transmit and receive directions. This parameter is a nominal value by the manufacturer. For most base station antennas, they are required to support the operating frequency range when the VSWR value is less than or equal to 1.5. In most cases, the antenna's performance varies according to the frequency. Performance degradation caused by this, however, is acceptable.
- The transmit power can reach the maximum when the antenna operates at the center frequency; therefore, the center frequency and frequency band can be determined according to this rule.
- When the feeder and the antenna match each other, the energy of high frequency waves is radiated. The waves that are on the feeder are only incident waves but not reflected waves, and they are traveling waves. When the feeder and the antenna do not match each other, only part of the energy of high frequency waves is radiated. Therefore, only part of energy is absorbed, and the rest is reflected and forms reflected waves.
 - The ratio of the reflected waves to the incident waves is the reflection coefficient, which is recorded as R.
 - VSWR is the ratio of power of standing wave antinode and amplitude of wave node power. It is also called standing wave coefficient.
 - The return loss (RL) is the ratio of reflected wave power and incident wave power on the antenna connector.
 - The VSWR and RL are both used to describe the status of antenna match. The difference is that the VSWR is described by voltage, while the RL is described by power.

Contents

1. Antenna Overview
2. Concepts Related to Antennas
- 3. Antenna Selection**
4. Traditional Indoor Distribution System

Antenna Selection Mode



- Frequency Band

- Select antennas based on the frequency band. To reduce engineering and purchase costs, use broadband antennas when both the broadband and narrowband antennas meet the specifications. A broadband antenna differs from a dual-band antenna in that the broadband antenna does not have additional power feeding ports.

- Beamwidth

- horizontal and vertical beamwidths are supported, which depend on and affect each other. Antennas are selected based on the coverage range and interference control. In urban areas, use antennas whose horizontal beamwidth is less than or equal to 65° to reduce cell handovers. In suburban areas, use antennas with the horizontal beamwidth of 80° to 90° to enhance coverage and avoid coverage holes.

- Gain

- Low-gain antennas have narrow beams and good directionality. They are mainly used for indoor coverage and coverage hole compensation in outdoor areas, such as behind buildings, new residential communities, and new professional markets. Medium-gain antennas are applicable to urban areas. On the one hand, the volume and size of such antennas are suitable. On the other hand, signals are evenly distributed within a short coverage radius thanks to the large vertical beamwidth. High-gain antennas are applicable to wide and open areas, for example, highways, railways, tunnels, and long and narrow areas.

Antenna Selection - Indoor and Outdoor Directions

| Antenna Pattern | | | Application Scenario | Antenna Type |
|-----------------|-------------------------|-------------------------------------|--|---------------------------------------|
| Indoor | Omnidirectional antenna | Omnidirectional horizontal coverage | Indoor omnidirectional coverage scenarios, such as offices, lecture halls, and conference rooms. | Ceiling-mount omnidirectional antenna |
| Outdoor | | | | Whip antenna |
| Indoor | | | | Built-in antenna |
| Outdoor | Directional antenna | Directional coverage and high gain | Outdoor omnidirectional coverage scenarios, such as open areas, squares, and parks. | Pole-mount omnidirectional antenna |
| Indoor | | | Indoor application scenarios, such as corridors and two inner walls. | Dual-band antenna |
| Outdoor | | | Outdoor application scenarios, such as oil wells, open suburbs, and P2P and P2MP backhaul. | Plate directional antenna |
| | | | | Plate cross-polarized antenna |



Ceiling-mount antenna



2.4G&5G outdoor omnidirectional antenna



Indoor directional antenna

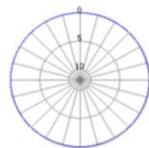


2.4G&5G outdoor directional antenna

HUAWEI

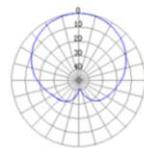
Antenna Selection - Antenna Type

Omnidirectional antenna



- A small antenna gain usually indicates a short coverage range.
- An omnidirectional antenna provides a large coverage area.
- An omnidirectional antenna has one port and is single-polarized. Therefore, two omnidirectional antennas are required to implement the polarization and MIMO features.

Directional antenna



- A high antenna gain usually indicates a long coverage range.
- A directional antenna provides a narrow coverage area, generating less interference to other APs.
- Directional antennas are classified into single-polarized and dual-polarized antennas. To implement the polarization and MIMO features, select two single-polarized antennas or only one dual-polarized antenna.

- For a coverage range of less than 300 m: Use omnidirectional antennas when the coverage area is round or square and the antennas can be deployed in the center.
- For a coverage range of more than 300 m: Use directional antennas.
- Use directional antennas in long and narrow coverage areas, such as scenic spots, streets, and tunnels.
- A pole is required for installing a directional antenna. The height of the pole depends on its diameter, fixing mode, and wind speed. It is recommended that the length of a pole on the rooftop be within 1 m to 3 m and not exceed 5 m.

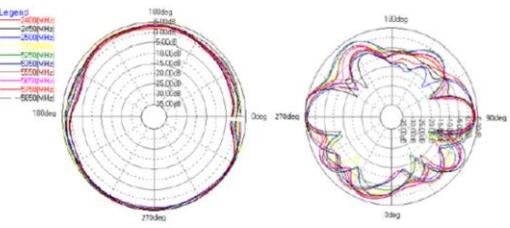
Antenna Selection - Frequency Band

Frequency band

- Select antennas based on the frequency band. To reduce engineering and purchase costs, use broadband antennas when both the broadband and narrowband antennas meet the specifications. A broadband antenna differs from a dual-band antenna in that the broadband antenna does not have additional power feeding ports.



Antenna model: 27011668
Gain: 4 dBi @ 2.4 GHz; 7 dBi @ 5 GHz



Horizontal radiation pattern

Vertical radiation pattern

- The radiation pattern is a graphical description of the relative field strength of the antenna. As the antenna radiates to three-dimensional space, several patterns are required for description.
- Dual-band antennas can work on both the 2.4 GHz and 5 GHz frequency bands. In this way, dual-band APs can be configured with only one type of antenna, facilitating installation and purchase. The antenna also features a low omnidirectional gain. It achieves 360-degree coverage and reduces the maximum power density in the omnidirectional direction with the same transmit power.

Antenna Selection - Antenna Gain (1/3)

- If there are specific bandwidth requirements, the relationship between the coverage range and the bandwidth is listed in the following table.

| Antenna | Frequency Band | Maximum Coverage Range (m) Bandwidth (Mbps) Scenario | Maximum Coverage Range Under Different Bandwidths (802.11n HT20 Mode, MIMO 2x2 Dual-Stream) | | | | | | | |
|--|----------------|--|---|-----|-----|-----|-----|-----|-----|-----|
| | | | 100 | 70 | 60 | 45 | 30 | 25 | 15 | 7 |
| Standard-configuration 11 dBi antenna | 2.4 GHz | Densely populated urban area | 90 | 100 | 110 | 150 | 200 | 300 | 350 | 450 |
| | | Urban area | 100 | 110 | 120 | 170 | 250 | 300 | 400 | 500 |
| | | Suburban area | 130 | 140 | 150 | 200 | 300 | 400 | 500 | 600 |
| | | Rural area | 150 | 170 | 200 | 300 | 400 | 500 | 600 | 800 |
| | 5 GHz | Densely populated urban area | 40 | 44 | 48 | 60 | 90 | 120 | 150 | 190 |
| | | Urban area | 40 | 45 | 50 | 70 | 100 | 130 | 160 | 200 |
| | | Suburban area | 50 | 60 | 65 | 90 | 130 | 180 | 200 | 300 |
| | | Rural area | 60 | 70 | 80 | 120 | 160 | 200 | 250 | 350 |

- Without specific bandwidth requirement: If the coverage range is less than 300 m, antennas with the gain of 11 dBi \pm 3 dBi are recommended.
- Without specific bandwidth requirement: If the coverage range is greater than or equal to 300 m, antennas with the gain of 18 dBi \pm 3 dBi are recommended.

Antenna Selection - Antenna Gain (2/3)

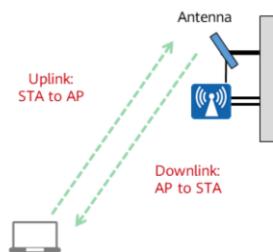
- If there are specific bandwidth requirements, the relationship between the coverage range and the bandwidth is listed in the following table.

| Antenna | Frequency Band | Maximum Coverage Range (m) Bandwidth Scenario | Maximum Coverage Range Under Different Bandwidths (802.11n HT20 Mode, MIMO 2x2 Dual-Stream) | | | | | | | |
|---|----------------|--|---|-----|-----|-----|-----|------|------|------|
| | | | 100 | 70 | 60 | 45 | 30 | 25 | 15 | 7 |
| High-gain antenna: 17 dBi @ 2.4 GHz; 15 dBi @ 5 GHz | 2.4 GHz | Densely populated urban area | 170 | 180 | 200 | 300 | 400 | 500 | 600 | 800 |
| | | Urban area | 180 | 200 | 220 | 300 | 450 | 600 | 700 | 900 |
| | | Suburban area | 240 | 260 | 300 | 400 | 600 | 750 | 900 | 1200 |
| | | Rural area | 300 | 320 | 350 | 600 | 900 | 1300 | 1600 | 2500 |
| | 5 GHz | Densely populated urban area | 55 | 60 | 70 | 100 | 140 | 180 | 210 | 280 |
| | | Urban area | 60 | 70 | 75 | 100 | 150 | 200 | 230 | 300 |
| | | Suburban area | 80 | 90 | 95 | 130 | 200 | 250 | 300 | 400 |
| | | Rural area | 90 | 100 | 120 | 150 | 240 | 300 | 350 | 480 |

- Without specific bandwidth requirement: If the coverage range is less than 300 m, antennas with the gain of 11 dBi \pm 3 dBi are recommended.
- Without specific bandwidth requirement: If the coverage range is greater than or equal to 300 m, antennas with the gain of 18 dBi \pm 3 dBi are recommended.

Antenna Selection - Antenna Gain (3/3)

- In an outdoor environment without obstacles, if an external antenna (11 dBi) is connected to an AP for coverage, plan STAs as follows: laptop: 300 m; mobile phone: 200 m.
- Based on the network planning, both the uplink and downlink must conform the following requirement: Signal field strength – System margin > Device receiver sensitivity. The system margin is related to the signal propagation environment. In most cases, the system margin is 10 dB.

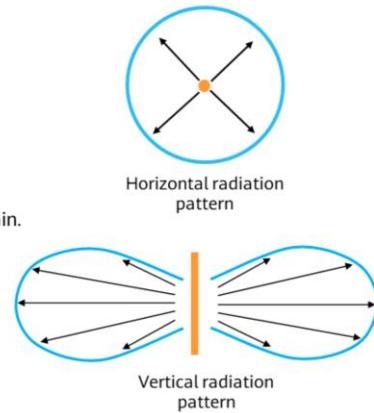


| Device | Transmit Power | Antenna Gain | Receive Sensitivity (2.4 GHz, 802.11n, and HT20) | |
|--------------|----------------|--------------------------|--|--------------------------|
| | | | Maximum Rate (MCS7/15) | Available Rate (MCS2/10) |
| AP | 27 dBm | Depending on the antenna | -71 dBm | -86 dBm |
| Laptop | 14 to 18 dBm | 0 dBi | -64 dBm | -77 dBm |
| Mobile phone | 10 to 13.8 dBm | 0 dBi | -64 dBm | -77 dBm |
| CPE | 14 dBm | 10 dBi | -68 dBm | -82 dBm |

- This slide introduces the formula for calculating the signal field strength and the network adapter parameters of common STAs.
- Note that the table lists common typical values, which may vary according to vendors.
- Formula for calculating the uplink signal field strength (without interference, cable loss, and obstacle loss):
 - Signal field strength = Transmit power + Transmit antenna gain – Transmission attenuation value + Receive antenna gain
- For example, in a rural area, an external antenna (11 dBi) is connected to an AP, the uplink signal field strength of a STA (a laptop as an example) on the 2.4 GHz frequency band at 300 m is:
 - $18 + 0 - 89.8 + 11 = -60.8 \text{ dBm}$.
 - After the 10 dB system margin is subtracted from the signal field strength, we get the optimal receiver sensitivity (-71 dBm) of the AP.

Antenna Selection - Beamwidth

- Antenna angle:
 - An antenna transmits most energy to the required direction.
- Relationship between the antenna gain and angle:
 - A smaller angle indicates a higher gain.
 - An antenna has horizontal and vertical angles.
- The antenna gain is related to the antenna radiation pattern. A narrower main lobe indicates a smaller minor lobe and higher gain.
- However, the antenna gain is not simply a "more is better" parameter. The key is to meet signal coverage requirements.



- An antenna has two horizontal and vertical beamwidths.
 - Horizontal beamwidth: indicates the beamwidth after the main lobe power of the horizontal beam decreases by 3 dB. It is also called horizontal half-power angle.
 - Vertical beamwidth: indicates the beamwidth after the main lobe power of the vertical beam decreases by 3 dB. It is also called vertical half-power angle
- There is another beamwidth (10 dB). It is the angle between the points in the main lobe that are down from the maximum radiation by 10 dB (power density reduced to one tenth).

Antenna Selection - Polarization Mode

- Dual-polarized antenna

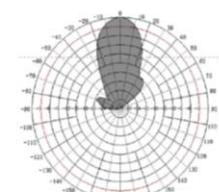
- A dual-polarized antenna transmits signals through two channels at the same time to perform comparable functions of two standalone antennas. For example, a 2x2 MIMO AP needs only one cross-polarized antenna for one frequency band, but needs two common polarized antennas for the same frequency band. The cross-polarized antenna has two polarization ports: +45° and -45° polarization ports. The purchase and installation costs for cross-polarized antennas are low. As fewer antennas are used, antenna installation and layout are easier.



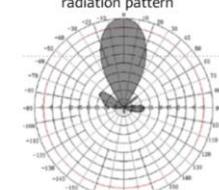
Dual-polarized directional antenna

Antenna number: 27010904
Gain: 8 dBi @ 2.4 GHz, 300 m

Applicable to the AP6510DN, AP6610DN, and AP8130DN



Horizontal radiation pattern



Vertical radiation pattern

Antenna Recommendations in Outdoor WLAN Scenarios (1/2)

| Scenario | Frequency Band | Antenna Part Number | Antenna Model | Remarks | Optional AP Model |
|---|----------------|---------------------|---------------|--|---|
| WDS wireless backhaul | 5 GHz | 27010890 | SL12845A | 2x2 AP point-to-point backhaul | WA161DD-NZ |
| | | 27011145 | SL12941A | 3x3 AP point-to-point backhaul | WA251DT-NE |
| Densely populated urban area or common urban area | 2.4 GHz | 27010661 | A25451804 | Continuous coverage (long coverage range required) | WA151DD-NZ (outside China) WA161DD-NZ (in China) |
| | | 27010812 | SL12764A | Hotspots in an urban area | |
| | 5 GHz | 27011044 | Not certified | Continuous coverage (long coverage range required) | |

Antenna Recommendations in Outdoor WLAN Scenarios (2/2)

| Scenario | Frequency Band | Antenna Part Number | Antenna Model | Remarks | Optional AP Model |
|-----------------------------|----------------|---------------------|---------------|--|---|
| Suburban area or rural area | 2.4 GHz | 27010661 | A25451804 | Scenario with high requirements on the antenna size and long-distance coverage | WA151DD-NZ (outside China) WA161DD-NZ (in China) |
| | | 27011071 | SL12865A | Single-polarized antenna, two of which are required to implement 2x2 MIMO | |
| | 5 GHz | 27011072 | SL12867A | Single-polarized antenna, two of which are required to implement 2x2 MIMO | |
| Residential area | 2.4 GHz | 27010904 | SL12872 | Horizontal coverage range of the AP ≤ 12 m (horizontal beamwidth: 60°) | WA151DD-NZ (outside China) WA161DD-NZ (in China) |
| | | 27010812 | SL12764A | Horizontal coverage range of the AP > 12 m (horizontal beamwidth: 30°) | |
| | 5 GHz | 27010906 | SL12872A | Horizontal coverage range of the AP ≤ 12 m (horizontal beamwidth: 60°) | |
| | | 27010889 | SL12844A | Horizontal coverage range of the AP > 12 m (horizontal beamwidth: 30°) | |
| Square or pedestrian street | 2.4 GHz | 27010812 | SL12764A | Scenario with high requirements on the installation size and but not on the coverage range | |
| | 5 GHz | 27010889 | SL12844A | | |

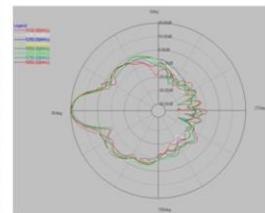
WLAN Outdoor Antenna Example (1/3)



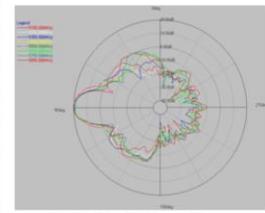
SL12845A

- This is a 5 GHz dual-polarized directional antenna with narrow beams and high gains, which is applicable to [WDS wireless backhaul \(2x2\) scenarios](#).

| Item | Description |
|------------------------------|---|
| Frequency range (MHz) | 5150 to 5850 |
| Polarization mode | $\pm 45^\circ$ |
| Antenna gain (dBi) | 19 \pm 1 |
| Horizontal beamwidth (°) | 15 \pm 3 |
| Vertical beamwidth (°) | 15 \pm 3 |
| FBR (dB) | ≥ 25 |
| Isolation (dB) | ≥ 30 |
| Input impedance (Ω) | 50 |
| VSWR | ≤ 1.8 |
| Connector | Type N female connector x 2 |
| Maximum power (W) | 50 |
| Surge protection | DC grounding |
| Dimensions (H x W x D) | 25 mm x 250 mm x 250 mm (0.98 in. x 9.84 in. x 9.84 in.) |
| Pole diameter (mm) | $\phi 35$ to $\phi 114$ |



Horizontal radiation pattern



Vertical radiation pattern

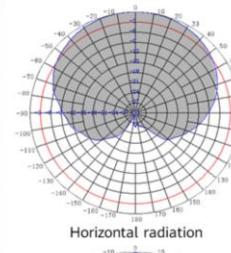
WLAN Outdoor Antenna Example (2/3)



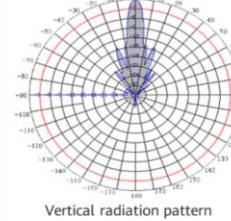
SL12865A

- This is a 2.4 GHz single-polarized **coverage** antenna, which is applicable to **suburban and rural areas** that do not have high requirements the antenna size. To achieve the MIMO 2*2 effect, **Two** such antennas are required to implement 2x2 MIMO.

| Item | Description |
|------------------------------|---|
| Frequency range (MHz) | 2400 to 2500 |
| Polarization mode | Vertical polarization |
| Antenna gain (dBi) | 15 ± 1 |
| Horizontal beamwidth (°) | 120 |
| Vertical beamwidth (°) | 7 |
| FBR (dB) | ≥ 21 |
| Input impedance (Ω) | 50 |
| VSWR | ≤ 1.5 |
| Connector | Type N female connector x 1 or 7/16DIN female connector |
| Maximum power (W) | 300 |
| Surge protection | DC grounding |
| Dimensions (H x W x D) | 80 mm x 1070 mm x 160 mm (3.15 in. x 42.13 in. x 6.30 in.) |
| Pole diameter (mm) | φ48 to φ135 |



Horizontal radiation



Vertical radiation pattern

 HUAWEI

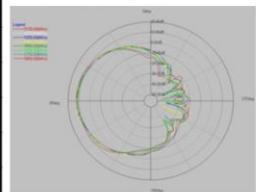
WLAN Outdoor Antenna Example (3/3)



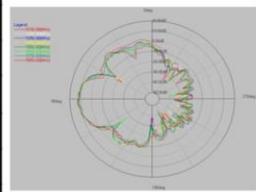
SL12844A

- This is a 5 GHz directional **coverage** antenna, which is applicable to **urban areas** that require antennas with a small size and a horizontal beamwidth of about 60 degrees.

| Item | Description |
|------------------------------|-----------------------------|
| Frequency range (MHz) | 5150 to 5850 |
| Polarization mode | $\pm 45^\circ$ |
| Antenna gain (dBi) | > 16 |
| Horizontal beamwidth (°) | 60 |
| Vertical beamwidth (°) | 6 |
| FBR (dB) | ≥ 23 |
| Isolation (dB) | ≥ 30 |
| Input impedance (Ω) | 50 |
| Standing wave ratio (SWR) | ≤ 1.8 |
| Connector | Type N female connector x 2 |
| Maximum Power (W) | 5 |
| Surge protection | DC grounding |



Horizontal radiation pattern



Vertical radiation pattern

WLAN Indoor Antennas



Whip omnidirectional antennas are delivered with indoor APs by default. The antenna gain is about 2 dB to 3 dB. Some antennas support only a single frequency band (2.4 GHz or 5.8 GHz), while some support dual frequency bands (2.4 GHz and 5.8 GHz).



Ceiling-mount antennas are usually mounted on the ceiling. The antenna gain is about 2 dB to 3 dB. Some antennas support only a single frequency band (2.4 GHz or 5.8 GHz), while some support dual frequency bands (2.4 GHz and 5.8 GHz). These antennas are used as **external** antennas of **indoor DAS APs** or **settled APs**.



Directional plate antennas are usually deployed indoors to provide directional coverage. The antenna gain is about 12 dBi to 15 dBi. Such antennas support dual frequency bands (2.4 GHz and 5.8 GHz) and are used as **external** antennas of **indoor settled APs**.



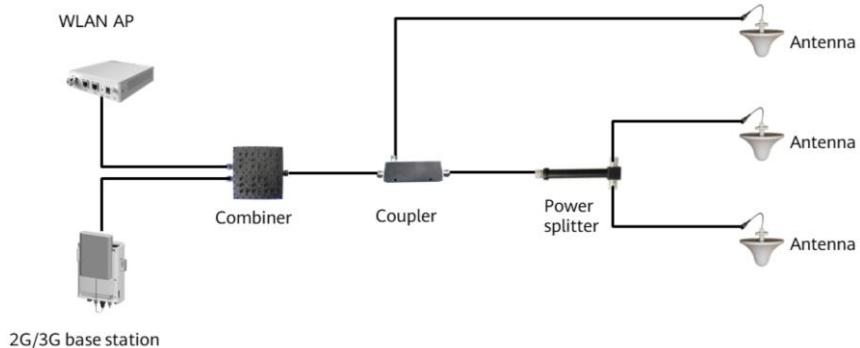
Desktop antennas are usually mounted on a desktop to enhance indoor coverage. The antenna gain is about 5 dBi. Such antennas support only the 2.4 GHz frequency band and are used as **external** antennas of **indoor settled APs**.

Contents

1. Antenna Overview
2. Concepts Related to Antennas
3. Antenna Selection
- 4. Traditional Indoor Distribution System**

Indoor Distribution System

- Indoor distribution system architecture



- Combiner, power splitter, and coupler are commonly used passive components used in an indoor distribution system. The combiner is mainly applied to multi-system (GSM/CDMA/3G/WLAN), or to different WLAN frequency bands. The coupler is used to unequally divide power and splitter is used to equally divide power.

Power Splitter

- It is used in an indoor distributed system and can evenly distribute the AP output power to the remote end. One-to-two, one-to-three, and one-to-four power splitters are commonly used, which can also be used together.
- A power splitter divides a signal into two or more signals.
 - Type: microstrip splitter and cavity splitter
 - The cavity splitter is applicable to high transmit power. When working for a long time, the cavity splitter is stabler than the microstrip splitter.
 - Only the microstrip splitter can be used as the combiner.



565 Huawei Confidential

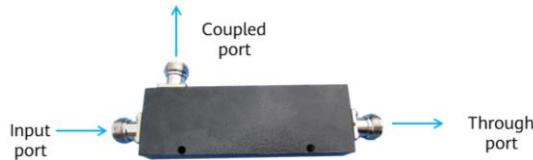
 HUAWEI

- The splitter equally divides energy to provide a wide frequency band by matching cascaded impedance conversion lines and isolation resistors.
- The splitter cascades two, three, or four channels to distribute power.
- Note:
 - A cavity splitter is applicable to high transmit power.
 - The output arms of a cavity splitter are not isolated. Therefore, the cavity splitter cannot be used as a combiner.
 - When working for a long time, the cavity splitter is stabler than the microstrip splitter.
 - When connecting passive components, consider port definition to ensure proper system running.
 - Passive components cannot work at overloaded power. Otherwise, the components may be damaged or the active devices may be faulty.
 - When connecting components, ensure that the interfaces are reliably connected. Otherwise, interface performance may degrade and the system cannot work.

Coupler

- A coupler divides a signal on a port into uneven signals on two output ports. It can couple a certain power level from the main signal for indoor coverage or detection.
 - Commonly used couplers are 5 dB, 6 dB, 7 dB, 10 dB, and 15 dB couplers.

$$\text{Output power of the coupled port (dBm)} = \text{Input power (dBm)} - \text{Coupling (dB)}$$



$$\text{Output power of the through port (dBm)} = \text{Input power (dBm)} - \text{Insertion loss (dB)}$$

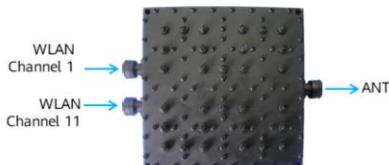
566 Huawei Confidential

 HUAWEI

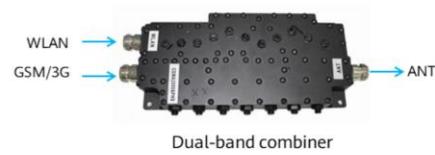
- Product type
 - Couplers are classified into cavity coupler and microstrip coupler based on power distribution.
 - The couplers must be selected properly based on network construction requirements.
- Note:
 - A cavity coupler is applicable to high transmit power.
 - When working for a long time, the cavity coupler is stabler than the microstrip coupler.
 - When connecting passive components, consider port definition to ensure proper system running.
 - Passive components cannot work at overloaded power. Otherwise, the components may be damaged or the active devices may be faulty.
 - When connecting components, ensure that the interfaces are reliably connected. Otherwise, interface performance may degrade and the system cannot work.

Combiner

- A combiner combines radio signals of multiple systems over one channel and distributes receive signals over one channel to ports of each system without interference. Combiners are classified into single-band and multi-band combiners.



WLAN single-band combiner



Dual-band combiner

Due to the limitation of port isolation, WLAN single-band combiners can combine signals only on channels 1 and 11.

- A combiner combines signals of multiple systems into a set of antenna system. In a wireless antenna system, input and output signals on different frequency bands are combined, and the antenna system is connected to the console through a feeder. This saves feeders and prevents antenna switching.
- In the WLAN field, combiners include single-band combiners (2.4 GHz) and multi-band combiners.
- The input port on a combiner limits the frequency.
- A combiner can reduce the number of antennas and feeders, save the antenna installation space, and improve the isolation between transmitters. Common combiners include dual-band combiners and triple-band combiners.

RF Coaxial Cable (Feeder)

- Common RF cable
 - RG-8 jumper, 1/2" super-flexible jumper, and 1/2" feeder
 - The diameters and losses of different cables are different.
 - RG-8

| Performance Specifications | 1/2" Super-Flexible Feeder | 1/2" Feeder |
|----------------------------|----------------------------|-----------------|
| Minimum bend radius | ≤ 40 mm | ≤ 80 mm |
| Loss (2.4 GHz) | < 19.2 dB/100 m | < 12.1 dB/100 m |
| Characteristic impedance | 50 Ω | |
| Operating temperature | -30°C to +60°C | |
| Additional requirements | Flame-retardant | |

A larger diameter has a small loss.



 HUAWEI

- A coaxial cable has the inner conductor and the outer shield sharing a geometric axis. A common coaxial cable has an inner conductor surrounded by a tubular insulation layer, surrounded by a tubular conducting shield. The cable is wrapped by a PVC jacket. The coaxial cable transmits high-frequency signals with little loss, prevents interference, and provides high bandwidth.
- There are two types of coaxial cables: 50 Ω and 75 Ω . The 75 Ω coaxial cable is used for the CATV system, and the 50 Ω coaxial cable is used for radio communication.
- An RF coaxial cable transmits signals and energy within the radio frequency range. RF coaxial cables are classified into three types based on functions: CATV coaxial cable, radio coaxial cable, and leakage coaxial cable.
- When signals are transmitted in a feeder, impedance loss and media loss are generated. The loss increases when the feeder length and working frequency increase. Therefore, the feeder should not be too long.

Radio Connector



Outdoor AP type-N connector
(Female)



FR cable type-N connector
(Male)



Dual-male type-N connector
(connecting the AP and antenna)



Polarity reversal SMA connector



Dual-female type-N connector
(connecting two feeders)

- An RF coaxial connector (RF connector for short) is installed on a cable or instrument to separate or combine electricity.
- Compared with other electrical components, the RF connector has a shorter history. The UHF connector invented in 1930 is the earliest RF connector. During the World War II, radar, broadcasting station, and microwave communication technologies developed fast. Accordingly, the type N, C-type, BNC, and TNC connectors were developed. After 1958, the SMA, SMB, and SMC connectors were developed. In 1964, the US issued the MIL-C-39012 RF coaxial connector specifications. Then, the RF connectors were standardized and commonly used.
- RF connector type:
 - For example, SMA-50JK represents the SMA-type 50 Ω converter. One end is male and the other end is female. BNC/SMA-50JK represents the converter with BNC male and SMA female, and the impedance is 50 Ω.
- The major name of a converter is the connector name or fraction.

Protection Components

- Surge protector



Antenna surge protection (between the antenna and AP)



Network port surge protection (between the outdoor AP and switch)

- Other protection components: optical fiber tube, ground cable, and waterproof tape.

- Surge protection devices are usually deployed between the electrical conduction and ground, and connected to the protected devices in parallel mode. When voltage exceeds the upper limit, a surge protection device limits voltage to protect the device. When voltage is restored, the surge protection device restores to ensure proper system power supply.
- An antenna surge protector provides the following functions: transmits wireless signals and protects interfaces, transmits control signals and protects receiving devices, protects television satellite devices, monitors signal transmission, protects receiving devices, protects wireless communication devices, and protects other radio devices.

Quiz

1. (Multi-Answer Question) Which of the following antenna types are classified by direction?
 - A. Omnidirectional antenna
 - B. Built-in antenna
 - C. External antenna
 - D. Directional antenna
2. $23 \text{ dBm} = ? \text{ mW}$

- 1. AD
- 2. $23 \text{ dBm} = ? \text{ mW}$
 - $+23 \text{ dBm}$ can be divided into $+10 \text{ dBm}$, $+10 \text{ dBm}$, and $+3 \text{ dBm}$.
 - The calculation procedure is as follows:
 - $1 \text{ mW} \times 10 = 10 \text{ mW}$
 - $10 \text{ mW} \times 10 = 100 \text{ mW}$
 - $100 \text{ mW} \times 2 = 200 \text{ mW}$

Summary

- Concepts, functions, and classification of antennas.
- Antenna parameters, including the measurement unit, antenna gain, beamwidth, and radiation pattern.
- Main performance specifications and model selection parameters of antennas.
- Components in an indoor distribution system.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future, market opportunities, product offerings and/or future performance, portfolio, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Overview of Common WLAN Deployment



Foreword

- During network planning, the capacity and coverage must be designed based on customer requirements, and a proper coverage mode must be selected to ensure the feasibility of the project.
- To provide good user experience for WLAN users, make proper WLAN network planning to reduce the probability of WLAN signal coverage holes and WLAN signal interference, properly plan the number of STAs connected to APs, and ensure bandwidth requirements of each STA.
- This course focuses on WLAN network planning to meet requirements of wireless engineers.

Objectives

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

- Describe the WLAN network planning and delivery process.
- Describe WLAN network requirement collection and site survey.
- Describe the capacity, frequency, and coverage planning of the WLAN network.
- Describe the WLAN network channel planning, AP deployment design, power supply and cabling design, and AP installation mode design.
- Describe WLAN project acceptance methods.

Contents

- 1. Introduction to WLAN Planning and Design**
2. WLAN Planning and Design Details
3. WLAN Project Acceptance
4. WLAN Planning Cases

Why Is Network Planning and Design Required?

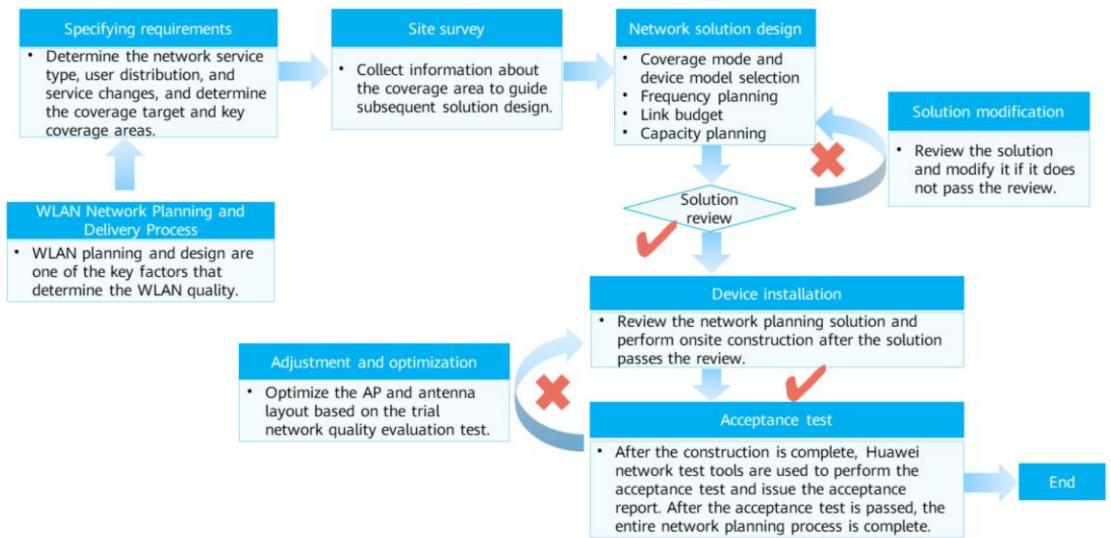
If professional WLAN planning and design are not performed, problems may occur frequently after the project is delivered.

| Low STA's signal strength | Slow Internet access of STAs | Severe co-channel interference | Poor experience in VIP areas |
|---|--|---|--|
| The AP transmit power is not considered during AP coverage distance design. As a result, signal coverage holes occur. | More concurrent users result in more fierce channel competition and higher probability of collision. | Co-channel interference indicates that two APs working at the same frequency interfere with each other. As a result, the wireless network quality is poor, the network speed is slow, or even the network is unavailable. | VIP areas are key areas covered by WLANs. Therefore, service and experience of VIP users must be ensured during solution design. |

Network planning and design are performed based on user requirements and actual conditions, laying a solid foundation for improving user experience.

- A WLAN uses radio signals (high-frequency electromagnetic waves) to transmit data. The strength of radio signals becomes weaker as the transmission distance increases. In addition, adjacent radio signals cause interference overlapping. All these factors reduce the signal quality or even cause network unavailability. To improve the WLAN quality and meet customers' requirements on network construction, WLAN planning and design are required. During WLAN planning and design, the AP models and quantity, installation positions and modes, and cable deployment modes need to be planned to ensure pervasive wireless network coverage, fast Internet access, and optimal network experience. If WLAN planning and design are not performed in the early stage, rework may be required after APs are installed. This is because network optimization after APs are installed may require AP reinstallation and re-cabling.

WLAN Network Planning and Delivery Process

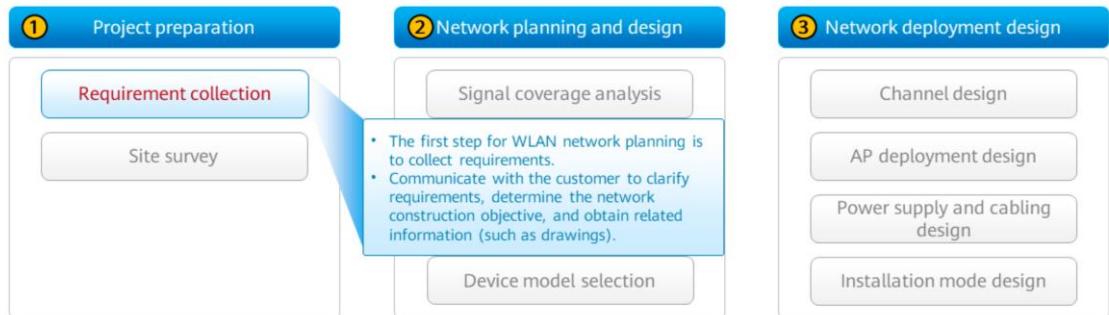


580 Huawei Confidential



- Specifying requirements
 - Determine the network service type, user distribution, and service changes, and determine the coverage target and key coverage areas.
- Site survey
 - Collect information about the coverage area to guide subsequent solution design.
- Network solution design
 - Coverage mode and device model selection
 - Frequency planning
 - Link budget
 - Capacity planning
- Engineering implementation
- Acceptance test
 - After the construction is complete, Huawei network test tools are used to perform the acceptance test and issue the acceptance report. After the acceptance test is passed, the entire network planning process is complete.
- Adjustment and optimization
 - Optimize the AP and antenna layout based on the trial network quality evaluation test.

WLAN Planning and Design



Requirement Collection (1/2)

| Requirement | Description | Network Planning Tool Support |
|--------------------------------|---|--|
| Regulatory restrictions | Check the equivalent isotropically radiated power (EIRP) limit and available channels. | - |
| Drawing information | Ensure that complete drawings with scale information are available. Computer-aided design (CAD) drawings of customer buildings can be obtained from the customer's capital construction management office. | - |
| Coverage | Determine the key coverage areas (such as office areas and meeting rooms) and common coverage areas (such as stairs and bathrooms) required by the customer. | Common projects' requirements for key and common coverage areas are pre-configured, and one-click setting is supported. |
| Field strength | The customer may impose specific requirements for the signal field strength in a coverage area, for example, -40 dBm to -65 dBm in key areas and greater than -75 dBm in common areas. | The field strength can be manually configured according to customers' specific requirements. If not required, the pre-configured empirical data can be used. |
| Number of access users | Determine the total number of STAs and the number of concurrent STAs in a coverage area. In a wireless office scenario, assume that each user has one mobile phone and one laptop. In this case, the number of STAs is calculated as follows: Number of STAs = Number of access users x 2 | Empirical data has been pre-configured and can be modified. |
| STA type | <ul style="list-style-type: none"> Type and number of STAs on the live network (common STAs include mobile phones, tablets, and laptops, and special STAs include scanners and cash registers) Proportion of MIMO types supported by STAs, based on which the number and models of APs can be determined (optional, based on the customer's technical competence) | - |
| Bandwidth | Major service types and bandwidth requirements for each user | Empirical data has been pre-configured and can be modified. |

- Signal coverage is not provided for areas with few wireless requirements, such as bathrooms, staircases, equipment rooms, and archive rooms.
- Generally, the signal strength of indoor dual-band APs should be greater than -65 dBm, and that of outdoor dual-band APs should be greater than -70 dBm.
- Concurrency indicates that both uplink and downlink services are performed.
- Common Internet access/Email sending and receiving: 512 kbit/s
- SD video: 2 Mbps
- Ceiling installation recommendation
- 100 m long-distance power supply through a PoE switch

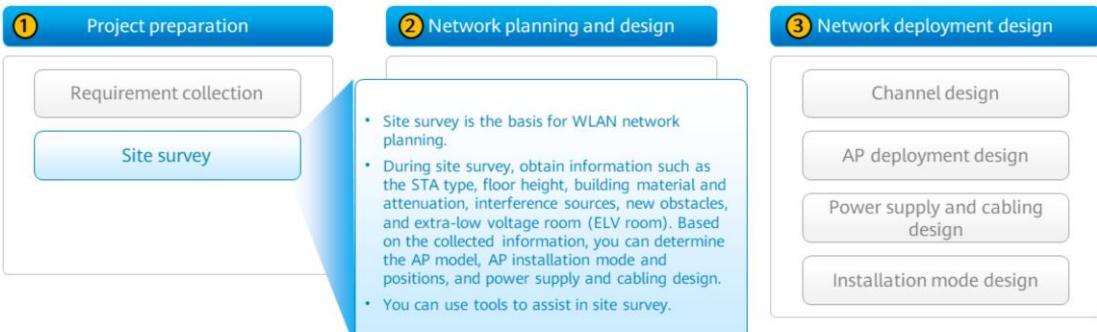
Requirement Collection (2/2)

| Requirement | Description | Network Planning Tool Support |
|-------------------|--|---|
| Coverage mode | Indoor settled, indoor distributed, or outdoor coverage. | Indoor, outdoor, and agile distributed scenarios are supported. |
| Power supply mode | Customer's requirements on the power supply mode, and available power supply facilities and areas. | PoE power supply can be drawn. |
| Switch location | Location of switches connected to the WLAN. | A topology with switches and cables can be drawn. |

Ensure that all possible requirements are collected, prepare a requirement collection checklist, and collect and record customer requirements based on the checklist.

- The detailed drawing of the coverage area is the basic requirement.
- The number of connected STAs needs to be considered.
- The power supply mode of the AP must be considered.
- If PoE power supply is used, the length of the network cable cannot exceed 80 m. If PoE++ is supported, the length of the network cable can reach 200 m.

WLAN Planning and Design



Site Survey Information Collection (1/2)

| Site Survey Item | Information (Example) | Remarks |
|--|---|--|
| Floor height | 3 m | Obtain the ceiling height and atrium height of a lobby or lecture hall. Use a rangefinder to measure the height. |
| Building materials and signal attenuation* | 240 mm thick brick wall (attenuation: 15 dB @ 2.4 GHz, 25 dB @ 5 GHz) | Obtain the building materials on the site and their thicknesses to determine signal attenuation values. If possible, test the signal attenuation onsite. |
| Interference sources | Information about Wi-Fi interference sources detected on the site | Check whether there is interference caused by sources, for example, mobile hotspots, Wi-Fi devices of other vendors, and non-Wi-Fi devices (such as Bluetooth devices and microwave ovens). Tools such as the CloudCampus app can be used to record interference source information. |
| New obstacles | New partitions on the site | Check whether obstacles onsite are consistent with those on the drawing. If not, mark the inconsistent areas and take photos. |
| Site photos | Global site photos | Take as many photos as possible to record the environment and transfer survey information. |

Note: On a WLAN, obstacles cause strong attenuation on wireless signals, which affects user experience. Testing the wall attenuation can improve reliability of network planning. Therefore, before site survey, master the methods of testing the attenuation of unknown obstacles.

Site Survey Information Collection (2/2)

| Site Survey Item | Information (Example) | Remarks |
|---|---|--|
| AP type | Common settled AP | Select indoor settled, agile distributed, outdoor, or high-density APs based on scenarios. |
| AP installation mode and position | Ceiling or wall mounting | Check whether APs can be mounted on the ceiling. If not, mount APs on the wall or junction boxes. |
| ELV room locations | ELV room locations | On the drawing, mark the locations of ELV rooms where switches are to be deployed. |
| Power supply cabling | Cables to be routed | Mark PoE power cables to be routed on the drawing. It is recommended that the length of a PoE power cable be less than or equal to 80 m. |
| Implementation feasibility | Whether APs can be deployed and cabling is feasible, and distance between an AP and switch and distance between an AP and power supply point. | Whether there are fireproof doors or it is difficult to drill holes for concrete bearing walls. |
| Outdoor site | Observe the main building and the height of the site | High buildings, street lamps, and towers in or near the coverage area can be used as main buildings of an AP site. Visually measure the height. |
| Outdoor signal propagation environment | Signal propagation environment in the coverage area | Understand the situation of the coverage area and check whether there are obstacles such as tall buildings and trees around the coverage area. If possible, take photos of some areas for future use or archiving. |

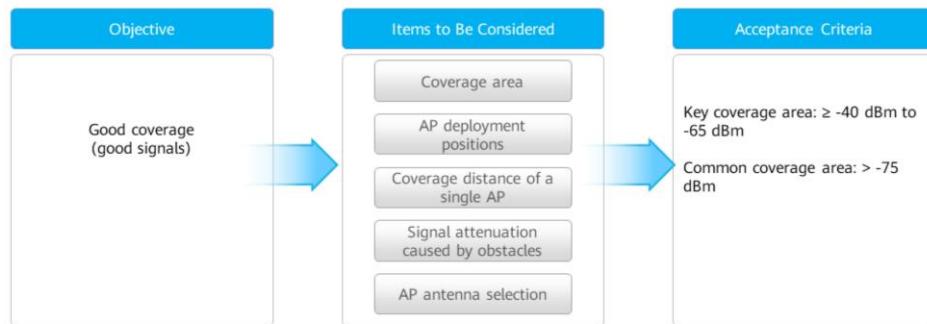
Contents

1. Introduction to WLAN Planning and Design
- 2. WLAN Planning and Design Details**
3. WLAN Project Acceptance
4. WLAN Planning Cases

WLAN Planning and Design



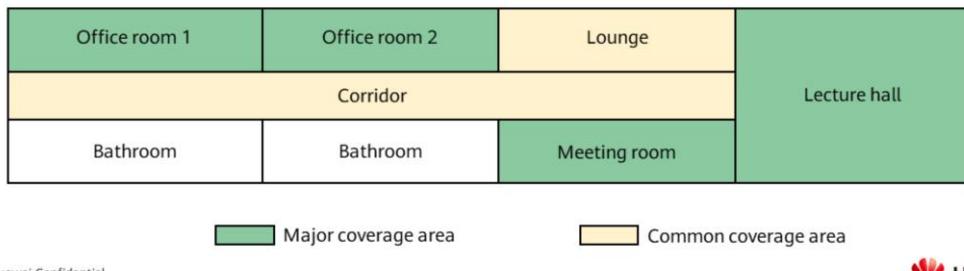
Signal Coverage Design Rules



- The coverage can be simply understood as the number of Wi-Fi signal bars on a mobile phone.

Signal Coverage Requirement Analysis: Coverage Area

| Coverage | Field Strength | Typical Area in Common Projects |
|-----------------------|--------------------|---|
| Major coverage area | -40 dBm to -65 dBm | Dormitory room, library, classroom, hotel room, lobby, meeting room, office, hall, etc. |
| Common coverage area | > -75 dBm | Corridor, kitchen, storeroom, and dressing room |
| Special coverage area | N/A | Areas where coverage or installation is limited or not allowed, for the sake of service security, property management, or other reasons |



- Before planning a project, communicate with the customer to determine the WLAN coverage area based on the onsite environment and drawings.
- Key coverage area: dorm room, library, classroom, hotel room, lobby, meeting room, office room, exhibition hall, etc.
- The area division must be confirmed with the customer and marked on the drawing provided by the customer to facilitate subsequent planning.

Signal Coverage Requirement Analysis: AP Deployment Position

Requirement analysis

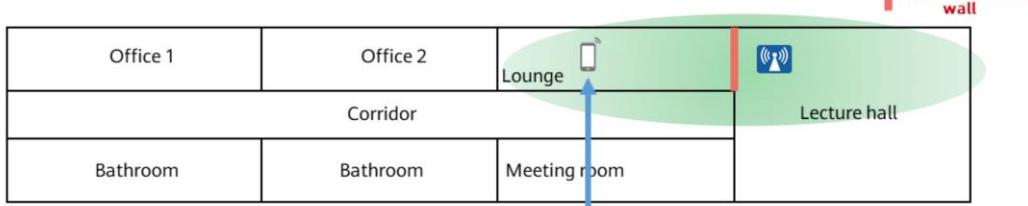
- APs cannot be installed in the lounge.
- APs in the lecture hall are used to provide signal coverage (with -75 dBm field strength).

Site survey

- The signal attenuation value of the wooden partition wall is 5 dBm.

Coverage analysis

- Final signal field strength = AP transmit power + Antenna gain – Transmission attenuation – Signal attenuation caused by obstacles



Signal field strength at the mobile phone position shown in the figure = 20 (recommended AP transmit power) + 3 (antenna gain) – 60 (transmission attenuation) – 5 (signal attenuation caused by obstacles) = **-42 dBm**

Note: When the built-in antenna is used, the transmit power and antenna gain are calculated together to simplify memorization.

- You can obtain the antenna gain from the product documentation.
- The attenuation value of the transmission distance is obtained through calculation.

Signal Coverage Requirement Analysis: Coverage Distance and Attenuation of a Single AP

- Coverage distance by a single AP

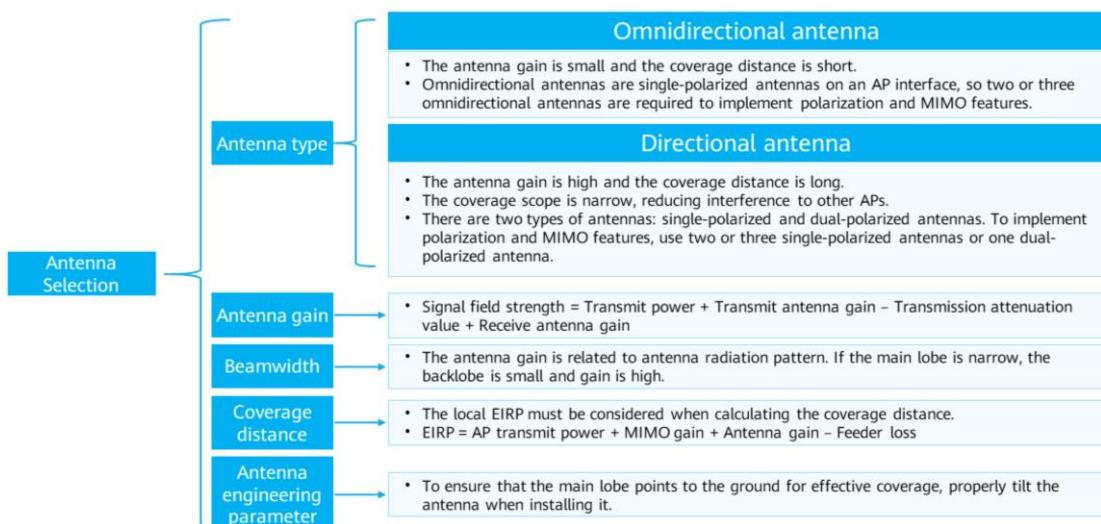
| Distance | 1 m | 2 m | 5 m | 10 m | 20 m | 40 m | 80 m | 100 m |
|----------|-------|---------|---------|-------|---------|--------|----------|--------|
| 2.4 GHz | 46 dB | 53.5 dB | 63.5 dB | 71 dB | 78.5 dB | 86 dB | 93.6 dB | 96 dB |
| 5.8 GHz | 53 dB | 62 dB | 74 dB | 83 dB | 92 dB | 101 dB | 110.1 dB | 113 dB |

- Signal attenuation caused by common obstacles

| Obstacle | Thickness (mm) | 2.4 GHz Signal Attenuation (dB) | 5 GHz Signal Attenuation (dB) |
|---------------------|----------------|---------------------------------|-------------------------------|
| Synthetic material | 20 | 2 | 3 |
| Asbestos | 8 | 3 | 4 |
| Wood door | 40 | 3 | 4 |
| Glass window | 50 | 4 | 7 |
| Heavy colored glass | 80 | 8 | 10 |
| Brick wall | 120 | 10 | 20 |
| Brick wall | 240 | 15 | 25 |
| Armored glass | 120 | 25 | 35 |
| Concrete | 240 | 25 | 30 |
| Metal | 80 | 30 | 35 |

- Formula for calculating the signal field strength (ignoring interference and cable loss):
- Received signal field strength = AP's transmit power + Antenna gain – Transmission attenuation – Penetration loss
- When the signal transmission distance is 20 m, the signal field strength (5.8 GHz) is calculated as follows:
- AP transmit power (20 dBm) + Antenna gain (omnidirectional antenna: 3 dBi) – Transmission attenuation (92 dB) – Signal attenuation caused by obstacles (0 dB) = -69 dBm
- Antenna gain: Indoor APs generally use built-in omnidirectional antennas, and the antenna gain is 3 dBi.

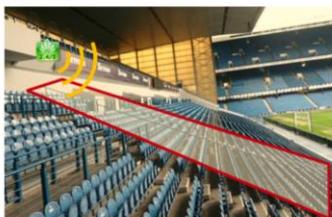
Signal Coverage Requirement Analysis: Antenna Selection



- EIRP: Effective Isotropic Radiated Power
- $EIRP \geq AP\ transmit\ power + MIMO\ gain + Antenna\ gain - Feeder\ loss$

Signal Coverage Requirement Analysis: Device Selection Case

- Case: Stadium



Edge coverage



Ceiling coverage

Device selection procedure

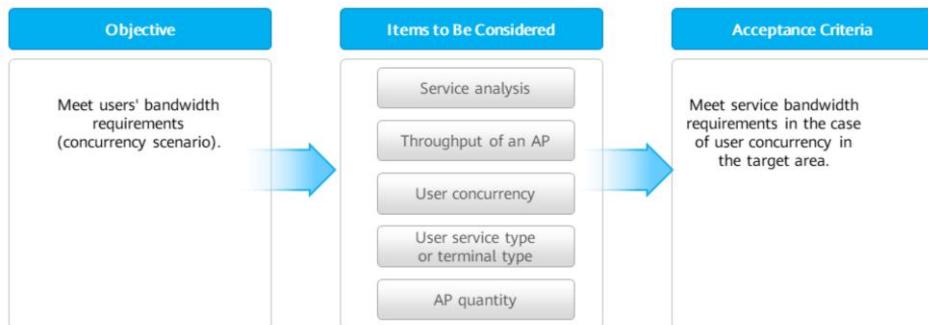
- AP selection: The customer requires the APs in compliance with 802.11ax (Wi-Fi 6) to provide signal coverage for the stand. Therefore, select outdoor models that support external antennas.
- Antenna selection:
 - Antenna gain: Determine the antenna gain based on the AP transmit power, coverage distance, and bandwidth requirements.
 - Antenna angle: The stadium is a high-density scenario. Therefore, the antenna angle should be as small as possible. For example, small-angle antennas (horizontal angle 15° and vertical angle 15°) are used at 5.8 GHz frequency band.
 - Antenna engineering parameters: The azimuth and downtilt are adjustable during deployment and need to be planned based on site requirements.

- AP selection: The stand is located outdoors. The customer requires the APs in compliance with 802.11ax (Wi-Fi 6), so outdoor models with external antennas, such as AirEngine 8760R-X1E (supporting PoE power supply), can be selected.
- Antenna selection
 - Antenna gain: Determine the antenna gain based on the AP transmit power, coverage distance, and bandwidth requirements.
 - Antenna angle: The stadium is a high-density scenario. Therefore, the antenna angle should be as small as possible. For example, ANT5G19D2NR (horizontal angle 15° and vertical angle 15°) is used at 5.8 GHz frequency band.
 - Antenna engineering parameters: The azimuth and downtilt are adjustable during deployment. Plan the azimuth and downtilt based on site requirements.

WLAN Planning and Design



Capacity Design Rules



- The user bandwidth can be simply understood as the network bandwidth required by a STA to use a service.
- User concurrency and bandwidth requirements vary with areas, so the design should be based on different scenarios and areas.

Service Analysis

| Service Type | Single-Service Baseline Rate (Mbps) | | Proportion of Services in Different Scenarios | | | |
|-------------------------|-------------------------------------|-------|---|---------|----------------------|----------------|
| | Excellent | Good | Meeting Room | Canteen | Multimedia Classroom | Office Area... |
| Web page browsing | 8 | 4 | 50% | 60% | 20% | ... |
| Streaming media (1080p) | 16 | 12 | 10% | 10% | 50% | ... |
| Streaming media (4K) | 50 | 22.5 | 0% | 0% | 0% | ... |
| VoIP (voice) | 0.25 | 0.125 | 10% | 0% | 0% | ... |
| Electronic whiteboard | 32 | 16 | 10% | 0% | 0% | ... |
| Email | 32 | 16 | 5% | 0% | 0% | ... |
| File transfer | 32 | 16 | 0% | 0% | 0% | ... |
| Desktop sharing | 2.5 | 1.2 | 0% | 0% | 20% | ... |
| Gaming | 2 | 1 | 0% | 0% | 0% | ... |
| Instant messaging | 0.5 | 0.25 | 15% | 30% | 10% | ... |

Calculate the capacity based on specified service bandwidth and concurrency in specific scenarios. If required bandwidth is not specified in a specific scenario, you can evaluate the bandwidth based on the scenario-specific bandwidth requirements.

In a meeting room scenario, to evaluate the bandwidth for excellent experience, the formula is as follows:

Bandwidth required by a single user = $8*50\% + 16*10\% + 0.25*10\% + 32*10\% + 32*5\% + 0.5*15\% = 10.5 \text{ Mbps}$

- Total bandwidth = Number of users x Concurrency rate x Bandwidth for each user
- Number of APs = Total bandwidth/Bandwidth of each AP

Throughout Design Rules

- Throughput refers to the total amount of data that an AP can transmit per unit time. Throughput is calculated using the following formula:

$$\text{Throughput} = \text{User access bandwidth} \times \text{Maximum number of concurrent STAs}$$

- Throughput design example

Assume that a customer wants to use Wi-Fi 6 and requires 8 Mbps access bandwidth per user. In this case, the required throughout of a single-radio AP is 120 Mbps (8×15) and that of a dual-radio AP is 192 Mbps (8×24).

| Maximum Number of Concurrent STAs with Different Bandwidths (Dual Spatial Streams, 802.11ax) | | | |
|--|------------------------------------|--|---|
| No. | User Access Bandwidth (Per Capita) | Maximum Number of Concurrent STAs (Single Radio) | Maximum Number of Concurrent STAs (Dual Radios) |
| 1 | 2 Mbps | 42 | 72 |
| 2 | 4 Mbps | 24 | 41 |
| 3 | 6 Mbps | 18 | 29 |
| 4 | 8 Mbps | 15 | 24 |
| 5 | 16 Mbps | 9 | 14 |
| 6 | 50 Mbps | 3 | 5 |

WLAN Network Planning Specifications (1)

- Bandwidth requirement of a single STA (dual spatial streams, Wi-Fi 5) and maximum number of concurrent STAs

| Maximum number of concurrent STAs with different bandwidths on Wi-Fi 5 APs | | | | |
|--|-----------------------|--|---|---|
| No. | User Access Bandwidth | Maximum Number of Concurrent STAs (Single Radio) | Maximum Number of Concurrent STAs (Dual Radios) | Maximum Number of Concurrent STAs (Triple Radios) |
| 1 | 1 Mbps | 30 | 55 | 85 |
| 2 | 2 Mbps | 22 | 40 | 62 |
| 3 | 4 Mbps | 12 | 22 | 34 |
| 4 | 6 Mbps | 11 | 20 | 31 |
| 5 | 8 Mbps | 10 | 18 | 28 |
| 6 | 16 Mbps | 5 | 9 | 14 |

This table is an important basis for AP model selection (single radio, dual radios, or triple radios) and AP quantity design.

- The maximum number of concurrent STAs (single radio) is based on the 5 GHz frequency band.
- The maximum number of concurrent STAs (dual radios) is based on 2.4 GHz and 5 GHz frequency bands.
- The maximum number of concurrent STAs (triple radios) is based on one 2.4 GHz frequency band and two 5 GHz frequency bands.

WLAN Network Planning Specifications (2)

- Bandwidth requirement of a single STA (dual spatial streams, Wi-Fi 6) and maximum number of concurrent STAs

| Maximum number of concurrent STAs with different bandwidths on Wi-Fi 6 APs | | | | |
|--|-----------------------|--|---|---|
| No. | User Access Bandwidth | Maximum Number of Concurrent STAs (Single Radio) | Maximum Number of Concurrent STAs (Dual Radios) | Maximum Number of Concurrent STAs (Triple Radios) |
| 1 | 2 Mbps | 42 | 72 | 114 |
| 2 | 4 Mbps | 24 | 41 | 65 |
| 3 | 6 Mbps | 18 | 29 | 47 |
| 4 | 8 Mbps | 15 | 24 | 39 |
| 5 | 16 Mbps | 9 | 14 | 23 |

This table is an important basis for AP model selection (single radio, dual radios, or triple radios) and AP quantity design.

- The preceding table assumes that the AP supports 802.11ax 8*8 HT20 mode. The following sections assume that APs support 802.11ax 8*8 HT20 and STAs support 802.11ax dual spatial streams.

Scenario-based AP Quantity Calculation

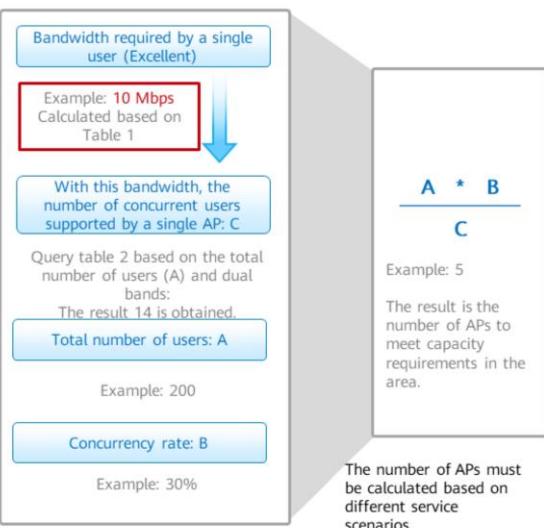
Table 1

| Service Type | Single-Service Baseline Rate (Mbps) | | Percentage |
|-------------------------|-------------------------------------|-------|------------|
| | Excellent | Good | |
| Web page browsing | 8 | 4 | 50% |
| Streaming media (1080p) | 16 | 12 | 10% |
| Streaming media (4K) | 50 | 22.5 | 0% |
| VoIP (voice) | 0.25 | 0.125 | 10% |
| Electronic whiteboard | 32 | 16 | 10% |
| Email | 32 | 16 | 5% |
| File transfer | 32 | 16 | 0% |
| Desktop sharing | 2.5 | 1.2 | 0% |
| Gaming | 2 | 1 | 0% |
| Instant messaging | 0.5 | 0.25 | 15% |

Table 2

| Maximum number of concurrent STAs with different bandwidths (dual spatial streams, 802.11ax) | | |
|--|--|---|
| User Access Bandwidth | Maximum Number of Concurrent STAs (Single Radio) | Maximum Number of Concurrent STAs (Dual Radios) |
| 8 Mbps | 15 | 24 |
| 16 Mbps | 9 | 14 |
| ... | ... | ... |

601 Huawei Confidential



- Bandwidth required by a single user (Excellent) in a meeting room = $8*50\% + 16*10\% + 0.25*10\% + 32*10\% + 32*5\% + 0.5*15\% = 10.5$ Mbps
- The total number of users refers to the total number of STAs connected to the WLAN in this scenario.
- The number of concurrent STAs is the concurrency rate multiplied by the total number of users, and refers to the number of users that are connected to the WLAN and transmit data.
- The concurrency rate is an empirical value.

WLAN Planning and Design



Device Model Selection Factors

| | |
|--|--|
| MIMO | The number of spatial streams ranges from 4 to 12. An AP with more spatial streams supports higher throughput and larger access capacity. Therefore, select APs with a proper number of spatial streams based on the application scenario and access density. |
| Antenna | Indoor APs support omnidirectional, directional, and smart antennas. Outdoor APs support omnidirectional and directional antennas. Indoor scenario: Smart antennas provide the best coverage effect. Therefore, APs with smart antennas are recommended. Directional antennas are suitable for high installation scenarios. Omnidirectional antennas are suitable for scenarios where the coverage area is small and the deployment is not dense. Outdoor scenario: Use directional antennas for long-distance coverage and wireless backhaul, and omnidirectional antennas for short-distance coverage. |
| Maximum transmit power (combined power) | The Wi-Fi transmit power is controlled by the country code and varies depending on the local regulations. When the transmit power gets closer to the specified upper limit, the transmitted signal is stronger and the coverage distance is longer. For details, see the <i>Channel and Power Restrictions</i> in the product documentation. |
| Antenna gain | A higher antenna gain indicates a stronger signal strength and longer coverage distance. Therefore, the AP with a higher antenna gain is preferred. |
| Power supply | The power supply mode is related to the deployment scenario. Currently, PoE power supply is used in most scenarios. You can also use a power supply or use dual power supplies for backup. |
| Wi-Fi standard | The Wi-Fi standard has evolved to the sixth generation, and each generation of the standard is compatible with earlier ones. The latest Wi-Fi 6 standard greatly improves the Wi-Fi speed and capacity, and achieves a four-fold increase in the throughput and capacity. Therefore, Wi-Fi 6 APs are recommended. |

WLAN Planning and Design



Channel Design

- **Confirm with customers about available channels allowed by the local laws and regulations.**
 - For example, the available 5 GHz channels for bridge backhaul transmission are 149, 153, 157, 161, and 165.
 - Available channels in each country or region are different. Some countries or regions may reserve some channels. Confirm the local available channels before performing network planning.
- **Avoid co-channel interference.**
 - In the case of multiple floors, avoid overlapping with channels of APs at the same or adjacent floors.
 - If channel overlapping cannot be avoided, reduce AP power to minimize the overlapping areas.



Channel Planning Rules



606 Huawei Confidential



- Confirm with customers about available channels allowed by the local laws and regulations.
 - Query the local available channels in the channel compliance table and confirm with the local user.
 - For example, channels 1, 6, and 11 are available on the 2.4 GHz frequency band in China.
 - To prevent interference between channels, the interval between central frequencies of each two channels in the 2.4 GHz frequency band must be larger than or equal to 25 MHz. It is recommended that channels 1, 6, and 11 be used in overlapping mode.
 - Available channels on the 5.8 GHz band: 149, 153, 157, 161, and 165
 - Some channels may be reserved in different countries or regions. Therefore, you need to confirm the reserved channels before the planning.
- Avoid co-channel interference.
 - Do not use the same channel in any direction.
 - In the case of multiple floors, avoid overlapping with channels of APs at the same or adjacent floors.
 - If channel overlapping cannot be avoided, reduce AP power to minimize the overlapping areas.
 - Channel compliance:
 - The available channels and the maximum transmit power of radio signals in the channels vary according to countries and regions. Radio signals in different channels may have different signal strengths.

WLAN Planning and Design



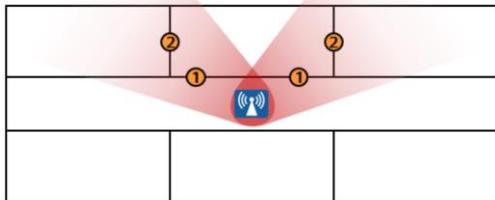
AP Deployment Design

- Channel Planning - Indoor Settled APs
 - Reduce cross-floor interference.
 - Avoid channel conflicts.
 - Plan channels uniformly.

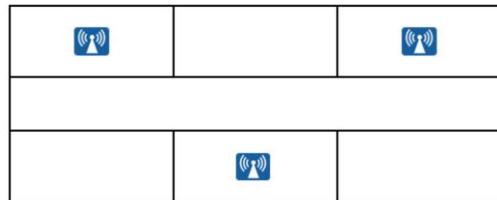
| Floor Number | Three APs on One Floor | | |
|---------------|------------------------|----|----|
| Seventh floor | 1 | 6 | 11 |
| Sixth floor | 11 | 1 | 6 |
| Fifth floor | 6 | 11 | 1 |
| Fourth floor | 1 | 6 | 11 |
| Third floor | 11 | 1 | 6 |
| Second floor | 6 | 11 | 1 |
| 1st floor | 1 | 6 | 11 |

- For channel distribution, ensure the minimum co-channel interference and prevent cross-layer interference.
- If the AP's channels conflict with channels of users' Wi-Fi devices, adjust the channel distribution.
- If channel conflicts cannot be avoided by adjusting APs' channel distribution, discuss with the owners of the Wi-Fi devices to re-distribute the channels.

AP Deployment Rules



Improper AP deployment: Signals penetrate several walls.

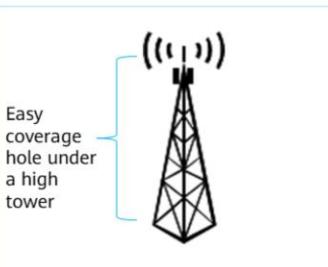


Proper AP deployment: Signals penetrate one wall.

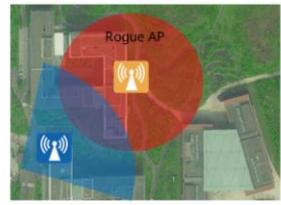
- When installing an AP, try to reduce the number of obstacles that signals traverse.
- Ensure that the front side of an AP faces the target coverage area and the APs are far away from the interference source.
- If PoE power supply is required, consider the distance between an AP and ELV room. It is recommended that the distance be less than 80 m. If PoE++ power supply is used, it is recommended that the distance be less than 200 m.

AP Deployment Design

- Site design rules (outdoors)



Radar stations, radio transmitters, and television transmitters



Preventing channel interference of APs in other systems

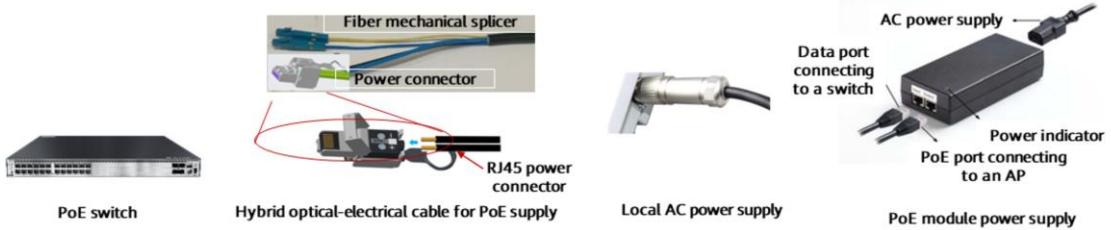
- The path between a site and its coverage area must be visible and cannot be blocked by obstacles.
- Avoid heavy electromagnetic interference or other signal interference near the site
- Reliable power sources must be available for a site.

WLAN Planning and Design



Power Supply and Cabling Design: Power Supply Mode Design

- PoE power supply (recommended)
 - PoE switches are used for data transmission and power supply of APs (through Ethernet cables or hybrid optical-electrical cables).
- Local power supply
 - Non-PoE switches forward data packets sent from APs, and APs use independent power supplies.
- PoE module power supply
 - PoE injectors are used for data transmission and power supply of APs.



612 Huawei Confidential

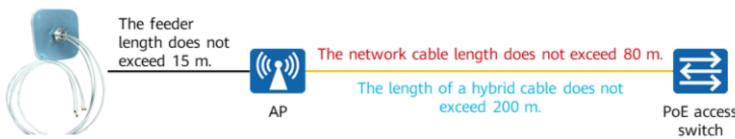
 HUAWEI

- Local power supply is inconvenient. Exposed power cables affect the appearance and bring security risks.
- The PoE module supplies power and does not require power supply. However, a potential fault point is added, which is inconvenient for maintenance.
- PoE power supply is used, which facilitates construction and solves the problem of difficult power supply. The power supply is stable and secure.
- Hybrid cable: Currently, optical data is transmitted over the network port, and the transmission distance can reach 200 m.
 - Advantage: The cost of one-time cabling is low and the service life is long. Hybrid cables apply to long-distance power supply scenarios and reduces the PoE power supply distance.
 - Disadvantage: Hybrid optical-electrical switches are required, resulting in high costs. Optical modules are expensive, and one cable occupies two physical ports (one optical port and one electrical port). This means that more switches are used.

Power Supply and Cabling Design: Cabling Design

Cabling design rules

- The length of Ethernet cables between a switch and APs does not exceed 80 m.
- The length of hybrid optical-electrical cables between a switch and APs does not exceed 200 m.
- Reserve about 5 m of an Ethernet cable or optical/electrical hybrid cable at the AP side for future adjustment.
- Keep cables away from strong electromagnetic sources.
- Confirm with customers in advance so that customers will not stop engineering for property and appearance considerations.
- The longer the feeder, the weaker the signal strength within the antenna coverage range. The feeder should be as short as possible. The 15-m feeder is not recommended.



• Cabling design rules:

- In normal cases, the length of network cables cannot exceed 100 m due to signal attenuation. However, in actual projects, network cables are used to supply power to APs. If the length of a network cable exceeds 80 m, the network is affected. Therefore, it is recommended that the length of a network cable be less than or equal to 80 m.
- It is recommended that about 5 m be reserved for a network cable during AP deployment so that you can adjust AP locations for WLAN signal optimization. If signals are of poor quality, engineers can flexibly adjust AP locations to ensure good coverage.
- To avoid interference of high-voltage cables, it is recommended that low-voltage cables be deployed as far as possible from strong electromagnetic field.
- During cabling planning, communicate with the customer in advance about all the lines to prevent the construction progress from being affected by the customer's disagreement on the construction due to the property and aesthetic factors.

WLAN Planning and Design



Indoor Settled AP Installation Modes and Rules

Ceiling mounting



Wall mounting



Support mounting



- The installation mode is detailed as follows:

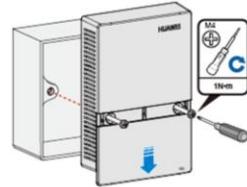
- Ceiling mounting (recommended): If the installation height is smaller than 6 m, use APs with omnidirectional antennas. If the installation height is greater than 6 m, use APs with directional antennas.
 - Wall mounting: If APs cannot be installed against the ceiling, the wall mounting mode is recommended.
 - Support mounting: This is a temporary installation mode when ceiling or wall mounting is not supported. This installation mode typically used in temporary exhibition scenarios.

Wall Plate AP Installation Mode

Desk-mounting



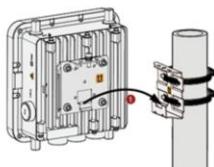
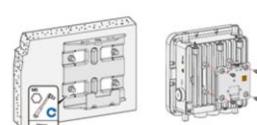
Panel mounting



- Installation modes:

- In addition to ceiling-mounted and wall-mounted installation modes, an indoor AP can also be installed on a desk or panel.
 - That is, an AP can be placed on the desktop or junction box (86 mm) in a room.

Installation Mode of Outdoor APs and Antennas

| Pole mounting | Wall Mounting | Installation modes and rules of outdoor antennas |
|--|--|--|
|   |   |  <ul style="list-style-type: none">• The azimuth and downtilt of an antenna can be flexibly adjusted based on the auxiliary mounting kits.• An AP can be installed on a wall without adjusting the antenna angle.• Outdoor omnidirectional antennas are installed at a height of 4 m to 6 m, and directional antennas are installed at a height of 6 m to 8 m. |

618 Huawei Confidential



- Outdoor installation mode:
 - The azimuth and downtilt of an antenna can be flexibly adjusted based on the auxiliary mounting kits.
 - An AP can be installed on a wall without adjusting the antenna angle.
 - Outdoor omnidirectional antennas are installed at a height of 4 m to 6 m, and directional antennas are installed at a height of 6 m to 8 m.

Contents

1. Introduction to WLAN Planning and Design
2. WLAN Planning and Design Details
- 3. WLAN Project Acceptance**
4. WLAN Planning Cases

WLAN Coverage Performance Acceptance Test

| WLAN signal field strength test | |
|---------------------------------|--|
| Objective | To verify that the WLAN signal strength in the target coverage area meets requirements. |
| Prerequisites | <ul style="list-style-type: none">The WLAN system is working properly.Testing devices and tools are ready. The latest version of CloudCampus@AC-Campus or inSSIDer has been downloaded and installed. |
| Test procedure | <ul style="list-style-type: none">Measurement point selection: Select typical positions that can reflect the signal coverage performance in the target coverage area, for example, edge of the target area, places where the users farthest from the antennas usually reside to connect to the Internet, and the area with the highest user density (major coverage area).After the STA at a measurement point successfully associates with a tested AP, start the WLAN testing tool or software to measure the RSSI of APs using the SSID to be tested. Measure the RSSI for more than 30s and calculate the average value or obtain a stable value. |
| Expected results | The RSSI is higher than or equal to -70 dBm in over 95% of the target coverage area. The RSSI is higher than or equal to -68 dBm in over 95% of the major coverage area. |
| Test result | <ul style="list-style-type: none">The WLAN testing tool and a laptop are used to collect test results. |

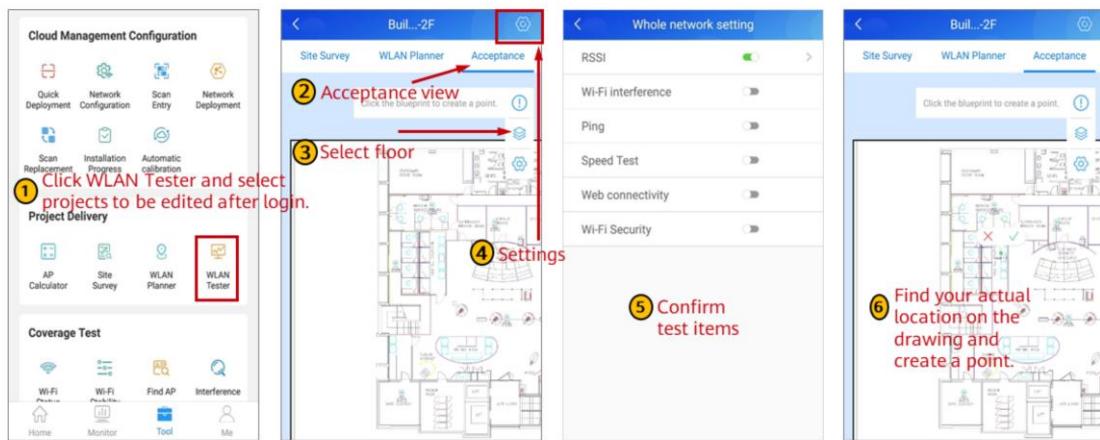
Service Performance Test Acceptance

| Network ping test | |
|-------------------|--|
| Objective | <ul style="list-style-type: none">To verify that the ping latency and packet loss ratio meet the project design requirements and acceptance criteria. |
| Prerequisites | <ul style="list-style-type: none">The WLAN system is working properly.Testing devices and tools are ready. |
| Test method | <ul style="list-style-type: none">Measurement point selection: Select typical positions that can reflect the signal coverage performance in the target coverage area, for example, edge of the target area, places where the users farthest from the antennas usually reside to connect to the Internet, and the area with the highest user density (major coverage area).Start a STA and make it associate with an AP and connect to the WLAN.Ping the local gateway from the STA. Set the ping packet size to 1500 bytes and send ping packets 100 times.Record the parameters such as the average latency and packet loss ratio. |
| Expected result | <ul style="list-style-type: none">The average latency of ping packets is less than or equal to 50 ms.The ping packet loss ratio does not exceed 3%. |

- Website access test
 - Test objective: To verify that HTTP website access delay and success rate meet the project design requirements and acceptance criteria.
 - Test method: At each measurement point, use a STA to connect to the WLAN. Enter the user name and password for web authentication, open homepages of different portal websites, and record the access delay and success rate.
 - Expected result: After the user enters the authentication user name and password, the latency for displaying the authentication success page is less than or equal to 3s. The website access success rate is greater than or equal to 95%.
- DHCP test
 - Test objective: To verify that STAs connected to the AP can obtain IP addresses.
 - Test method: Set the number of test times in advance and interval between two consecutive tests in advance. The STA successfully associates with the AP and accesses the network. The STA connects to the AP through the wireless network adapter to obtain an IP address.
 - Expected result: The IP address can be obtained.
- File synchronization test on the intranet server:
 - Test objective: To verify the download rate of the WLAN device.
 - Test method: Associate a STA with an SSID and ping the test PC. Enable the STA to download a 200 MB file from the intranet server.
 - Expected result: The STA successfully associates with the SSID and pings the test PC. If there is no interference, the download is complete within 3 minutes.

Project Acceptance (1/5)

- Using CloudCampus APP for acceptance



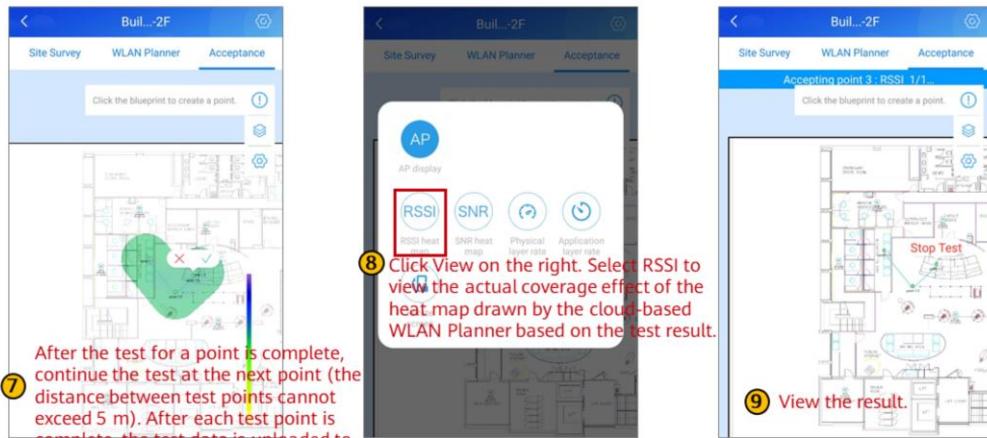
623 Huawei Confidential

HUAWEI

- Tool name: WLAN Planner
 - Function: online network planning tool. It does not need to be installed. You can use it directly after logging in to it using a uniportal account. It supports automatic identification of obstacles in drawings of .pdf, .jpg, .png, and .bmp formats. You do not need to download the latest version or apply for a license. The Google Chrome browser is recommended.
 - To obtain the tool and manual, visit <https://serviceturbo-cloud-cn.huawei.com/#/toolappmarket>.
- Tool name: CloudCampus APP
 - Function: tool for WLAN project delivery throughout the project lifecycle
 - AP Calculator: Quickly estimate the material list in the pre-sales phase to provide guidance for quotation.
 - Site Survey: Connect to WLAN Planner to record photos and texts based on drawings.
 - WLAN Planner: Connect to WLAN Planner to display network planning results, heatmaps, and AP attributes anytime anywhere.
 - WLAN Tester: Support one-click Wi-Fi health check, multi-point acceptance, and roaming test to meet test requirements of daily Wi-Fi projects. In addition, Excel data and Word reports can be exported. In addition, the antenna alignment function is supported.
 - To obtain the tool and manual, search for CloudCampus APP in Huawei AppGallery, Google Play, or APP Store, or download CloudCampus_APP from the forum link.

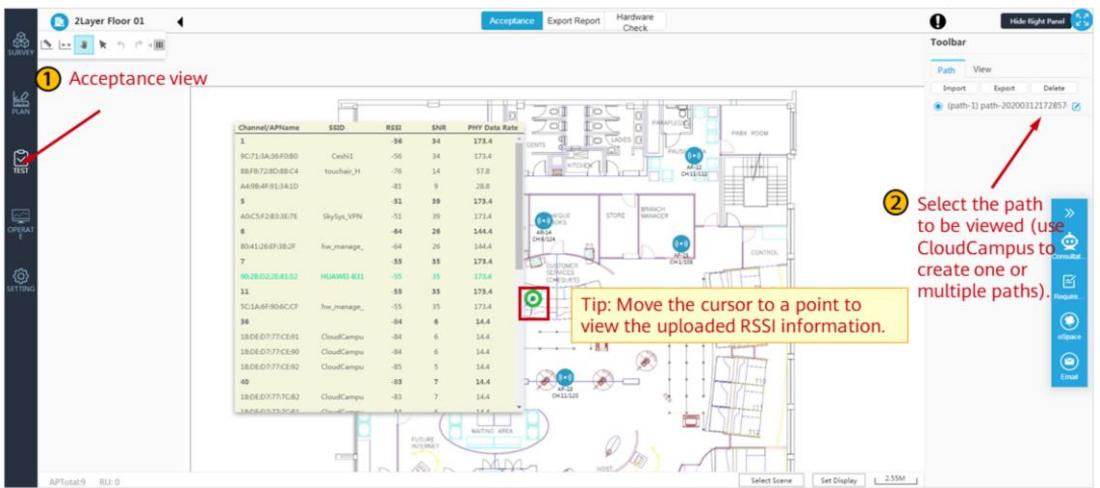
Project Acceptance (2/5)

- Using CloudCampus APP for acceptance



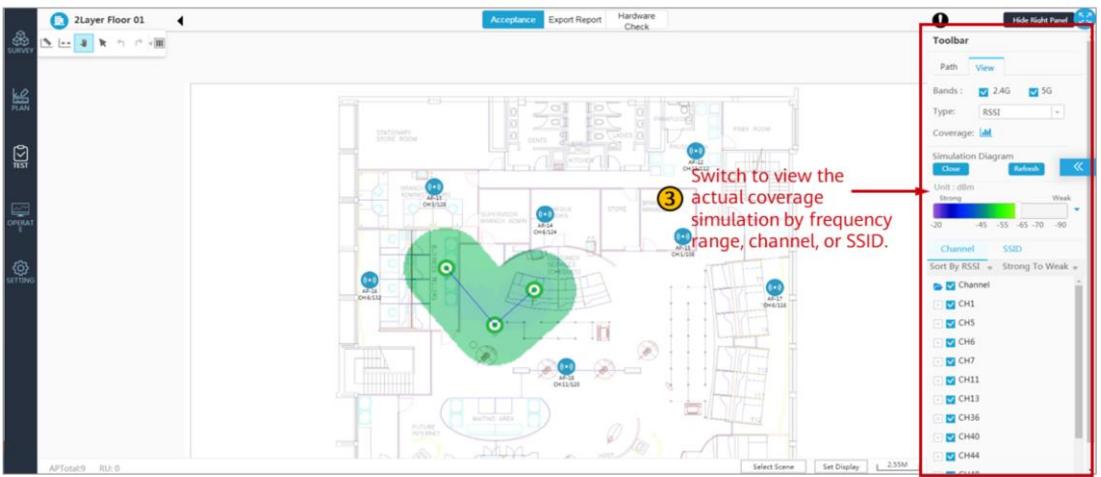
Project Acceptance (3/5)

- Viewing on WLAN Planner



Project Acceptance (4/5)

- Viewing on WLAN Planner



Project Acceptance (5/5)

- Viewing acceptance test results on the cloud

The screenshot shows the 'Acceptance' tab of the WLAN Report interface. A red arrow points from the text below to the 'Format' dropdown, which is set to 'Word'. The 'Acceptance Report' section includes fields for Language (Chinese, English), Bands (2.4G, 5G, 2.4G/5G), Heat Map Content (RSSI, SNR, Physical Layer Rate, Application Layer Rate), Multi-point Test (Point Detail, Ping, MOS, Speed Test, RSSI, WiFi Interference, Web Connect), and a 'Choose Path to Export' table.

④ Export the acceptance report in Word or PDF format. The report can be filtered by multiple dimensions, including test area, test path, test item, frequency band, SSID, BSSID, and channel.

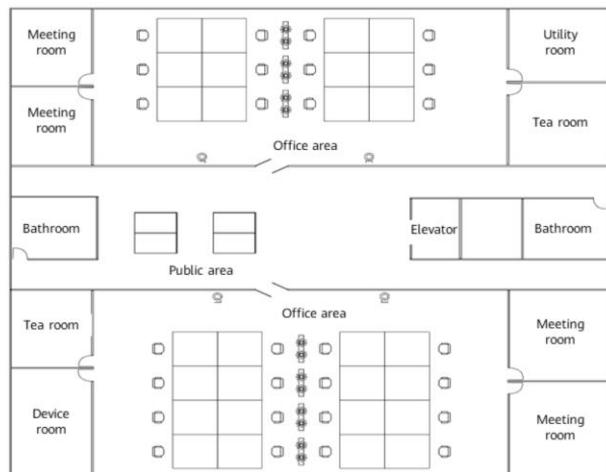
| AP | SSID | Channel |
|----------------------|-------|--------------|
| | BSSID | BSSID Number |
| 78 | | 3 |
| 789 | | 2 |
| BoCloud-Public | | 1 |
| BoCloud-Public-5G | | 1 |
| ccg-quiet | | 1 |
| Ceshi1 | | 2 |
| CloudCampus_guest | | 3 |
| CloudCampus_Open | | 3 |
| CloudCampus_passcode | | 3 |
| HQO | | 2 |
| HUAWEI-8315-8152 | | 1 |
| hw_manage_3820 | | 1 |

Contents

1. Introduction to WLAN Planning and Design
2. WLAN Planning and Design Details
3. WLAN Project Acceptance
- 4. WLAN Planning Cases**

Planning Case: Indoor Settling Project in the Office Area (1/3)

- Office building drawings:



Planning Case: Indoor Settling Project in the Office Area (2/3)

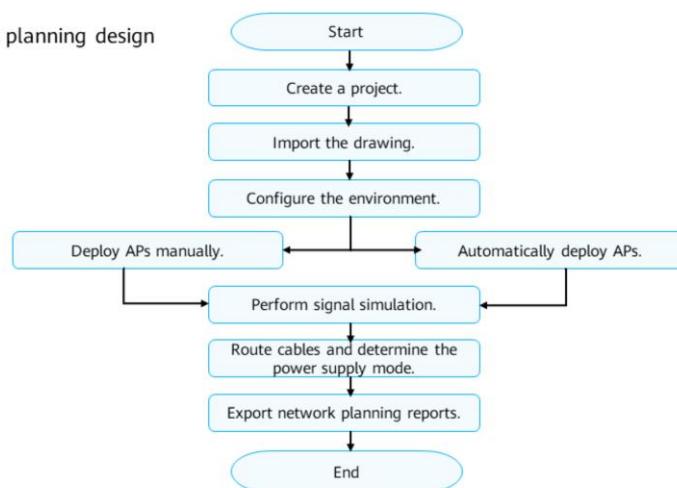
- User requirement collection:

| Requirement | Description |
|------------------------|---|
| Coverage Area | The coverage area locates on the third floor of an office building, with a space of 130 m x 80 m. Office seats and meeting rooms are the major coverage area, and corridors and tea rooms are the common coverage area. |
| Field strength | Ensure that the major office area can receive signals. |
| Number of access users | About 100 users. For details about the distribution, see the drawing. |
| Bandwidth | At least 1 Mbit/s for each user |
| Coverage mode | Indoor settled |
| Power supply mode | PoE power supply |
| Switch location | Switches are deployed in the room next to the stair in the upper right corner of the office area. |

- In the onsite environment, most buildings use concrete, glass walls, and wooden doors, and there is no third-party or non-Wi-Fi interference source. Confirm with the customer that cables are routed on the ceiling.
- Device selection:
 - In indoor settled deployment scenarios, the latest indoor AirEngine Wi-Fi 6 model can be used. Compared with a Wi-Fi 5 AP, the AirEngine Wi-Fi 6 indoor model has higher performance, supports access of STAs complying with multiple protocols, and has industry-leading smart antennas. Therefore, signals can move with users and are more stable.
- Coverage design:
 - Use obstacles with high signal attenuation, such as load-bearing walls, to divide a large coverage area into multiple small coverage areas. In this project, the office area and meeting room are divided into eight areas. A single AP can meet the requirements of each area. Therefore, a total of eight APs are required.
- Deployment design:
 - Each AP is deployed on the ceiling in the middle of a small coverage area. Channels of an AP are staggered with that of other APs (such as 1/149, 6/153, and 11/157).

Planning Case: Indoor Settling Project in the Office Area (3/3)

- Logic of network planning design using tools:



632 Huawei Confidential



- Link to the planning tool: <https://serviceturbo-cloud.huawei.com/serviceturbocloud/#/Toolsummary?entityId=d59de9ac-e4ef-409e-bbdc-eff3d0346b42>
- The following figure shows the process of WLAN network planning in indoor scenarios.
- Create a project.
 - Before you use WLAN Planner to plan the WLAN, you need to create a project, select a country where the network is planned, and set the environment type.
- Import the drawing.
 - After you create a project, you need to create a building and import the drawing, so that you can set the environment type and deploy APs on the drawing to simulate the WLAN planning.
- Configure the environment.
 - You can set obstacles, coverage areas, and interference sources on the drawing to simulate the actual environment, making the simulation more nature.
- Deploy APs.
 - Automatically deploy APs.
 - WLAN Planner automatically calculates the number, locations, and working channels of APs based on the obstacle status (locations and types) and requirements on the coverage areas (such as the AP type, minimum field strength, and signal type), and places the calculated APs on the drawing.
 - Deploy APs manually.
 - Based on the actual environment and deployment experience, you can manually deploy APs using the tool to meet users' signal coverage requirements.

Quiz

1. (Single choice) Which of the following obstacles will cause the highest attenuation of 2.4 GHz signals if they have the same thickness?
A. Metal B. Asbestos C. Wooden door D. Tinted glass
2. (Multiple choice) Which of the following belongs to the AP deployment principle?
A. When installing an AP, try to reduce the number of obstacles that signals traverse.
B. Ensure that the front side of an AP faces the coverage area.
C. Deploy APs in concealed places.
D. Deploy APs far from interference sources.
3. Why is channel planning required? How to plan channels?

- 1. A
- 2. ABD
- Why is channel planning required? How to plan channels?
 - To prevent interference between channels, the interval between central frequencies of each two channels in the 2.4 GHz frequency band must be larger than or equal to 25 MHz. It is recommended that channels 1, 6, and 11 be used in overlapping mode.
 - In the 5.8 GHz frequency band, non-overlapping channels 149, 153, 157, 161, and 165 are used, with 20 MHz of separation between each two channels.

Summary

After completing this course, you understand the following:

- WLAN planning and design process
- WLAN planning basics
- WLAN capacity, frequency, and coverage planning rules

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors
that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.

