

Huawei Access Points

FAQ

Issue **01**
Date **2014-01-25**

Copyright © Huawei Technologies Co., Ltd. 2014. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://enterprise.huawei.com>

About This Document

Declaration

This document is applicable to all product versions. The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Intended Audience




This document describes the questions you may encounter during the installation, configuration, and maintenance of the device and provides the answers.



This document is intended for:

- System maintenance engineers
- Commissioning engineers
- Network monitoring engineers
- Onsite maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Remarks
 DANGER	Indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.
 WARNING	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.

Symbol	Remarks
 TIP	Provides a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italic</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Security Conventions

- Password setting

When configuring a password in plain text, the password is saved in the configuration file in plain text. The plain text has high security risks, so the cipher text is recommended. To ensure device security, change the password periodically.

When you configure a password in cipher text that starts and ends with %@@@.....%@@@ or @@@@.....@@@@ (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting.

- Encryption algorithm

Currently, the device uses the following encryption algorithms: DES, 3DES, AES, RSA, SHA1, SHA-2, MD5 and SMS4. The encryption algorithm depends on the applicable

scenario. Use the recommended encryption algorithm; otherwise, security defense requirements may be not met.

- For the symmetrical encryption algorithm, use AES with the key of 128 bits or more.
- For the asymmetrical encryption algorithm, use RSA with the key of 2048 bits or more.
- For the hash algorithm, use SHA with the key of 256 bits or more.
- For the HMAC algorithm, use HMAC-SHA2.

- **Personal data**

Some personal data may be obtained or used during operation or fault location of your purchased products, services, features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

Change History

Changes between document issues are cumulative. Therefore, the latest document version contains all changes made to previous versions.

Changes in Issue 01 (2014-01-25)

Initial commercial release.

Contents

About This Document.....	ii
1 Protocols and Basic Concepts.....	1
1.1 What Are the Differences Between 802.11a/b/g/n Standards?.....	2
1.2 Where Are Interference Sources in WLAN and How Is the Interference Strength?.....	2
1.3 What Are WLAN Reliability Features?.....	3
1.4 What Are the Relationship and Difference Between WLAN and Wi-Fi?.....	3
1.5 What Are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing?.....	3
1.6 What Are the Differences Between HT20 and HT40, How Is the 11n 40 MHz Channel Is Partitioned, and What Are the Meanings of Plus and Minus?.....	5
1.7 What Is the WLAN Coverage Range?.....	5
1.8 What Are the BSS and SSID?.....	5
1.9 What Is the Working Process of 802.11n Short GI?.....	5
1.10 What Are the Advantages and Disadvantages of FHSS and DSSS?.....	6
1.11 Is the WLAN Rate the Upstream or Downstream Rate?.....	6
1.12 What Are the Physical Rate, Theoretical Rate, and Actual Rate in the 802.11 Standard?.....	6
1.13 What Is the Relationship Between WMM and 802.11e?.....	7
1.14 What Are the Implementations of 802.11n Frame Aggregation Technologies, MSDU and MPDU?.....	7
1.15 Does an AP Listen to and Send Frames over One Channel?.....	8
1.16 How Does a STA Synchronize the Channel When the Associated AP Switches to Another Channel?.....	8
2 Product FAQs.....	10
2.1 AP FAQs.....	11
2.1.1 How Do I View Operations on the Device?.....	11
2.1.2 How Do I Defend Against Bogus DHCP Servers at the User Side?.....	11
2.1.3 How Do I Locate VAP Creation Failure?.....	11
2.1.4 Why Is a VAP Created?.....	11
2.1.5 What States Does an AP Have?.....	12
2.1.6 What Are Characteristics of a Fat AP and a Fit AP? What Are Differences Between Them? What Is the Applicable Scenario?.....	12
2.1.7 How Can I Determine Whether an AP Is Qualified?.....	13
2.1.8 How Many Access Users Are Recommended for Each AP?.....	14
2.1.9 Do APs Support Power Adjustment and What Is the Power Adjustment Mechanism?.....	14
2.1.10 How Many Users Does an AP with Different Performance Support in 802.11n Mode?.....	14

2.1.11 Does an AP Configured with Multiple SSIDs Support the Same Number of Access Users as an AP Configured with One SSID?.....	15
2.1.12 Can an AP (Single Radio) with Different SSIDs Work at Different Channels?.....	15
2.1.13 Is the Number of Access Users in Dual-band Mode Twice the Number of Access Users in Single-band Mode?.....	15
2.1.14 Can 802.11n Devices Work Only in 802.11n Mode? Can 802.11n Devices Work in 802.11bg Mode?.....	15
2.1.15 What Methods Does an AP Use to Prevent Interference?.....	15
2.1.16 How Does an AP Adjust the Rate?.....	15
2.1.17 Can Huawei 802.11n APs Automatically Switch Between 2.4 GHz and 5 GHz?.....	15
2.1.18 Can Antennas in an Antenna Group on APs That Support MIMO Technology Be Used Independently?.....	16
2.1.19 What Is the AP Bandwidth When an AP Does Not Use the MIMO Antenna?.....	16
2.1.20 What Are the Mappings Between WMM Queues and 802.1p Priorities?.....	16
2.1.21 How Do I Calculate AP Power?.....	16
2.2 Antennas and Accessories.....	16
2.2.1 How Are Antennas Classified? Which Antennas Are Often Used by Huawei?.....	16
2.2.2 Can Antennas Amplify Signals?.....	18
2.2.3 What Is Antenna Coverage?.....	18
2.2.4 Is the Antenna Gain Determined During Production? Can the Antenna Gain Be Adjusted?.....	18
2.2.5 What Are the Antenna Tilt, Field Angle, and Beam Angle?.....	18
2.2.6 In Which Scenario Does the Outdoor AP Apply To?.....	19
3 WLAN Network Planning and Optimization.....	21
3.1 WLAN Network Planning.....	22
3.1.1 How Can I Determine Orientation of Antennas?.....	22
3.1.2 Which Coverage Mode Is Suitable for a Student Dormitory Building?.....	22
3.1.3 If Multiple Users Deploy APs in the Same Area, Can These APs Work Properly?.....	22
3.1.4 How Many Types of Target Coverage Areas Are There on WLAN Networks? What Are Field Strength Requirements in These Areas?.....	22
3.1.5 What Jobs Need to Be Done and What Information Needs to Be Collected During Site Survey?.....	23
3.1.6 How Can I Evaluate Influence of Co-Channel Interference on Bandwidth on an AP's Air Interface? How Can I Avoid Interference Between Devices Using the Same Channel?.....	24
3.1.7 How Can AP's Channels Be Distributed to Avoid or Reduce Internal and External Interference?.....	24
3.1.8 How Can Channels Be Allocated to Obtain a Better Performance?.....	24
3.2 WLAN Network Optimization.....	25
3.2.1 Why Is the Signal Strength That a STA Receives from an AP Weak?.....	25
3.2.2 What Measures Can Be Taken If the Network Access Rate Is Low Due to Weak WLAN Signal Strength?.....	26
3.2.3 How Can a WLAN Network Be Optimized?.....	26
3.2.4 What Are Common Problems on a WLAN Network?.....	26
3.3 Universal.....	27
3.3.1 How to Do Calculate Signal Strength on a WLAN Network?.....	27
3.3.2 What Are Penetration Losses Caused by Various Obstacles?.....	29
3.3.3 Can Circular Polarization and Cross Polarization Be Used on WLAN Networks? What Are Their Usage Scenarios?.....	30

3.3.4 Can APs Automatically Select Channels with Higher Quality? Can They Change Channels When Current Channels Encounter Interference from an Electromagnetic Wave Source such as a Microwave Oven?.....	30
3.3.5 How Do Signal Measurement Tools Calculate the SNR? Does a Higher SNR Value Indicate a Better Signal Quality?.....	30
3.3.6 What Measures Can Be Taken Against Multipath Interference?.....	30
4 Access Authentication.....	31
4.1 Why Cannot Users Associate with APs When WPA-PSK Authentication Is Used?.....	32
4.2 Why Cannot STA Associate with an AP When WEP Authentication Is Used?.....	32
4.3 What Are Advantages and Disadvantages of WAPI Authentication?.....	32
4.4 What Is the Difference Between Portal Authentication and 802.1X Authentication?.....	32
4.5 What Authentication Protocols Are Supported During STA Login? Which One Is Recommended and Why?.....	33
5 STA.....	34
5.1 STA Receives Strong Signals from an AP, But the Network Speed Is Slow. How Can I Locate the Problem?.....	35
5.2 Why Is the Association Rate Displayed on Wireless Terminals Low?.....	35
5.3 Why Does a STA Fail to Associate with an AP When WEP and TKIP Encryption Is Configured in 802.11n Mode?.....	35
5.4 The Laptop Uses the 802.11b/g NIC. How Can I Associate It with a 802.11n AP?.....	36
5.5 I Bought a Wi-Fi NIC. The Vendor States It Is an 802.11a/b/g/n Network Card, But Why Did I Fail to Search 5 GHz AP Signals (AP Works on Channel 149) Using This NIC?.....	36
5.6 Why Did STA Fail to Search 802.11n Signals After the AP Is Enabled with 802.11n?.....	36
5.7 Does BT Download Occupy High Bandwidth and Reduce WLAN Efficiency?.....	36
5.8 Does an Online 802.11b/g Terminal Affect the Rate of an Online 802.11n Terminal?.....	37
5.9 How Can I Separate Two STAs that Connect to the Same SSID?.....	37
6 Others.....	38
6.1 What Is the Function of the WLAN QoS Profile?.....	39
6.2 What Is the Difference Between the WMM Mandatory Switch and WMM Function Switch?.....	39
6.3 Is the Scanned Air Port MAC Address of the SSID Sent by Huawei APs in Multicast Mode the Same as the AP's MAC Address?.....	39

1 Protocols and Basic Concepts

About This Chapter

- 1.1 What Are the Differences Between 802.11a/b/g/n Standards?
- 1.2 Where Are Interference Sources in WLAN and How Is the Interference Strength?
- 1.3 What Are WLAN Reliability Features?
- 1.4 What Are the Relationship and Difference Between WLAN and Wi-Fi?
- 1.5 What Are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing?
- 1.6 What Are the Differences Between HT20 and HT40, How Is the 11n 40 MHz Channel Is Partitioned, and What Are the Meanings of Plus and Minus?
- 1.7 What Is the WLAN Coverage Range?
- 1.8 What Are the BSS and SSID?
- 1.9 What Is the Working Process of 802.11n Short GI?
- 1.10 What Are the Advantages and Disadvantages of FHSS and DSSS?
- 1.11 Is the WLAN Rate the Upstream or Downstream Rate?
- 1.12 What Are the Physical Rate, Theoretical Rate, and Actual Rate in the 802.11 Standard?
- 1.13 What Is the Relationship Between WMM and 802.11e?
- 1.14 What Are the Implementations of 802.11n Frame Aggregation Technologies, MSDU and MPDU?
- 1.15 Does an AP Listen to and Send Frames over One Channel?
- 1.16 How Does a STA Synchronize the Channel When the Associated AP Switches to Another Channel?

1.1 What Are the Differences Between 802.11a/b/g/n Standards?

The following tables lists the differences between 802.11a/b/g/n standards in frequency band, compatibility, theoretical rate, and actual rate.

Protocol	Frequency Band	Compatibility	Theoretical Rate	Actual Rate
802.11a	5 GHz	NA	54 Mbit/s	About 22 Mbit/s
802.11b	2.4 GHz	NA	11 Mbit/s	About 5 Mbit/s
802.11g	2.4 GHz	Compatible with 802.11b	54 Mbit/s	About 22 Mbit/s
802.11n	2.4 GHz, 5 GHz	Compatible with 802.11a/b/g	300 Mbit/s (two spatial flows)	About 80 to 220 Mbit/s

1.2 Where Are Interference Sources in WLAN and How Is the Interference Strength?

Two frequency bands are available on WLANs: 2.4 GHz and 5 GHz.

The 2.4 GHz frequency band is the Industrial, Scientific, and Medical (ISM) open frequency band. Interference sources in the 2.4 GHz frequency band include cordless phones, baby monitors, microwave ovens, wireless cameras, bluetooth devices, infrared sensors, and fluorescent light ballasts.

Compared with 2.4 GHz frequency band, 5 GHz frequency band has fewer interference sources and more devices begin to use the 5 GHz frequency band, such as cordless phones, radars, wireless sensors, and digital satellites.

In most cases, microwave ovens work at the frequency band ranging from 2.4 to 2.5 GHz, which overlaps the 2.4 GHz frequency band used by WLAN devices. In addition, the power of microwave ovens ranges between 800 W and 2000 W, which is much higher than the transmit power of APs and STAs. Even though interference shielding is performed, microwave ovens still have severe interference on WLAN devices. Microwave ovens greatly reduce the throughput of WLAN devices if they are within a distance shorter than 8 meters around WLAN devices.

The power of cordless phones is about 3 W, which is higher than the AP's transmit power. According to the test analysis on the interference caused by cordless phones on WLAN devices, when the distance between cordless phones and APs (or STAs) is within 1 meter, interference increases significantly. When the distance is shorter than 0.5 meter, WLAN devices are even offline and the cordless phone voice is not clear. Therefore, you are advised to deploy cordless phones more than 2 meters away from APs or STAs.

The transmit power of wireless cameras ranges from 500 to 1000 MW. In indoor scenarios, wireless cameras may affect the WLAN network but have lighter interference than microwave ovens and cordless phones. Therefore, you are advised to deploy wireless cameras far away from WLAN devices during WLAN planning.

Bluetooth devices use the frequency hopping spread spectrum (FHSS) technology and 1 MHz channel bandwidth. If a bluetooth device is sending data at the frequency band overlapping with a WLAN channel that is being monitored by a WLAN device, the WLAN device selects a random backoff period. During this period, the bluetooth device changes to work at a non-overlapping channel, allowing the WLAN device to send data. Therefore, bluetooth devices have small interference on WLAN devices. This interference can be ignored during WLAN planning.

1.3 What Are WLAN Reliability Features?

- WLAN service protection mechanisms: IP source guard (IPSG), DHCP snooping, statically configured MAC-IP table, and dynamic ARP inspection (DAI)
 - IPSG: This function defends against IP packet attacks by filtering out packets with forged IP addresses.
 - DHCP snooping: MAC-IP entries are dynamically generated and MAC-IP entries are reported to the AP. DHCP snooping protects WLAN servers and clients against attacks from ARP, IP, or DHCP packets with forged IP and MAC addresses.
 - Statically configured MAC-IP table: Only administrators can configure static IP addresses. Users using static IP addresses can connect to the network only after their MAC addresses are bound to the static IP addresses by administrators. Packets whose MAC addresses and IP addresses do not match are considered as invalid packets and are discarded.
 - DAI: It is an ARP security technology that intercepts ARP packets, discards ARP packets that do not match the DHCP snooping binding table, and records ARP attack logs. DAI can also limit the rate of ARP packets. DAI protects a device from ARP snooping attacks and prevents errors in the ARP cache table.

1.4 What Are the Relationship and Difference Between WLAN and Wi-Fi?

Wi-Fi is a trademark of the Wireless Local Area Networks Alliance (WLANA). It is actually not a standard and only ensures that products using this trademark can interoperate with each other. As most Wi-Fi products use the IEEE 802.11b standard, Wi-Fi usually refers to 802.11b. Wi-Fi is a new technology that uses the WLAN protocol.

Wi-Fi can provide wireless coverage in an area with a radius of up to 90 m (300 inches), while the WLAN can provide wireless coverage in an area with a radius 5 km (with antennas used). The biggest advantage of Wi-Fi is its high transmission speed (up to 11 Mbit/s). Wi-Fi is a short-distance wireless transmission technology applicable to offices and households.

1.5 What Are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing?

- Multiple input multiple output (MIMO) is an antenna system that consists of M transmit antennas and N receive antennas. The MIMO technology allows spaces to become the resources used to improve performance and increases the coverage range of the wireless system.

The MIMO system generates multiple spatial flows with each antenna generating a maximum of one spatial flow. The single input single output (SISO) system sends or receives one spatial flow (one copy of signals) at a time. The MIMO technology allows multiple antennas to send and receive multiple spatial flows (multiple copies of signals) simultaneously and to differentiate the signals sent to or received from different spaces. An 802.11n device supports up to 4x4 MIMO, a maximum of four spatial flows, with a rate of up to 600 Mbit/s.

- The maximal ratio combining (MRC) technology improves the signal quality of the receive end.

In MRC, the same signal from the transmit end is received by the receive end through multiple paths (multiple antennas) because the receive end receives this signal using multiple antennas. Generally, among multiple paths, there is one path providing better signal quality than the other paths. The receive end uses a certain algorithm to allocate different weights to receiving paths. For example, the receive end allocates the highest weight to the receiving path providing the best signal quality, which improves the signal quality of the receive end. When none of multiple receiving paths can provide better signal quality, the MRC technology can ensure better receive signals.

- The beamforming or Transmit Beam Forming (TxBF) technology produces the strong directional radiation pattern based on the strong correlation of the spatial channel and wave interference principle, making the main lobe of the radiation pattern adaptive to point to the wave direction. This technology improves the SNR, system capacity, and coverage range. Beamforming or TxBF is an optional feature in the 802.11n standard.

Beamforming includes explicit beamforming and implicit beamforming. Explicit beamforming requires the receive end to send information about the received signal to an AP. The AP then adjusts the transmit power to the optimal value according to the signal information. This function increases the SNR of the receive end and improves the receiving capability. Implicit beamforming allows an AP to automatically adjust the transmit power to increase the SNR of the receive end based on channel parameters without requiring the receive end to work with the AP. Currently, mainstream terminals do not support beamforming.

- Space time block coding (STBC) transmits multiple copies of one data flow in wireless communication. STBC uses many antennas to produce multiple receive versions of data, improving data transmission reliability. Among these data copies, optimal copies are combined to provide most reliable data. This redundancy increases the chance of using one or more copies of received data to correctly decode the received data. STBC combines all the copies of received signals to produce the useful data.
- The MIMO technology provides the system with the spatial multiplexing gain and spatial diversity gain.

In spatial multiplexing, multiple antennas are used on the receive end and transmit end and multipath components in spatial communication is used, allowing signals to be transmitted over multiple data channels (MIMO sub-channels) in the same frequency band. This technology makes the channel capacity linearly increase with the growing number of antennas. This increase in channel capacity does not require additional bandwidth and does not consume additional transmit power. Therefore, spatial multiplexing is an efficient means to improve channel capacity and system capacity.

In spatial multiplexing, serial-to-parallel conversion is performed on the transmitted signal to produce several parallel signal flows, which are then transmitted using their respective antennas in the same frequency band simultaneously. Due to the use of multipath propagation, each transmit antenna produces a unique spatial signal for the receive end. After the receive end receives the mixed signals of data, it differentiates these parallel data flows based on the fading between different spatial channels. Spatial multiplexing requires the spacing between transmit and receive antennas to be greater than the distance, ensuring that each sub-channel of the receive end is an independently fading channel.

1.6 What Are the Differences Between HT20 and HT40, How Is the 11n 40 MHz Channel Is Partitioned, and What Are the Meanings of Plus and Minus?

The channel bandwidth in HT20 mode is 20 MHz, and the channel bandwidth in HT40 mode is 40 MHz. Two neighboring 20 MHz channels are bundled to form a 40 MHz channel. One channel functions as the main channel, and the other as the auxiliary channel. The main channel sends Beacon packets and data packets, and the auxiliary channel sends other packets. When the HT40 mode is used in the 2.4 GHz frequency band, there is only one non-overlapping channel. Therefore, you are not advised to use the HT40 mode in the 2.4 GHz frequency band.

Two neighboring 20 MHz channels can be bundled into a 40 MHz channel. If the center frequency of the main 20 MHz channel is higher than that of the auxiliary channel, 40MHz-plus is displayed; otherwise, 40MHz-minus is displayed. For example, if the center frequency 149 and the center frequency 153 reside on two 20 MHz channels, 149plus indicates that the two 20 MHz channels are bundled to form a 40 MHz channel.

1.7 What Is the WLAN Coverage Range?

Generally, the WLAN coverage range varies according to the environment. When no external antenna is used, the WLAN coverage range is about 250 meters. In the semi-open space or the space with a compartment, the WLAN coverage range is about 35 to 50 meters. When external antennas are used, the WLAN coverage range increases with the antenna gain and is determined according to customer requirements. If an outdoor antenna and amplifier are used, the WLAN coverage range can reach up to several tens of kilometers.

1.8 What Are the BSS and SSID?

SSID: service set identifier.

BSS: basic service set, an area covered by an AP. Each BSS is identified by a BSSID. The simplest WLAN contains only one BSS, and all STAs are in the BSS. To enable the STAs to communicate, disable STA isolation.

1.9 What Is the Working Process of 802.11n Short GI?

When the radio chip sends data in OFDM modulation mode, it divides a frame into different data blocks to send. To ensure data transmission reliability, the guard interval (GI) is used between the data blocks to ensure that the receive end correctly parses each data block. During spatial propagation, the delay will occur on wireless signals at the receive end because of multipath. If subsequent data blocks are transmitted fast, these data blocks will interfere with the original data block. The GI is used to avoid such interference. The common GI is 800 us, whereas the short GI defined in the 802.11n standard is 400 us, which increases the physical connection rate by 11%.

1.10 What Are the Advantages and Disadvantages of FHSS and DSSS?

The direct sequence spread spectrum (DSSS) technology has advantages in high-reliability applications, whereas the frequency hopping spread spectrum (FHSS) technology has advantages in low-cost applications. Generally, DSSS fast transmits data in full-band mode, and allows for a higher transmission frequency in the future. The DSSS technology applies to a fixed environment or applications requiring high transmission quality. Therefore, DSSS wireless products are usually used in wireless plants, wireless hospitals, network communities, and campus networking. The FHSS technology applies to the endpoints requiring fast mobility. Because the FHSS transmission range is small, more FHSS devices than DSSS devices are required in the same transmission environment, which requires a high cost.

1.11 Is the WLAN Rate the Upstream or Downstream Rate?

WLAN rate refers to the wireless rate of data transmissions between APs and STAs or between bridges and downstream nodes. Devices on both ends work in half-duplex mode, that is, they can only receive or send data at a time. The WLAN rate is the sum of upstream and downstream rates. Common users mainly use Internet access services to browse web pages, most of which is downstream traffic. In this case, the WLAN rate refers to the downstream rate.

1.12 What Are the Physical Rate, Theoretical Rate, and Actual Rate in the 802.11 Standard?

1. The WLAN physical rate is the physical layer rate of a radio interface, that is, the physical layer rate at which a radio interface keeps sending data. For example, the 802.11b physical rate is 11 Mbit/s and the 802.11g physical rate is 54 Mbit/s.
2. What is the relationship between the user theoretical rate and physical rate? The physical rate indicates only the performance of a radio interface, but users only care about how much bandwidth and rate they can use. The following uses the 802.11b standard as an example and assumes that a user packet is 1500 bytes. After a 32-byte header is prepended to the packet, the packet is longer than an Ethernet data frame. The checksum bits in 802.11b and Ethernet are both 4 bytes. The longest data frames (1536 bytes) are transmitted at the rate of 11 Mbit/s. The transmission time is $[1536 \text{ (bytes)} \times 8 \text{ (bit)}] / 11 \text{ Mbit/s} = 1117$ microseconds.

On the WLAN, a link code and PLCP header (exclusively used by WLAN) are prepended to a data frame. The transmission time of the link code and PLCP header is 192

microseconds. In addition to the interframe gap, a random period (delay offset) is required during the transmission of data frames on WLANs. In 802.11b, the average delay offset is 360 microseconds.

On the WLAN, an ACK frame is received from the remote end each time a data frame is sent to confirm successful communication. The next data frame is sent only after the ACK frame is received. The total transmission time is 213 microseconds.

The transmission time of a 1500-byte data frame includes the waiting time and ACK transmission time, equaling 1882 microseconds.

$$1117 + 192 + 360 + 213 = 1882$$

In this case, the theoretical maximum UDP throughput for 1500-byte data frames is 7.1 Mbit/s.

3. The preceding calculation result is based on the UDP model and 1500-byte frames. The actual usage scenarios are much complex than the preceding scenario. Additionally, the number of STAs also greatly affects AP performance. Therefore, the actual user rate is usually tested. In most cases, the actual rate of 802.11b can reach about 4.7 Mbit/s.

1.13 What Is the Relationship Between WMM and 802.11e?

802.11e defines Quality of Service (QoS) for the wireless LAN, which provides the required service quality for voice and multimedia applications and enhances network performance. Wi-Fi Multimedia (WMM) defines four access categories, including voice, video, best effort, and background to optimize network communication quality and ensure stable access of corresponding applications to network resources. The WMM standard is a subset of IEEE 802.11e.

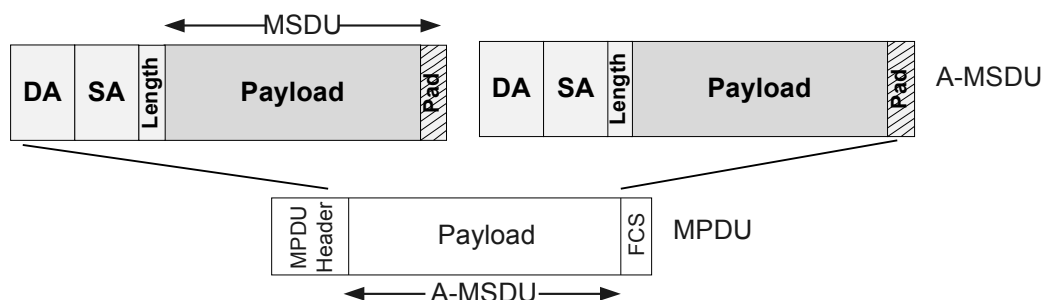
1.14 What Are the Implementations of 802.11n Frame Aggregation Technologies, MSDU and MPDU?

MSDU is short for MAC service data unit.

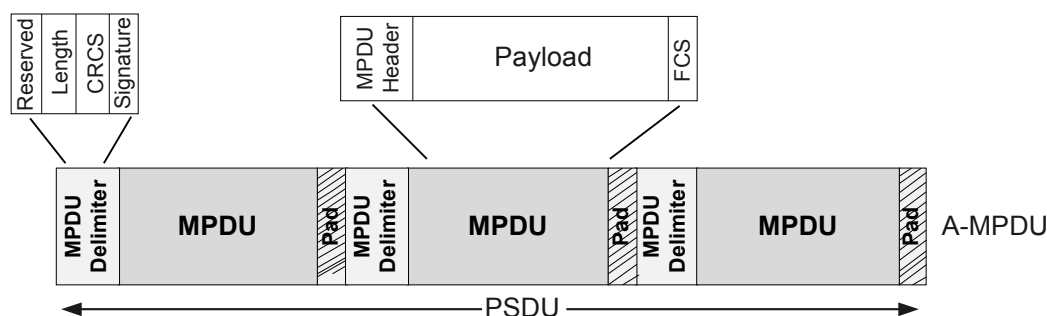
MPDU is short for MAC protocol data unit.

In wireless network security, an MSDU is an Ethernet packet. After integrity check MIC, framing, encryption, serial number assignment, CRC checksum, and MAC header are added to an MSDU, the MSDU becomes an MPDU. An MPDU is a data frame encapsulated using 802.11.

The A-MSDU technology aggregates multiple MSDUs into a large payload. Typically, when an AP or a STA receives an MSDU from the protocol stack, it tags the MSDU with an Ethernet header, called the A-MSDU subframe. The A-MSDU technology encapsulates multiple A-MSDU subframes into an MPDU, which is called an A_MPDU subframe, in accordance with the 802.11 protocol, as shown in the following figure:



The A-MPDU technology aggregates several A_MPDU subframes encapsulated in accordance with the 802.11 protocol. Sending several MPDUs at a time reduces the PLCP preamble and header required to send each 802.11 packet, increasing the system throughput, as shown in the following figure.



1.15 Does an AP Listen to and Send Frames over One Channel?

An AP receives or sends frames over one channel at one time.

- An AP sends and receives frames over the configured channel.
- During neighbor detection, an AP sends probe request frames to all channels and receives probe response frames.
- In station mode, an AP listens to Beacon frames over all channels.

1.16 How Does a STA Synchronize the Channel When the Associated AP Switches to Another Channel?

- If both the STA and AP support channel change notification, the AP sends an action frame (802.11h) to the STA after the AP switches to a channel. The action frame is used to notify the STA of switching the channel immediately or after n Beacon intervals. The STA then switches the channel and retains online.
- If the AP supports channel change notification but the STA does not support channel change notification, the AP sends an action frame to the STA, notifying the STA of switching the channel immediately or after n Beacon intervals. The STA does not process the action frame, and goes offline after the AP switches to the channel.

- If the AP and STA do not support channel change notification, the AP switches to a channel and the STA goes offline.

2 Product FAQs

About This Chapter

[2.1 AP FAQs](#)

[2.2 Antennas and Accessories](#)

2.1 AP FAQs

2.1.1 How Do I View Operations on the Device?

A device records user operations in logs. You can view the log file to check operations.

1. Run the **save logfile** command to save the log information in the log file buffer to the log file.

To reduce the number of times information is written into the storage medium, information generated on the device is saved into the log buffer before being saved into the log file. When the log buffer is full, the system saves the logs in the log buffer to the log file.

You can run the **save logfile** command to save logs that are not automatically saved by system to the log file and clear the log file buffer.

2. Run the **dir logfile/** command to check information about the log files saved on the storage medium.

Too many log files occupy device storage resources. The device stores a maximum of 200 log files by default. If the number of log files exceeds the maximum value, the system deletes the oldest log files.

3. Run the **display logfile file-name** command to check log files on the device.

NOTE

Some old log files cannot be viewed because the device limits the number of log files a user can view. To view all log files, configure the device to save log information to a log host. For details on how to configure the device to send logs to a log host, see **Outputting Log Information to a Log Host** in Information Center Configuration of the Huawei Wireless Access Points Configuration Guide - Device Management.

2.1.2 How Do I Defend Against Bogus DHCP Servers at the User Side?

If a bogus DHCP server is deployed on a customer network, STAs may obtain invalid IP addresses from the bogus DHCP server but not from the AP or authorized DHCP server.

To defend against bogus DHCP servers, disable the DHCP trusted port on an AP in service set view. A DHCP server sends three types of DHCP packets: Offer, ACK, and NACK. When the AP receives any of these DHCP packets from a user-side interface, it considers the packet sender as a bogus DHCP server. The AP then discards the packets.

2.1.3 How Do I Locate VAP Creation Failure?

Operation procedure:

1. Check whether the VAP of the AP is fully configured.
2. Check whether the radio interface is bound to the radio profile.
3. Check whether the service set is configured correctly and bound to the radio interface.

2.1.4 Why Is a VAP Created?

A VAP is created to provide different services, including parameter settings.

2.1.5 What States Does an AP Have?

AP states include:

- normal: The AP is in normal state.
- committing: The WLAN service configuration is being committed.
- commit-failed: The WLAN service configuration fails to be committed.

2.1.6 What Are Characteristics of a Fat AP and a Fit AP? What Are Differences Between Them? What Is the Applicable Scenario?

Item	FAT AP	FIT AP
Function	It integrates the WLAN physical layer functions, user data encryption, user authentication, QoS, network management, roaming technologies, and application layer functions.	A FIT AP has only the encryption and radio functions and cannot work independently of an AC.
Network solution	<p>A FAT AP can provide wireless access independently.</p> <ul style="list-style-type: none"> ● Each AP is an independent node. The channels and power on each AP are configured independently. The AP is easy to install. ● The APs work independently, so the FAT APs do not support large-sized, continual, and cooperative WLANs and do not support advanced applications. ● Each AP requires an independent security policy. If there are a lot of APs on the network, network management, maintenance, and upgrade are difficult. ● Quality on WLANs is difficult to measure. 	<p>FIT APs must be work with an AC to provide wireless access.</p> <ul style="list-style-type: none"> ● An AC allocates channels for AP groups and automatically adjusts transmit power. The AC +FIT AP mode reduces interference between APs and increases network coverage range. ● Both Layer 2 roaming and Layer 3 roaming are supported. ● Unauthorized APs are easily detected and processed. ● Maintenance and operation data is collected by the AC, but not APs. The AC provides powerful AP processing capability and higher performance than AP.

Item	FAT AP	FIT AP
Management and maintenance	FAT APs have complex structure and are difficult to manage in a centralized manner.	The FIT AP configuration is delivered by an AC. This facilitates centralized management of FIT APs.
Application scenario	FAT AP applies to SOHO or small-scale WLANs.	FIT AP applies to large-scale enterprise WLANs, and industry and carrier WLANs.

2.1.7 How Can I Determine Whether an AP Is Qualified?

1. Observe whether the AP indicator works normally. See description of indicators in installation guide of the packaging to determine whether AP indicators are working properly.
2. You can determine whether an AP is qualified by logging in to the AP. Before the login, ensure that the network cable used to connect to the AP is working properly.

NOTE

If the AP needs to connect to an Ethernet switch, ensure that the Ethernet cable is working properly. If the Ethernet cable is not working properly, for example, RJ-45 connectors are short-circuited, the AP may fail to be powered on or fail to work properly. Before connecting an Ethernet cable to the AP, use the cable test tool to check whether the cable is qualified. If the cable is unqualified, replace it.

- a. Check whether you can log in to the AP through the serial interface and enter the CLI.
 - Connect the AP and PC using the serial cable.
 - Log in to the AP through the serial interface. On the AP serial interface, the baud rate is 9600 bit/s, the data bit is 8, the stop bit is 1, and there is no parity bit.

If the login succeeds, the AP is working properly.

- b. Check whether you can use a command to log in to the AP through the serial interface.

NOTE

- The default IP address of the AP is 169.254.1.1.
- Enter the default user name **admin** and initial password **admin@huawei.com**.
- Assign the PC with an IP address on the same network segment as the default IP address of the AP. Connect the network cable to the AP and PC.
- Log in to the AP using Telnet.

If the login succeeds, the AP is working properly. If the login fails, reset the AP to restore the factory settings. Then, log in to the AP again.

3. Enter `http://169.254.1.1` on the web page to log in to a fat AP.

NOTE

- The default IP address of the AP is 169.254.1.1.
- Enter the default user name **admin** and initial password **admin@huawei.com**.

If the login succeeds, the AP is working properly. If the login fails, reset the AP to restore the factory settings.

2.1.8 How Many Access Users Are Recommended for Each AP?

When the upstream rate and downstream rate are 1 Mbit/s and 2 Mbit/s, it is recommended that a single-band AP connects to a maximum of 20 users and a dual-band AP connects to a maximum of 40 users.

When the upstream rate and downstream rate are 512 kbit/s and 2 Mbit/s, it is recommended that a single-band AP connects to a maximum of 20 users and a dual-band AP connects to a maximum of 40 users.

When the upstream rate and downstream rate are 1 Mbit/s and 1 Mbit/s, it is recommended that a single-band AP connects to a maximum of 25 users and a dual-band AP connects to a maximum of 45 users.

When the upstream rate and downstream rate are 512 kbit/s and 1 Mbit/s, it is recommended that a single-band AP connects to a maximum of 25 users and a dual-band AP connects to a maximum of 45 users.

When the upstream rate and downstream rate are 512 kbit/s and 512 kbit/s, it is recommended that a single-band AP connects to a maximum of 30 users and a dual-band AP connects to a maximum of 45 users.

2.1.9 Do APs Support Power Adjustment and What Is the Power Adjustment Mechanism?

Power adjustment is similar to channel adjustment.

2.1.10 How Many Users Does an AP with Different Performance Support in 802.11n Mode?

Performance	Number of Supported Users
11n 1x1 MIMO HT20 with a single spatial stream (65 Mbit/s) and rate limit 512 kbit/s per user	23
11n 2x2 MIMO HT20 with two spatial streams (130 Mbit/s) and rate limit 1 Mbit/s per user	25
11n 1x1 MIMO HT40 with a single spatial stream (150 Mbit/s) and rate limit 1 Mbit/s per user	28
11n 2x2 MIMO HT40 with two spatial streams (300 Mbit/s) and rate limit 1 Mbit/s per user	45

2.1.11 Does an AP Configured with Multiple SSIDs Support the Same Number of Access Users as an AP Configured with One SSID?

Yes, an AP configured with multiple SSIDs support the same number of access users as an AP configured with one SSID.

2.1.12 Can an AP (Single Radio) with Different SSIDs Work at Different Channels?

An AP with different SSIDs cannot work at different channels. A radio has only one channel.

2.1.13 Is the Number of Access Users in Dual-band Mode Twice the Number of Access Users in Single-band Mode?

If there are sufficient system resources, the number of access users in dual-band mode is twice the number of access users in single-band mode. Limited by system resources, the number of access users in dual-band mode may not be twice the number of access users in single-band mode.

2.1.14 Can 802.11n Devices Work Only in 802.11n Mode? Can 802.11n Devices Work in 802.11bg Mode?

802.11n devices can work in multiple modes including 802.11bg mode.

2.1.15 What Methods Does an AP Use to Prevent Interference?

The AP uses the following methods:

1. Adjusts channels.
2. Multiplexes channels.
3. Adjusts the rate at which packets are sent.

2.1.16 How Does an AP Adjust the Rate?

When signal quality becomes bad, an AP changes the modulation mode to reduce the transmission rate. This also reduces the bit error ratio.

2.1.17 Can Huawei 802.11n APs Automatically Switch Between 2.4 GHz and 5 GHz?

Huawei 802.11n APs cannot automatically switch between 2.4 GHz and 5.8 GHz frequency bands. Switching is performed manually.

2.1.18 Can Antennas in an Antenna Group on APs That Support MIMO Technology Be Used Independently?

Yes. When using independently, antennas using the MIMO technology cannot achieve the optimal performance. Multi-antenna MIMO technology can increase AP throughput and provide diversity receiving capability, improving the receive SNR.

2.1.19 What Is the AP Bandwidth When an AP Does Not Use the MIMO Antenna?

When an AP supporting 802.11n does not use the MIMO antenna, 150 Mbit/s bandwidth is supported.

2.1.20 What Are the Mappings Between WMM Queues and 802.1p Priorities?

WMM classifies data packets into four queues. 802.1P provides eight priorities. Users can configure the mappings between WMM queues and 802.1p priorities.

2.1.21 How Do I Calculate AP Power?

Assume the chip of the AP3010DN-AGN provides a transmit power of 50 mW, and the AP3010DN-AGN has two antennas, each of which can increase the transmit power by 2.5 times. The AP transmit power is 250 mW ($50 \times 2.5 \times 2 = 250$ mW), that is 24 dBm, which is calculated based on the formula: $10\log(50 \times 2.5 \times 2) = 17 + 4 + 3 = 24$ dBm.

2.2 Antennas and Accessories

2.2.1 How Are Antennas Classified? Which Antennas Are Often Used by Huawei?

The following antenna types are used:

- Usage: communication antennas, television antenna, radar antenna
- Working frequency band: short wave antenna, ultra-short wave antenna, microwave antenna
- Direction: omnidirectional antenna, directional antenna
- Appearance: wire antenna, mesh antenna

Huawei often uses the following antennas:

- Indoor antenna
 - Indoor directional antenna



- Indoor SMA antenna



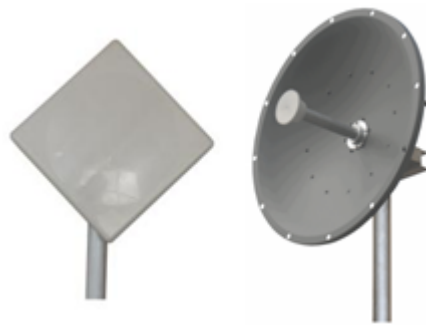
- Outdoor antenna
 - 2.4G&5G omnidirectional antenna



- 2.4G&5G directional antenna



- Backhaul antenna

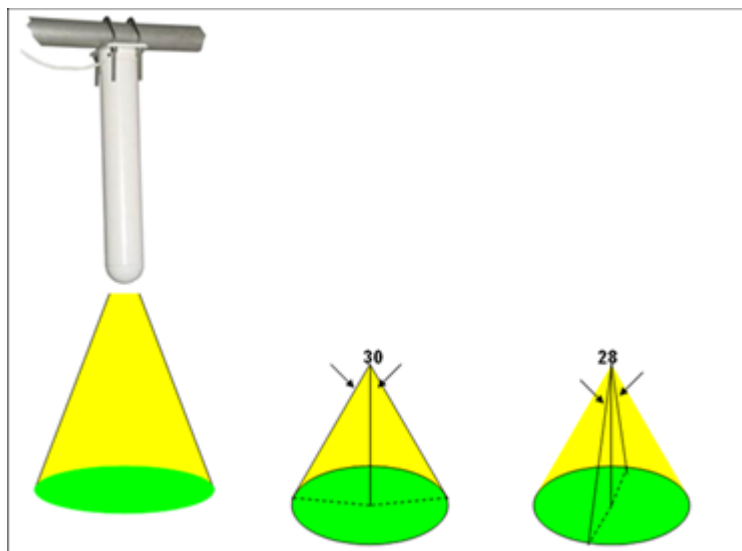


2.2.2 Can Antennas Amplify Signals?

Antennas are passive components. They can only collect wireless signals, but cannot amplify signals. A smaller antenna angle indicates a higher gain.

2.2.3 What Is Antenna Coverage?

The antenna coverage depends on the antenna angle and gain. The antenna coverage area is similar to a taper.

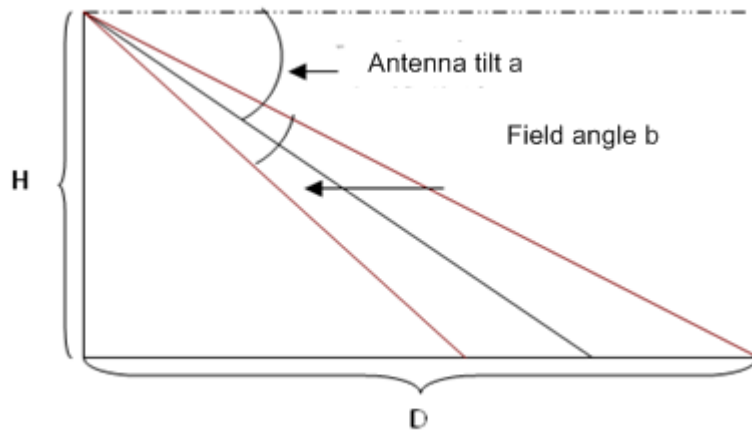


2.2.4 Is the Antenna Gain Determined During Production? Can the Antenna Gain Be Adjusted?

No, the gain is a fixed attribute of an antenna and cannot be adjusted.

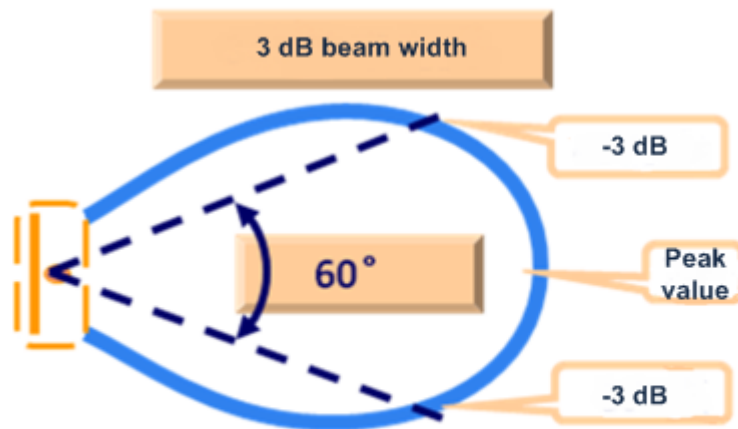
2.2.5 What Are the Antenna Tilt, Field Angle, and Beam Angle?

Antenna tilt: angle between the antenna emission direction and the horizontal direction.



Field angle: angle between the two directions opposed to each other over the beam axis for which the luminous intensity is half that of the maximum luminous intensity.

The field angle often refers to the beam angle.



2.2.6 In Which Scenario Does the Outdoor AP Apply To?

The outdoor AP applies to squares, residential areas, schools, dormitories, campuses, open areas with dense population, commercial streets that have high requirements for wireless data services.

The following figure shows campus WLAN coverage scenario.



3 WLAN Network Planning and Optimization

About This Chapter

[3.1 WLAN Network Planning](#)

[3.2 WLAN Network Optimization](#)

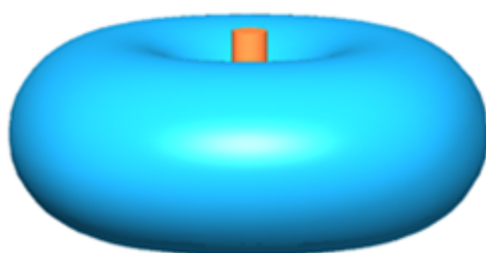
[3.3 Universal](#)

3.1 WLAN Network Planning

3.1.1 How Can I Determine Orientation of Antennas?

A good signal coverage can be obtained if you place antennas with a correct polarization direction. From the following figure, you can see that the gain of an AP's omnidirectional antenna is the highest in the direction vertical to the antenna.

Figure 3-1 Signal radiation of an omnidirectional antenna



When an AP is placed horizontally or wall-mounted, the major lobes of antennas should be placed vertically to receive the optimal signal coverage and then it will have the best connection.

3.1.2 Which Coverage Mode Is Suitable for a Student Dormitory Building?

A student dormitory building has a high density of users who require high bandwidth. Therefore, indoor DAS APs or indoor APs are recommended.

3.1.3 If Multiple Users Deploy APs in the Same Area, Can These APs Work Properly?

WLAN signals are transmitted in the 2.4 GHz frequency band. If APs of multiple users are deployed in the same area, co-channel interference or even signal disorder occurs. As a result, users in this area cannot obtain expected wireless network access.

3.1.4 How Many Types of Target Coverage Areas Are There on WLAN Networks? What Are Field Strength Requirements in These Areas?

WLAN networks involve the following target coverage areas:

- Major coverage areas: places where many users need to connect to the Internet, such as dormitories, libraries, classrooms, hotel lobbies and guest rooms, meeting rooms, offices, and exhibition halls.

- Minor coverage areas: places where few users need to connect to the Internet, such as bathrooms, stairways, lifts, corridors, and kitchens.
- Special coverage areas: special areas where users allow or prohibit WLAN access.

Depending on WLAN access requirements in the preceding areas, various field strengths must meet the following requirements:

- Hotspot field strength: The field strength in major coverage areas ranges from -40 dBm to -65 dBm. A field strength higher than -40 dBm may cause receiver overload, and a field strength lower than -65 dBm may reduce the network connection rate.
- Edge field strength: It is determined based on the receiving sensitivity and edge bandwidth. Generally, the edge field strength should be higher than -75 dBm. The network connection rate in minor areas can be lower than that in major areas.
- Interference field strength: The co-channel interference strength in an area cannot exceed -80 dBm.
- Leakage field strength: The leakage field strength 10 m away from a building cannot exceed -90 dBm.

3.1.5 What Jobs Need to Be Done and What Information Needs to Be Collected During Site Survey?

A site survey involves the following tasks:

- Determine the coverage objects and requirements.
- Obtain the layout of the areas to be covered from the customer.
- Learn about the network topologies in the areas.
- Obtain contact information of customer's onsite technical personnel.
- Identify device installation positions and power supply mode (completed by the asset management personnel of the property management).
- Determine the positions to install APs, power cables, and network cables with the asset management personnel. Check whether Internet access resources are available.
- Determine whether a distributed antenna system (DAS) is required according to the coverage objectives. If a DAS is available, obtain the DAS design drawings from the customer. If not, ask the carrier whether a DAS is required. If a new DAS needs to be established, determine the positions of antennas with the asset owners.
- Check the construction materials and calculate signal loss.
- Check for interference sources.

Collect the following information during a site survey:

- Layout of the coverage areas
Mark the cabling routes and device installation positions on the layout drawings.
- Building arrangement and structure in the coverage areas
Calculate signal coverage distance of APs based on building arrangement and structure.
- Number of users and required bandwidth
Calculate the network capacity based on the number of users and bandwidth required.
- Device installation positions

- Topology and bandwidth resources of the wired network
- Whether there are sufficient optical fibers and wired network resources to transmit WLAN data
- Signal losses caused by walls, doors, windows, and other construction materials
- Locations and signal strengths of interference sources
- Requirements of users

3.1.6 How Can I Evaluate Influence of Co-Channel Interference on Bandwidth on an AP's Air Interface? How Can I Avoid Interference Between Devices Using the Same Channel?

Co-channel interface is a major factor that reduces an AP's maximum throughput. When APs are placed close to each other, their signals have a large overlapping coverage area, resulting in severe co-channel interference. In this case, APs' maximum throughput decreases greatly.

To avoid co-channel interference, adjust APs' transmit power and increase the intervals between APs. You can also use directional antennas and smart antennas to restrict the signal coverage area.

3.1.7 How Can AP's Channels Be Distributed to Avoid or Reduce Internal and External Interference?

Use a cellular channel distribution to avoid channel overlapping. For example, there are only three non-overlapping channels in the 2.4 GHz frequency band: channel 1, channel 6, and channel 11. A proper channel distribution can greatly reduce co-channel interference on a WLAN network. Follow these principles when distributing radio channels:

- Use non-overlapping channels in adjacent areas.
- Adjust APs' transmit power to avoid co-channel interference between areas.
- Use a cellular channel distribution so that channels can be multiplexed without causing overlapping coverage areas.

3.1.8 How Can Channels Be Allocated to Obtain a Better Performance?

There are only three non-overlapping channels in the 2.4 GHz frequency band: channels 1, 6, and 11. If channels of neighboring APs conflict, channel interference occurs, degrading user access experience.

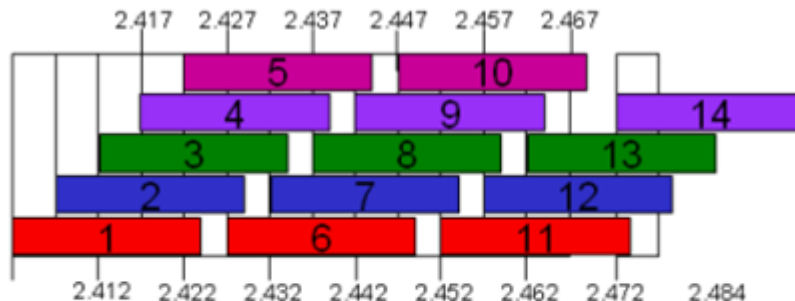
- Make an AP channel plan before you perform data configurations. You are advertised to manually configure AP channels. The automatic channel adjustment is not recommended.
- If channels of non-Huawei neighboring APs conflict with that of Huawei APs, negotiate with the non-Huawei vendors and change conflicting channels.

Use spatial staggered channels to increase network capacity.

- Channels of neighboring APs are staggered. For example, neighboring APs uses channels in the 2.4 GHz frequency band in a fixed sequence of 1, 6, 11, 1, 6, and 11.

- The 5 GHz frequency band is preferred when it is deployed. In the 5 GHz frequency band, non-overlapping channels are channels 149, 153, 157, 164, and 165.

Pan of Frequency Bands in 802.11b/g Mode



Frequency multiplex on a cellular network:

Use non-overlapping channels
Such as channels 1, 6, and 11 in adjacent areas.
Adjust APs' transmit power to avoid co-channel interference between areas.
Use a cellular channel distribution so that channels can be multiplexed without causing overlapping coverage areas.



3.2 WLAN Network Optimization

3.2.1 Why Is the Signal Strength That a STA Receives from an AP Weak?

The possible causes are:

- The transmit power of the AP is low. In this case, increase the transmit power.
- The antenna system of the AP (indoor DAS AP) is not properly deployed.
 1. The output power on antenna interfaces is low because the AP connects to excess antennas. Or the feeder lines are too long.
 2. The passive devices (combiner, splitter, and coupler) do not comply with design principles or specifications or are not properly connected.
 3. The passive devices have unloaded interfaces.
- The STA is far away from the AP's antennas, so the signal loss is large.
- Signals are blocked by a beam, post, concrete wall, metal door, or other obstacles between the STA and antennas. In this case, change the antenna installation positions.

3.2.2 What Measures Can Be Taken If the Network Access Rate Is Low Due to Weak WLAN Signal Strength?

Symptom	Cause	Measure
There are too many users that connect to the Internet in some time.	Many users are surfing on the Internet at the same time at night, and traffic volume has exceeded the APs' capacities. Therefore, the network is congested or the network performance deteriorates.	802.11n APs can be deployed in the dormitory building to provide higher capacities.
The signal strength in some corners is weak.	Users are sitting at upper berths far away from the door.	It is recommended that users sit at desk or other positions close to the door.
Gaming users are disconnected from the Internet.	Gaming is a delay-sensitive service. If many users play online games in peak hours, the network is congested.	Upgrade the APs or play online games in off-peak hours.
The signal strength on STAs is weak (only one or two signal strength bars).	The signal coverage in this room is insufficient.	Check the signal strength of all antennas on the AP covering this room. If all antennas have a weak signal strength, check the AP and combiner. If one antenna has a weak signal strength, check the splitter and this antenna.

3.2.3 How Can a WLAN Network Be Optimized?

A WLAN network can be optimized by:

- Adjusting APs' transmit power
- Adjusting the antenna system
- Adjusting APs' channels
- Reducing interference
- Adjusting network-side topology and bandwidth

3.2.4 What Are Common Problems on a WLAN Network?

Problems on a WLAN network are classified into the following types:

- Problems at the network side
 - Insufficient bandwidth

- Link failures
- Incorrect configuration
- Problems at the AP side
 - Incorrect AP working mode
 - Power supply failures
 - Faults of network cables connected to APs
- Radio coverage problems
 - Co-channel interference
 - Improper channel distribution
 - Insufficient antenna coverage
 - Faults of passive devices in the antenna system

3.3 Universal

3.3.1 How to Do Calculate Signal Strength on a WLAN Network?

Wireless signal strength decreases during transmission because of free-space loss, penetration loss, and device and connection loss. You need to consider these link budgets when calculating the signal strength.

- Free-space loss model

The free-space loss model is used to calculate the link budget of indoor DAS APs and indoor APs. The following formulas are used:

- $20\log f + 20\log d - 28$ (f: MHz; d: m)
- $20\log f + 20\log d + 32.4$ (f: MHz; d: km)
- $20\log f + 20\log d + 92.4$ (f: GHz; d: km)

- COST231-Hata model

The COST231-Hata model is used to calculate the link budget of outdoor APs and applies to 2000 MHz or lower frequency bands. To calculate the link budget on the 2.4 GHz frequency band, a correction parameter C_m is used: $PL = 46.3 + 33.9\lg(f) - 13.82\lg(hb) - a(hm) + (44.9 - 6.55\lg(hb))\lg(d) + C_m$

The C_m value depends on the environment:

- Dense Urban: -3
- Urban: -6
- Suburban: -12
- Rural: -20
- In the formula, hb indicates the height of base station antenna (in meters), and hm indicates the height of mobile station antenna (in meters).
- f indicates the antenna working frequency (in MHz), and d indicates the transmission distance (in km).
- a is a function, which also depends on the environment:

- Dense urban and urban: $a(Hr) = 3.2\log_2(11.75 Hr) - 4.97$
- Suburban and rural: $a(Hr) = (1.1\log f - 0.7) Hr - (1.56\log(f) - 0.8)$

- Penetration loss

APs' coverage area is restricted by the multipath effect. Penetration and diffraction capabilities of wireless signals are weak; therefore, wireless signals attenuate greatly when blocked by obstacles. The following are penetration loss values of 2.4 GHz radios when penetrating various materials:

- 8 mm board: 1-1.8 dB
- 38 mm board: 1.5-3 dB
- 40 mm wooden door: 2-3 dB
- 12 mm glass: 2-3 dB
- 250 mm concrete wall: 20-30 dB
- Brick wall: 15 dB
- Inter-floor penetration: 30 dB
- Elevator: 20-40 dB

- Device and connection losses

Radio frequency (RF) devices, such as cable connectors, splitters, couplers, combiners, and AC filters, have insertion losses.

- The insertion loss of a cable connector ranges from 0.1 dB to 0.2 dB.
- The insertion loss of a combiner is 0.5 dB.
- For the insertion losses of passive devices, see corresponding product manuals. [Table 3-1](#) lists transmission losses of various cables.

Table 3-1 Cable transmission losses

Name	Transmission loss in 900 m dB/100 m	Transmission loss in 2100 m dB/100 m	Transmission loss in 2400 m dB/100 m
1/2-inch feed line	7.04	9.91	12.5
7/8-inch feed line	4.02	5.48	6.8

- Link budget calculation method

- Power budget

Transmit power + Tx gain - path loss + Rx gain = Signal strength

- AP transmit power

An AP's transmit power depends on its specifications.

- AP Tx antenna gain and STA Rx antenna gain

The antenna gain is determined by antenna specifications. Generally, the value is 2 dBi.

- Path loss

Path losses include free-space loss, penetration loss, and loss on cables.

The penetration loss cannot be calculated accurately because it depends on wall materials and signal transmission angle. Generally, the penetration loss count as 25 dB.

3.3.2 What Are Penetration Losses Caused by Various Obstacles?

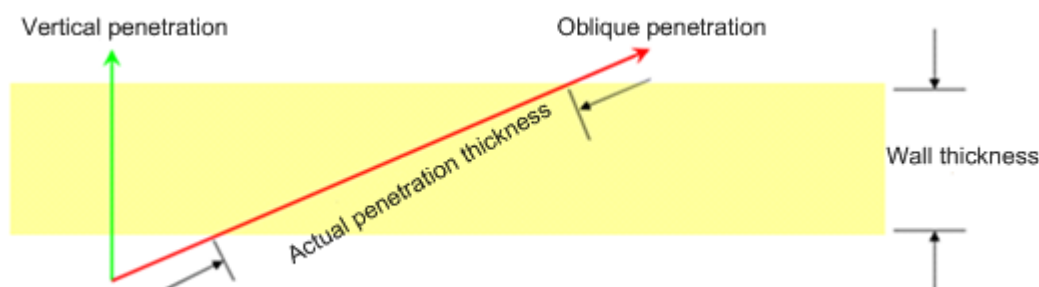
Obstacles in the coverage area of an indoor or outdoor AP can cause an obvious loss of signals. The following table lists the path losses in 2.4 GHz and 5 GHz frequency bands caused by various obstacles.

2.4 GHz Path Loss	
Glass window (non tinted)	2 dB
Wooden door	3 dB
Cubicles	3 to 5 dB
Dry wall	4 dB
Marble	5 dB
Brick wall	8 dB
Concrete wall	10 to 15 dB

5 GHz Path Loss	
Typical interior wall	
PVC plate	0.6 dB
Gypsum plate	0.7 dB
Plywood	0.9 dB
Gypsum wall	3.0 dB
Rough chipboard	2.0 dB
Veneer board	2.0 dB
Glass plate	2.5 dB
6.2 cm Sound proof door	3.6 dB
Typical exterior wall	
Double-glazed window	11.7 dB
Concrete block wall	11.7 dB

If there are metal objects, load-bearing columns, or beams in the target coverage area, ensure that wireless signals are not blocked by them because they cause a large penetration loss.

The penetration loss is minimum when signals penetrate a wall vertically, and the penetration loss is much larger when wireless signals penetrate a wall obliquely. Therefore, when you install APs, try to reduce the incidence angle of signals.



3.3.3 Can Circular Polarization and Cross Polarization Be Used on WLAN Networks? What Are Their Usage Scenarios?

Circular polarization has not been applied to WLAN networks. Cross polarization (+45 and -45 degrees) is used on outdoor post antennas. Cross-polarized antennas provide wireless signals at 2.4 GHz and 5 GHz frequency bands.

3.3.4 Can APs Automatically Select Channels with Higher Quality? Can They Change Channels When Current Channels Encounter Interference from an Electromagnetic Wave Source such as a Microwave Oven?

Huawei APs support automatic channel selection. However, in large-scale AP deployment, channels are selected before deployment. Changing one AP's channel will cause channel switching on other APs, affecting wireless services on the entire network. Therefore, automatic channel selection is not recommended.

3.3.5 How Do Signal Measurement Tools Calculate the SNR? Does a Higher SNR Value Indicate a Better Signal Quality?

The SNR value obtained using a signal measurement tool is not the actual SNR on a network adapter. The tool obtains the SNR value by comparing the detected signal strength with a predefined noise value (-96 dBm for example). A high SNR value does not indicate a good signal quality because the high SNR may be caused by interference signals. The signal quality should be evaluated by the SNR and signal to interference ratio (SIR).

3.3.6 What Measures Can Be Taken Against Multipath Interference?

The following technologies can be used against multipath interference: smart antenna, multiple-input and multiple-output (MIMO) beamforming, MIMO space-time block coding (STBC), and MIMO maximal ratio combining (MRC).

4 Access Authentication

About This Chapter

- 4.1 Why Cannot Users Associate with APs When WPA-PSK Authentication Is Used?
- 4.2 Why Cannot STA Associate with an AP When WEP Authentication Is Used?
- 4.3 What Are Advantages and Disadvantages of WAPI Authentication?
- 4.4 What Is the Difference Between Portal Authentication and 802.1X Authentication?
- 4.5 What Authentication Protocols Are Supported During STA Login? Which One Is Recommended and Why?

4.1 Why Cannot Users Associate with APs When WPA-PSK Authentication Is Used?

The possible causes are as follows:

- The STA does not support WPA2-PSK. For example, the computer runs an early version of Windows XP without patches installed, the computer may not support WPA2-PSK. Patches need to be installed on the computer.

4.2 Why Cannot STA Associate with an AP When WEP Authentication Is Used?

The possible causes are as follows:

- No WEP SSID is added to the STA. Many STAs associate with WEP SSIDs by using encryption without authentication. However, the AP uses both authentication and encryption. Therefore, the STA cannot associate with the SSID. The SSID must be manually configured on the STA. At last, set the encryption type to share mode.
- The key index configured on the AP is different from the key index on the STA. By default, the key index of an AP is 0 (ranging from 0 to 3), and the key index of STA is 1 (ranging from 1 to 4). Key index 0 on the AP matches key index 1 on the STA.

4.3 What Are Advantages and Disadvantages of WAPI Authentication?

WLAN authentication and Privacy Infrastructure (WAPI) has three independent elements: STA, AP, and Authentication Service Unit (ASU), to ensure authentication security. Encryption keys are generated after negotiation. WAPI authentication uses the SMS4 algorithm and supports 802.1X authentication applying to a large-scale network.

WAPI applies to scenarios requiring high security level. In WAPI authentication, the ASU server must check certificates, which requires support from STAs. Currently, a few STAs support WAPI. STA hardware needs to be upgraded to support WAPI. Software application is not widely used because of its low efficiency.

4.4 What Is the Difference Between Portal Authentication and 802.1X Authentication?

Portal authentication and 802.1X authentication are similar at the network side. Portal authentication is simple but has poor information security. 802.1X authentication is complex to install and configure but ensures high information security. The two authentication modes are used based on service types. 802.1X authentication is recommended for scenarios requiring high security. The combination of portal authentication and 802.1X authentication is used to meet

requirements of different service on the existing networks. The following table shows the comparisons between portal authentication and 802.1X authentication.

Item	Portal	802.1X
Client	Only requires a browser and does not require a client.	Requires a dedicated 802.1X client.
Server	Requires a portal server.	Requires a dedicated RADIUS server.
Installation and configuration	Requires no configuration and is easy to use.	Requires multiple configuration steps.
Encryption	Does not encrypt data.	Uses dynamic WEP encryption.
Security	Passwords entered on web pages are encrypted by SSL. Network traffic is not encrypted and can be intercepted by anyone. No other security measures are required.	802.1X authentication provides higher security than portal authentication. 802.1X encapsulates authentication packets in EAP format and supports multiple encryption algorithms. EAP-TLS, EAP-MD5, and EAP-SIM authentication modes are used based on the site requirements. Certificates are obtained to authenticate clients and servers.

4.5 What Authentication Protocols Are Supported During STA Login? Which One Is Recommended and Why?

The following authentication modes are supported: 802.1X, MAC, Portal, MAC+Portal, EAP-TLS, EAP-PEAP, and EAP-PAP. The MAC+Portal mode is recommended. This mode is secure and easy to use. No client is required. Users do not need to enter passwords in a specified period.

5 STA

About This Chapter

- 5.1 STA Receives Strong Signals from an AP, But the Network Speed Is Slow. How Can I Locate the Problem?
- 5.2 Why Is the Association Rate Displayed on Wireless Terminals Low?
- 5.3 Why Does a STA Fail to Associate with an AP When WEP and TKIP Encryption Is Configured in 802.11n Mode?
- 5.4 The Laptop Uses the 802.11b/g NIC. How Can I Associate It with a 802.11n AP?
- 5.5 I Bought a Wi-Fi NIC. The Vendor States It Is an 802.11a/b/g/n Network Card, But Why Did I Fail to Search 5 GHz AP Signals (AP Works on Channel 149) Using This NIC?
- 5.6 Why Did STA Fail to Search 802.11n Signals After the AP Is Enabled with 802.11n?
- 5.7 Does BT Download Occupy High Bandwidth and Reduce WLAN Efficiency?
- 5.8 Does an Online 802.11b/g Terminal Affect the Rate of an Online 802.11n Terminal?
- 5.9 How Can I Separate Two STAs that Connect to the Same SSID?

5.1 STA Receives Strong Signals from an AP, But the Network Speed Is Slow. How Can I Locate the Problem?

Locate the problem as follows:

1. Check the number of users associated with the AP. The number of associated users cannot exceed the upper limit allowed by the AP.
2. Check the channel and power of the AP. The channel and power must be set to fixed values, but cannot use default settings.
3. Change the connection mode on the AP to high-speed access.
4. Check whether upstream bandwidth limit is set on the AP.
5. Check antennas on APs:
 - The interval between the antennas on different APs cannot be smaller than 10 m.
 - The interval between the antennas on the same AP cannot be smaller than 7 m.
6. Use the dedicated tools to scan adjacent-channel interference. Check whether there is strong interference near the STA.

5.2 Why Is the Association Rate Displayed on Wireless Terminals Low?

- This is because wireless terminals are far away from APs. As a result, radio signals are weak. In this case, the association rate that is negotiated by the wireless terminals is low. Specifically, the signal transmission rate of 802.11g APs includes 54 Mbit/s, 48 Mbit/s, 24 Mbit/s, 18 Mbit/s, and 12 Mbit/s. Some wireless terminals display strong signal strength, but their actual signal strength is poor. The signal strength can be measured by using dedicated testers or test software such as *wirelessmon*.
- The 802.11n is backward compatible with the 802.11b/g, so the 802.11n APs can be encrypted in the mode of WEP or TKIP. The association rate displayed on the STAs may be only 54 Mbit/s because the 802.11n standard does not define the WEP or TKIP encryption mode. If the 802.11n APs use the WEP or TKIP encryption mode, the STAs are associated only at 802.11g rates. Some NICs of the STAs support only the 802.11b/g APs. When the STAs are associated with the 802.11n APs, the maximum association rate is only 54 Mbit/s. The 802.11n APs can also be configured with the 802.11b/g radio frequency type, because the 802.11n is backward compatible with the 802.11b/g.

5.3 Why Does a STA Fail to Associate with an AP When WEP and TKIP Encryption Is Configured in 802.11n Mode?

The 802.11n mode defines the WEP or TKIP encryption mode. When the two encryption modes are used, STAs may fail to associate with the AP.

5.4 The Laptop Uses the 802.11b/g NIC. How Can I Associate It with a 802.11n AP?

You can associate it with 802.11n AP if the AP does not set the 802.11n-only mode. However, the signal transmission rate of the APs in 802.11b mode is low. In contrast, the time that the 802.11n APs take to transmit radio signals at 300 Mbit/s accounts for only 1/27 of the time that the 802.11b APs take to transmit radio signals. Therefore, when a comparatively large number of old wireless terminals are connected to the 802.11n APs, the AP performance decreases considerably. To ensure high performance of the entire WLAN, the 802.11b STAs will be disabled to access the network.

5.5 I Bought a Wi-Fi NIC. The Vendor States It Is an 802.11a/b/g/n Network Card, But Why Did I Fail to Search 5 GHz AP Signals (AP Works on Channel 149) Using This NIC?

5 GHz AP signals are divided into three frequency bands: low frequency (5150 MHz to 5250 MHz), intermediate frequency (5250 MHz to 5350 MHz), and high frequency (5725 MHz to 5825 MHz). China supports low and intermediate frequency bands, but the Radio Association of China authorizes the 5.8 GHz frequency. Therefore, in China, the 5 GHz AP works on radio channels that use the 5.8 GHz frequency. These optional channels include channels 149, 153, 157, 161, and 165. Many types of NICs in the market support the 5.2 GHz frequency but not the 5.8 GHz frequency. To connect your NIC to 5 GHz AP signals, you can change the AP's working channels to the channels in low and intermediate frequency bands.

5.6 Why Did STA Fail to Search 802.11n Signals After the AP Is Enabled with 802.11n?

This is because the IEEE 802.11n draft protocol does not support a high throughput rate of the WEP or TKIP unicast ciphers. If the STA uses the WEP or WPA-TKIP encryption mode, the data transmission rate will decrease to 54 Mbit/s. In WEP or TKIP mode, if the STA uses the 802.11b/g/n NIC to associate with APs, it can only be associated with 802.11g APs. As a result, the displayed signal transmission rate is 54 Mbit/s but not the 802.11n rate. This is restricted by the IEEE 802.11 standard.

5.7 Does BT Download Occupy High Bandwidth and Reduce WLAN Efficiency?

Currently, no evidence shows that the BT service reduces WLAN air interface efficiency. However, if BT users exist on the WLAN, other users feel that the network quality decreases. This is because air interface bandwidth is occupied by BT users. Therefore, user experience is poor on the WLAN with BT users.

5.8 Does an Online 802.11b/g Terminal Affect the Rate of an Online 802.11n Terminal?

Yes. 802.11b/g terminals have a low rate and occupy the air port for a longer time when forwarding the same traffic as 802.11n terminals. This lowers the rate of an online 802.11n Terminal.

5.9 How Can I Separate Two STAs that Connect to the Same SSID?

Huawei APs support Layer 2 isolation. When Layer 2 isolation is enabled, STAs cannot communicate at Layer 2. Only the upstream interface and virtual access point (VAP) interface can exchange data.

6 Others

About This Chapter

[6.1 What Is the Function of the WLAN QoS Profile?](#)

[6.2 What Is the Difference Between the WMM Mandatory Switch and WMM Function Switch?](#)

[6.3 Is the Scanned Air Port MAC Address of the SSID Sent by Huawei APs in Multicast Mode the Same as the AP's MAC Address?](#)

6.1 What Is the Function of the WLAN QoS Profile?

The QoS profile defines the local priority and CAR. The WLAN QoS profile is bound to a user group. After WLAN users are authenticated successfully, the RADIUS server delivers authentication information containing the user group name to the AC. The AC delivers QoS CAR to the AP to limit STA data packets.

6.2 What Is the Difference Between the WMM Mandatory Switch and WMM Function Switch?

The WMM function switch controls the entire WMM function of an AP. The entire WMM function includes the WMM mandatory switch and EDCA parameter.

The WMM mandatory switch controls whether the terminals that do not support WMM can connect to a WMM-support AP.

6.3 Is the Scanned Air Port MAC Address of the SSID Sent by Huawei APs in Multicast Mode the Same as the AP's MAC Address?

No, the scanned air port MAC address of the SSID sent by Huawei APs in multicast mode is self-originated according to certain parameters including the carrier ID and device ID, and may differs from the AP's MAC address, which ensures global uniqueness of the SSID.