Huawei iGuard AirEngine 6776-X7TH Access Point Datasheet

Next-Gen Wi-Fi 7 AP with Hidden Imaging Device Detection

Product Overview

Huawei iGuard AirEngine 6776-X7TH is a next-generation indoor Wi-Fi 7 (802.11be) access point (AP) that not only delivers advanced connectivity but also detects hidden imaging devices, such as pinhole cameras, in the surrounding space, safeguarding trade secrets and personal privacy. It supports three bands—2.4 GHz (2x2 MIMO), 5 GHz (2x2 MIMO), and 6 GHz (4x4 MIMO)—offering up to 8 spatial streams and delivering data rates of up to 13.66 Gbps. Powered by Wi-Fi 7 innovations, the AP significantly enhances the wireless experience for users. Its advanced features make AirEngine 6776-X7TH ideal for indoor coverage in offices, hotels, education, and healthcare, environments.



AirEngine 6776-X7TH

- Provides services simultaneously on the 2.4GHz, 5GHz, and 6GHz frequency bands, with flexible radio switching. It supports a maximum of 3 radios and 8 spatial streams, delivering an overall device rate of up to 13.66 Gbit/s.

Work Mode	MIMO	Peak Data Rate
Mode1	2.4GHz (2x2) +5GHz (2x2) +6GHz (4x4)	13.66 Gbit/s
Mode2	2.4GHz (2x2) +5GHz-H (2x2) +5GHz-L (4x4)	7.89 Gbit/s
Mode3	2.4GHz (2x2) +5GHz (4x4)	6.45 Gbit/s

- Built-in dynamic-zoom smart antennas that can flexibly work in omnidirectional coverage mode (for wider coverage) or high-density coverage mode (for better network performance and user experience).
- USB port can be used for external IoT expansion (supporting protocols such as ZigBee, and RFID).
- Supports Bluetooth serial interface-based O&M through built-in Bluetooth and CloudCampus APP.
- Supports Fit, Fat and cloud management working modes, and enables Huawei cloud management platform to manage and operate APs and services on the APs, reducing network O&M costs.

Feature Descriptions

Wi-Fi 7 (802.11be) standard

Wi-Fi 7 (802.11be) is the Wi-Fi standard, also known as IEEE 802.11be or extremely high throughput (EHT). Based on Wi-Fi 6, Wi-Fi 7 introduces technologies such as 4096-quadrature amplitude modulation (QAM), multi-resource unit (MRU), multi-link operation (MLO), enhanced multi-user multiple-input multiple-output (MU-MIMO). Drawing on these cutting-edge technologies, Wi-Fi 7 delivers a higher data transmission rate and lower latency than Wi-Fi 6.

New Features in Wi-Fi 7

Multi-RU

In Wi-Fi 6, each user can send or receive frames only on the RUs allocated to them, which greatly limits the flexibility of spectrum resource scheduling. To resolve this problem and further improve spectrum efficiency, Wi-Fi 7 defines a mechanism for allocating multiple RUs to a single user. To balance the implementation complexity and spectrum utilization, the standard specifications impose certain restrictions on RU combination. That is, small RUs (containing fewer than 242 tones) can be

combined only with small RUs, and large RUs (containing greater than or equal to 242 tones) can be combined only with large RUs. Small RUs and large RUs can be combined together.

Higher-Order 4096-QAM

The highest order modulation supported by Wi-Fi 6 is 1024-QAM, which allows each modulation symbol to carry up to 10 bits. To further improve the rate, Wi-Fi 7 introduces 4096-QAM so that each modulation symbol can carry 12 bits. With the same coding, 4096-QAM in Wi-Fi 7 can achieve a 20% rate increase compared with 1024-QAM in Wi-Fi 6.

Multi-Link Mechanism

To efficiently utilize all available spectrum resources, the industry is in urgent need to introduce new spectrum management, coordination, and transmission mechanisms on the 2.4 GHz, 5 GHz, and 5 GHz frequency bands. The TGbe defines multi-link aggregation technologies, including the MAC architecture of enhanced multi-link aggregation, multi-link channel access, and multi-link transmission.

There are two modes as for MLO:

- High-concurrency mode, multiple links send different data to improve bandwidth.
- High-reliability mode, multiple links send the same data, improving reliability.

Wi-Fi Shield

Wi-Fi Shield is an innovative wireless security technology developed by Huawei. It transmits extra interference signals to ensure that only the target terminal can accurately receive data packets and signals, preventing malicious users from listening. The Wi-Fi shield function is supported. Eavesdropping terminals cannot capture packets over the air interface.

Wi-Fi CSI Sensing

Wi-Fi CSI sensing is a cutting-edge technology for implementing sensing by using channel state information (Channel State Information, CSI) generated during radio signal propagation. Based on the Wi-Fi 7 standard, Huawei innovatively introduces Wi-Fi CSI to sense the presence of personnel, so that Wi-Fi signals can be sensed wherever they are. Compared with cameras, it protects user privacy and applies to scenarios such as energy saving, health care, and smart security.

iCSSR

Intelligent coordinated scheduling and spatial reuse (iCSSR) enables multiple APs to collaboratively schedule transmission timeslots and parameters, allowing them to operate on the same channel. This significantly improves spectrum efficiency and boosts overall network performance.

Imaging Device Detection

The iGuard AP senses electronic device signals and applies AI algorithms for multi-dimensional modeling with individual calibration. It detects mainstream pinhole cameras using Wi-Fi, cellular networks, or local storage.

NOTE

- The iGuard APs are designed to detect hidden cameras using Wi-Fi, cellular networks, local storage, and others. Some security monitoring devices (such as box cameras, PTZ dome cameras, PTZ devices, and target recognition access control devices) and camera-equipped smart terminals (such as mobile phones, tablets, laptops, phone watches, smart glasses, and action cameras) share similar features to hidden cameras and may be detected. If such devices are detected, you can manually confirm and filter them.
- Electromagnetic interference from electrical appliances in the environment may affect detection accuracy. Huawei's iGuard AP supports the self-learning optimization function and can improve the detection accuracy through continuous deep learning for different environments. Before deploying the camera detection function for APs for the first time, eliminate risks by using a handheld detection device for assistance. Then, enable the self-learning optimization function for APs to adapt to the environment for 36 hours. During this period, you are advised to turn on electrical appliances in the room so interference sources are fully identified, achieving optimal detection performance.
- Enabling the camera detection function on APs must strictly follow network planning (see network planning guidelines). When the camera detection function is enabled on an AP, Wi-Fi services on the 2.4 GHz radio of the AP will be unavailable. If 2.4 GHz Wi-Fi services are required, 2.4 GHz radios of new or existing neighboring APs are recommended to cover the hidden camera detection areas. Other usage constraints and limitations are detailed in the product manual.

Leader AP

The leader AP integrates some WLAN AC functions and can be used to manage Fit APs in small- and medium-sized enterprises and stores, implementing WLAN AC-free access not requiring licenses and saving customer investment.

Basic Specifications

Fit AP mode

Item	Description
WLAN features	Compliance with IEEE 802.11be and compatibility with IEEE 802.11a/b/g/n/ac/ax Maximum ratio combining (MRC) Space time block code (STBC) Cyclic Delay Diversity (CDD)/Cyclic Shift Diversity (CSD) Beamforming Multi-user multiple-input multiple-output (MU-MIMO) Orthogonal frequency division multiple access (OFDMA) Preamble puncturing BSS Color TxBF TWT DPD Compliance with 4096-quadrature amplitude modulation (QAM) and compatibility with 1024-QAM, 256-QAM, 64-QAM, 16-QAM, 8-QAM, quadrature phase shift keying (QPSK), and binary phase shift keying (BPSK) Low-density parity-check (LDPC) Frame aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx) 802.11 dynamic frequency selection (DFS) Short guard interval (GI) in 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz modes Wi-Fi multimedia (WMM) for priority-based data processing and forwarding WLAN channel management and channel rate adjustment **NOTE** For detailed management channels, see the Country Codes & Channels Compliance. Automatic channel scanning and interference avoidance Service set identifier (SSID) hiding configuration for each AP, supporting Chinese SSIDs Signal sustain technology (SST) Unscheduled automatic power save delivery (U-APSD) Multi-user call admission control (CAC) Advanced cellular coexistence (ACC), minimizing the impact of interference from cellular networks 802.11k and 802.11v smart roaming 802.11r fast roaming (≤ 50 ms) Spectrum analysis Terminal location FTM (Fine Timing Measurement) location ASFN (Advanced Same Frequency Network)
Network features	Compliance with IEEE 802.3ab Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent

Item	Description
	Interface (MDI) and Media Dependent Interface Crossover (MDI-X) Compatibility with IEEE 802.1Q SSID-based VLAN assignment Eth-Trunk function Management channel of the AP's uplink port in tagged and untagged modes DHCP client, obtaining IP addresses through DHCP Tunnel data forwarding and direct data forwarding STA isolation in the same VLAN IPv4/IPv6 access control list (ACL) Link Layer Discovery Protocol (LLDP) Service holding when CAPWAP link disconnection in direct data forwarding mode Unified authentication on the AC AC dual-link backup Telemetry, quickly collecting AP status and application experience parameters MESH HotSpot2.0 IPv6 SAVI Downlink port-based LLDP Voice VLAN
QoS features	WMM power save Priority mapping for upstream packets and flow-based mapping for downstream packets Queue mapping and scheduling User-based bandwidth limiting Adaptive bandwidth management (automatic bandwidth adjustment based on the user quantity and radio environment) to improve user experience Application identification and QoS classification to improve voice quality for popular applications, such as Zoom, QQ, and WeChat Airtime scheduling Air interface HQoS scheduling Intelligent multimedia scheduling VIP bandwidth reservation VIP FastPass, per-packet power control Native-IP IFIT iFlow User-defined application
Security features	Open system authentication WPA2-PSK authentication and encryption (WPA2-Personal) WPA2-802.1X authentication and encryption (WPA2-Enterprise) WPA3-SAE authentication and encryption (WPA3-Personal) WPA3-802.1X authentication and encryption (WPA3-Enterprise) WPA-WPA2 hybrid authentication WPA2-WPA3 hybrid authentication WPA/WPA2/WPA2-PPSK authentication and encryption WPA/WPA2/WPA2-DPSK authentication and encryption Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and containment, attack detection and dynamic blacklist, and

Item	Description
	STA/AP blacklist and whitelist 802.1X authentication, MAC address authentication, and Portal authentication DHCP snooping 802.11w Protected Management Frames (PMF) CAPWAP DTLS data encryption and decryption URL filtering MACsec@ Uplink Ethernet port Wi-Fi Shield Secure boot Dot1x client
EAP types	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-CHAP, EAP-SIM, EAP-AKA, EAP-GTC, EAP-FAST, EAP-PEAP, EAP-MD5, EAP-MSCHAPv2, PEAPv0, PEAPv1
Maintenance features	Unified AP management and maintenance on the AC Automatic AP onboarding, automatic configuration loading, and plug-and-play (PnP) Automatic batch upgrade STelnet using SSHv2 SFTP using SSHv2 Remote wireless O&M through the Bluetooth serial port System status alarm Unified AP management on WebMaster
Sensing	Wi-Fi CSI Sensing

Fat AP mode

Item	Description
WLAN features	Compliance with IEEE 802.11be and compatibility with IEEE 802.11a/b/g/n/ac/ax Maximum ratio combining (MRC) Space time block code (STBC) Cyclic Delay Diversity (CDD)/Cyclic Shift Diversity (CSD) Beamforming Multi-user multiple-input multiple-output (MU-MIMO) Orthogonal frequency division multiple access (OFDMA) Preamble puncturing BSS Color TxBF Compliance with 4096-quadrature amplitude modulation (QAM) and compatibility with 1024-QAM, 256-QAM, 64-QAM, 16-QAM, 8-QAM, quadrature phase shift keying (QPSK), and binary phase shift keying (BPSK) Low-density parity-check (LDPC) Frame aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx) 802.11 dynamic frequency selection (DFS) Short guard interval (GI) in 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz modes Wi-Fi multimedia (WMM) for priority-based data processing and forwarding WLAN channel management and channel rate adjustment **NOTE**

Item	Description
	For detailed management channels, see the Country Codes & Channels Compliance. Automatic channel scanning and interference avoidance Service set identifier (SSID) hiding configuration for each AP, supporting Chinese SSIDs Signal sustain technology (SST) Unscheduled automatic power save delivery (U-APSD) Advanced cellular coexistence (ACC), minimizing the impact of interference from cellular networks 802.11k and 802.11v smart roaming 802.11r fast roaming (≤ 50 ms)
Network features	Compliance with IEEE 802.3ab Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X) Compatibility with IEEE 802.1Q SSID-based VLAN assignment DHCP client, obtaining IP addresses through DHCP Tunnel data forwarding and direct data forwarding STA isolation in the same VLAN IPv4 access control list (ACL) Link Layer Discovery Protocol (LLDP) Leader AP NAT
QoS features	WMM power save Priority mapping for upstream packets and flow-based mapping for downstream packets Queue mapping and scheduling User-based bandwidth limiting Airtime scheduling Intelligent multimedia scheduling VIP FastPass
Security features	Open system authentication WPA2-PSK authentication and encryption (WPA2-Personal) WPA3-SAE authentication and encryption (WPA3-Personal) WPA-WPA2 hybrid authentication WPA2-WPA3 hybrid authentication MAC address authentication, and Portal authentication DHCP snooping 802.11w Protected Management Frames (PMF) Secure boot
EAP types	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-CHAP, EAP-SIM, EAP-AKA, EAP-GTC, EAP-FAST, EAP-PEAP, EAP-MD5, EAP-MSCHAPv2, PEAPv0, PEAPv1
Maintenance features	STelnet using SSHv2 SFTP using SSHv2 Remote wireless O&M through the Bluetooth serial port System status alarm

Cloud-Managed AP mode

Item	Description
WLAN features	Compliance with IEEE 802.11be and compatibility with IEEE 802.11a/b/g/n/ac/ax Maximum ratio combining (MRC) Space time block code (STBC) Cyclic Delay Diversity (CDD)/Cyclic Shift Diversity (CSD) Beamforming Multi-user multiple-input multiple-output (MU-MIMO) Orthogonal frequency division multiple access (OFDMA) Preamble puncturing BSS Color TxBF TWT Compliance with 4096-quadrature amplitude modulation (QAM) and compatibility with 1024-QAM, 256-QAM, 64-QAM, 16-QAM, 8-QAM, quadrature phase shift keying (QPSK), and binary phase shift keying (BPSK) Low-density parity-check (LDPC) Frame aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx) 802.11 dynamic frequency selection (DFS) Short guard interval (GI) in 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz modes Wi-Fi multimedia (WMM) for priority-based data processing and forwarding WLAN channel management and channel rate adjustment **NOTE** For detailed management channels, see the Country Codes & Channels Compliance. Automatic channel scanning and interference avoidance Service set identifier (SSID) hiding configuration for each AP, supporting Chinese SSIDs Signal sustain technology (SST) Unscheduled automatic power save delivery (U-APSD) Automatic AP Online by NCE-Campus Multi-user call admission control (CAC) Advanced cellular coexistence (ACC), minimizing the impact of interference from cellular networks 802.11k and 802.11v smart roaming 802.11r fast roaming (≤ 50 ms) Spectrum analysis Terminal location FTM (Fine Timing Measurement) location
Network features	Compliance with IEEE 802.3ab Auto-negotiation of the rate and duplex mode, and automatic switchover between Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X) Compatibility with IEEE 802.1Q SSID-based VLAN assignment DHCP client, obtaining IP addresses through DHCP STA isolation in the same VLAN IPv4/IPv6 access control list (ACL) Link Layer Discovery Protocol (LLDP) Service holdover when the link to NCE-Campus is disconnected

Item	Description
	Unified authentication on the cloud management platform Network address translation (NAT) Telemetry, quickly collecting AP status and application experience parameters MESH Tunnel-AC IPv6 SAVI HotSpot2.0
QoS features	WMM power save Priority mapping for upstream packets and flow-based mapping for downstream packets Queue mapping and scheduling User-based bandwidth limiting Adaptive bandwidth management (automatic bandwidth adjustment based on the user quantity and radio environment) to improve user experience Application identification and QoS classification to improve voice quality for popular applications, such as Zoom, QQ, and WeChat Airtime scheduling Air interface HQoS scheduling Intelligent multimedia scheduling VIP bandwidth reservation VIP FastPass, per-packet power control Native-IP IFIT iFlow User-defined application
Security features	Open system authentication WPA2-PSK authentication and encryption (WPA2-Personal) WPA2-802.1X authentication and encryption (WPA2-Enterprise) WPA3-SAE authentication and encryption (WPA3-Personal) WPA3-802.1X authentication and encryption (WPA3-Enterprise) WPA-WPA2 hybrid authentication WPA2-WPA3 hybrid authentication WPA/WPA2/WPA2-PPSK authentication and encryption WPA/WPA2/WPA2-DPSK authentication and encryption 802.1X authentication, MAC address authentication, and Portal authentication Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS), including rogue device detection and containment, attack detection and dynamic blacklist, and STA/AP blacklist and whitelist DHCP snooping 802.11w Protected Management Frames (PMF) CAPWAP DTLS data encryption and decryption URL filtering MACsec@ Uplink Ethernet port Wi-Fi Shield Secure boot Build-in TPM module Dot1x client

Item	Description
EAP types	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-CHAP, EAP-SIM, EAP-AKA, EAP-GTC, EAP-FAST, EAP-PEAP, EAP-MD5, EAP-MSCHAPv2, PEAPv0, PEAPv1
Maintenance features	Unified AP management and maintenance on the cloud management platform Automatic AP onboarding, automatic configuration loading, and PnP Batch upgrade STelnet using SSHv2 SFTP using SSHv2 Remote wireless O&M through the Bluetooth serial port Real-time user configuration monitoring and fast fault locating using the NMS System status alarm Network Time Protocol (NTP)
Sensing	Wi-Fi CSI Sensing

Technical Specifications

Item		Description
Technical specifications	Dimensions (H x W x D)	60 mm x 220 mm x 220 mm
	Weight	1.54 kg
	Interface type	1 x 1G/10G SFP+ 1 x 100M/1GE/2.5GE/5GE/10GE(RJ-45) 1 x 10M/100M/1GE(RJ-45) 1 x USB **NOTE** • The 10GE (RJ-45) supports PoE input. • The 10G SFP+ supports the 10GE optical module, 2.5G optical module,1G optical module.
	Bluetooth	Bluetooth 6.0
	IoT	• Built-in multi-protocol IoT interfaces, flexibly supporting BLE, ZigBee, HomeKit, and Thread* • USB port extension external IoT (Supports protocols such as ZigBee, RFID) **NOTE** Features marked with asterisks (*) can be implemented through software upgrade.
	LED indicator	Indicates the power-on, startup, running, alarm, and fault states of the system.
Power specifications	Power input	• DC: 43.2 V~57.6 V • PoE power supply: In compliance with 802.3bt/at **NOTE** When 802.3at power is supplied, the AP will operate with restrictions, and the details refer to the Info-Finder.
	Maximum power consumption	24.8 W (excluding USB) **NOTE**

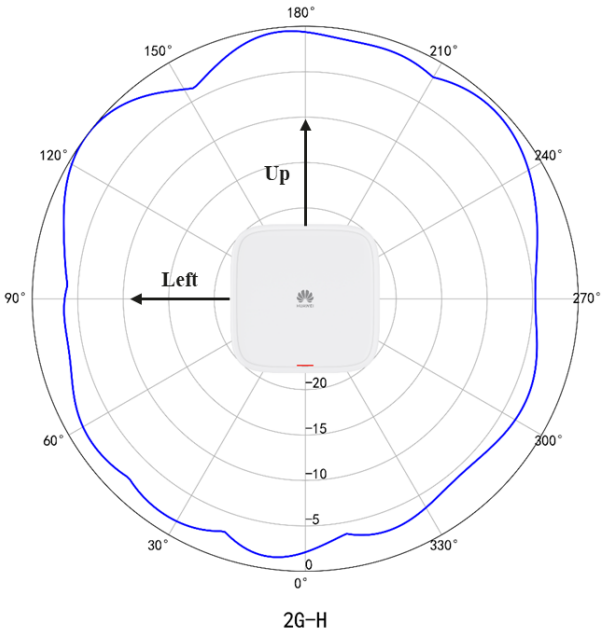
Item		Description		
		The actual maximum power consumption depends on local laws and regulations.		
Environmental specifications	Operating temperature	-10°C to +50°C **NOTE** The value may vary depending on the installation environment.		
	Storage temperature	-40°C to +70°C		
	Operating humidity	5% to 95%		
	Altitude	-60 m to +5000 m		
	Atmospheric pressure	53 kPa to 106 kPa		
Imaging device detection specifications	Detected types	Mainstream pinhole cameras using Wi-Fi, cellular networks, or local storage		
	Detection radius	3 to 5 meters		
Radio specifications	Antenna type	Built-in dynamic-zoom smart antennas		
	Antenna gain	2.4 GHz: 4 dBi 5 GHz: 5 dBi 6 GHz: 5 dBi	2.4 GHz: 4 dBi 5 GHz: 5 dBi 6 GHz: 5 dBi	2.4 GHz: 4 dBi 5 GHz: 5 dBi 6 GHz: 5 dBi
		NOTE • The gains above are the single-antenna peak gains. • The actual transmit power depends on local laws and regulations.		
	Maximum number of SSIDs per device	48 (16 per radio)		
	Maximum number of users per device	1800 (600 per radio) **NOTE** The actual number of users varies according to the application environment.		
	Maximum transmit power	2.4 GHz: 20 dBm/chain 5 GHz: 20 dBm/chain 6 GHz: 19 dBm/chain **NOTE** Above are the combined power powers. The actual transmit power depends on local laws and regulations.		
	Frequency bands	2.400 to 2.4835 GHz ISM 5.150 to 5.250 GHz U-NII-1 5.250 to 5.350 GHz U-NII-2A 5.470 to 5.725 GHz U-NII-2C 5.725 to 5.850 GHz U-NII-3/ISM **NOTE** The available bands and channels are dependent on the configured regulatory domain (country).		

Standards Compliance

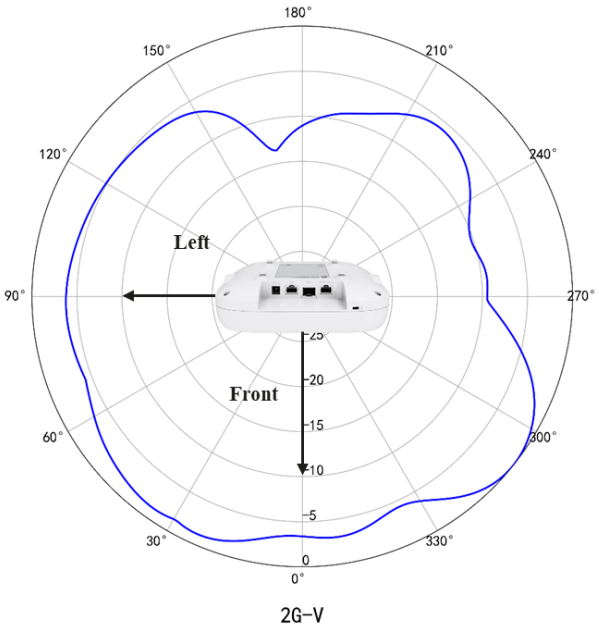
Item	Description		
Safety standards	• EN 62368-1	• IEC 62368-1	
Radio standards	• ETSI EN 300 328	• ETSI EN 301 893	• ESTI EN 303 687
EMC standards	• EN 301 489-1 • EN 301 489-17 • EN 60601-1-2 • EN 55032 • EN 55035	• AS/NZS CISPR32 • CISPR 32 • CISPR 35	• IEC/EN61000-4-2 • IEC/EN 61000-4-3 • IEC/EN 61000-4-4 • IEC/EN 61000-4-5 • IEC/EN 61000-4-6 • ICES-003
IEEE standards	• IEEE 802.11a/b/g • IEEE 802.11n • IEEE 802.11ac • IEEE 802.11ax • IEEE 802.11be	• IEEE 802.11h • IEEE 802.11d • IEEE 802.11e • IEEE 802.11k	• IEEE 802.11v • IEEE 802.11w • IEEE 802.11r
Security standards	• 802.11i，Wi-Fi Protected Access (WPA)，WPA2，WPA2-Enterprise，WPA2-PSK，WPA3，WAPI • 802.1X • Advanced Encryption Standards(AES)，Temporal Key Integrity Protocol(TKIP)，WEP，Open • EAP Type(s)		
EMF	• EN 62311	• EN 50385	
RoHS	• Directive 2002/95/EC & 2011/65/EU • (EU)2015/863		
Reach	• Regulation 1907/2006/EC		
WEEE	• Directive 2002/96/EC & 2012/19/EU		

Antennas Pattern

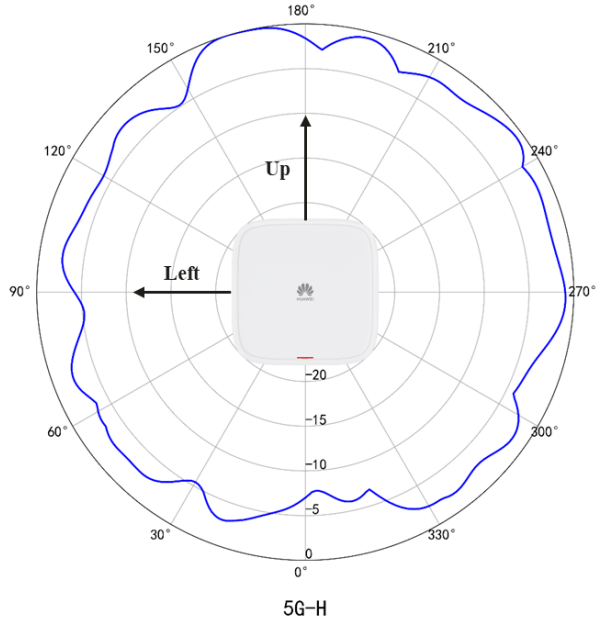
Model 1: 2.4GHz+5GHz+6GHz



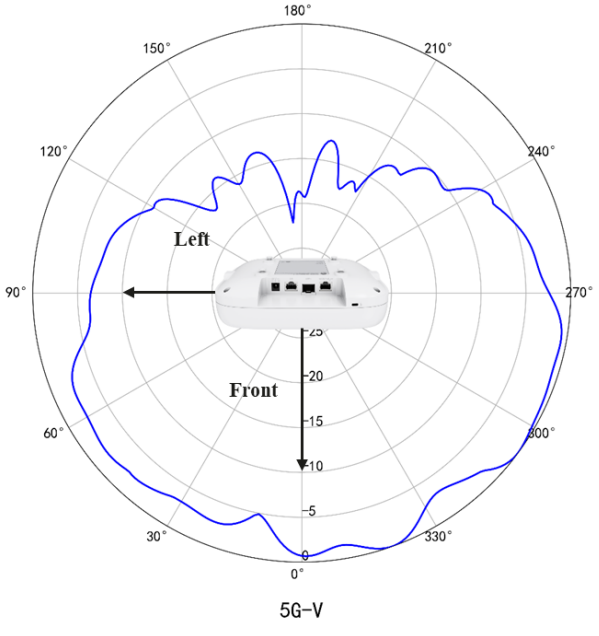
2.4GHz (Horizontal)



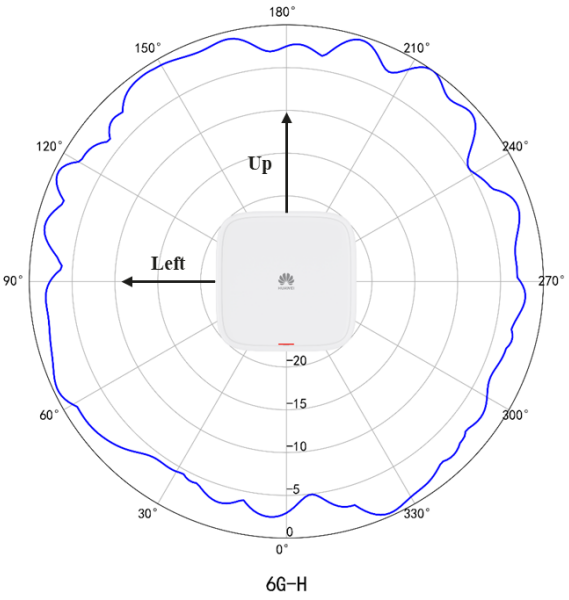
2.4GHz (Vertical)



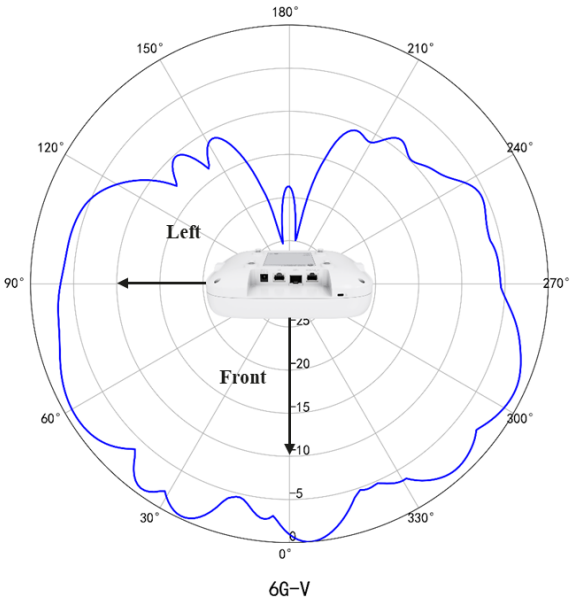
5GHz (Horizontal)



5GHz (Vertical)

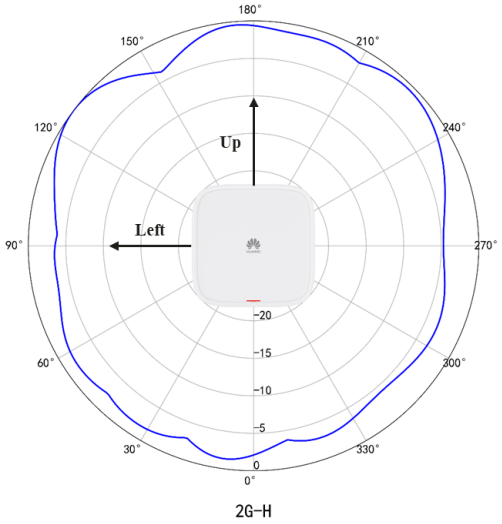


6GHz (Horizontal)

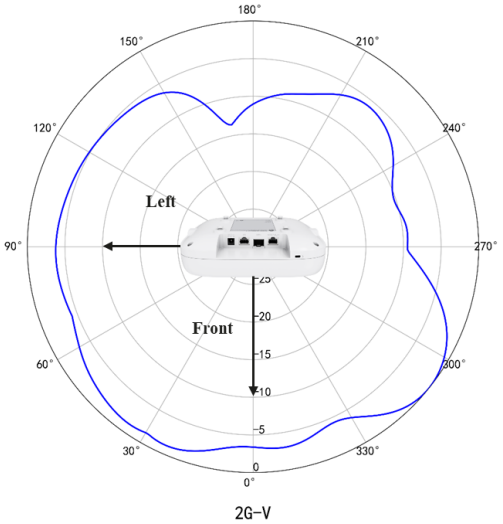


6GHz (Vertical)

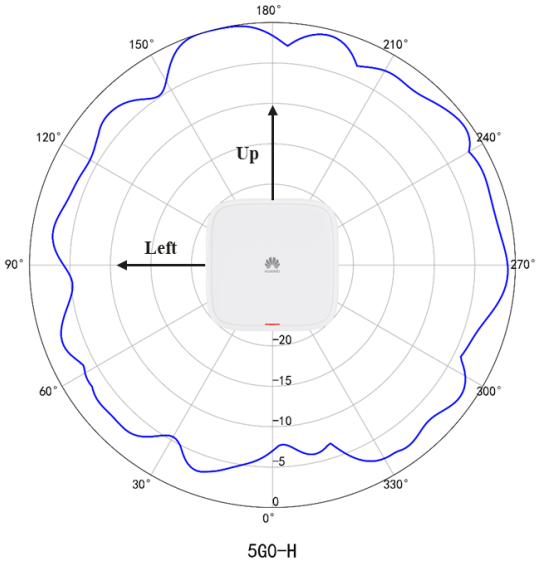
Model 2: 2.4GHz+5GHz+5GHz

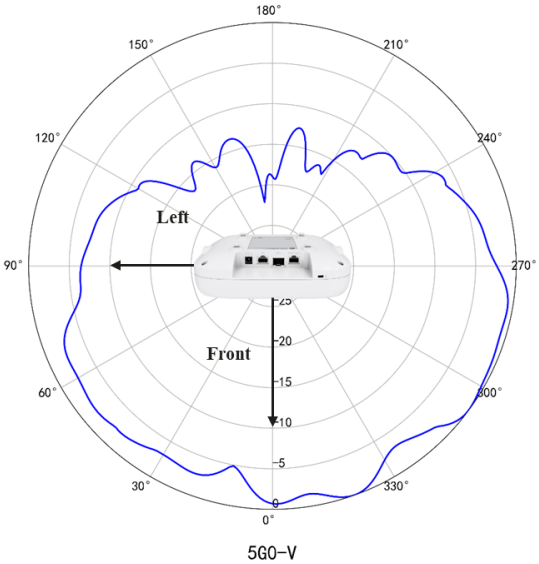


2.4GHz (Horizontal)

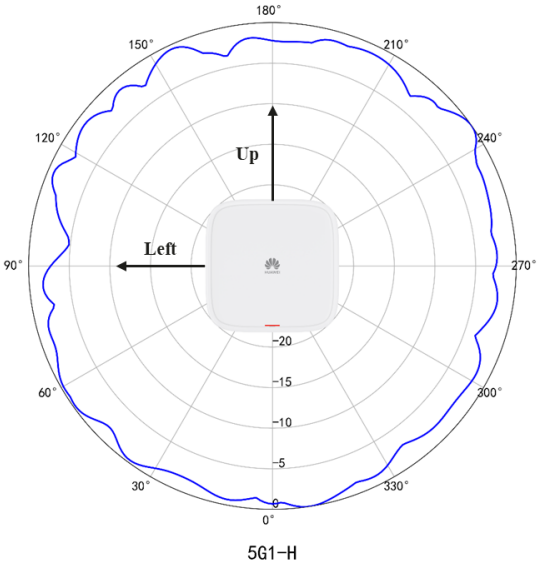


2.4GHz (Vertical)

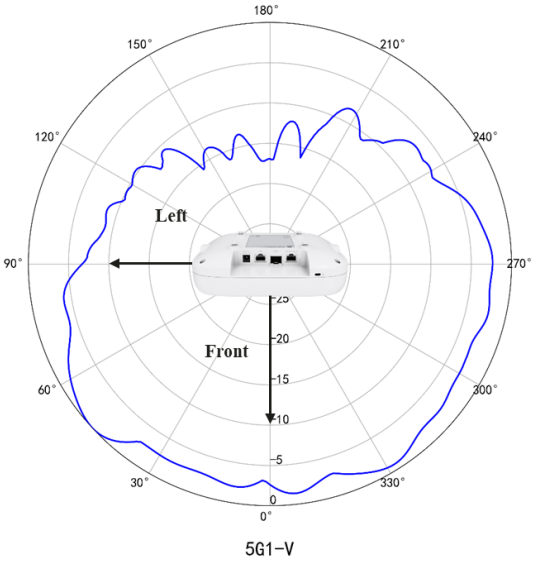




5GHz_1 (Horizontal)



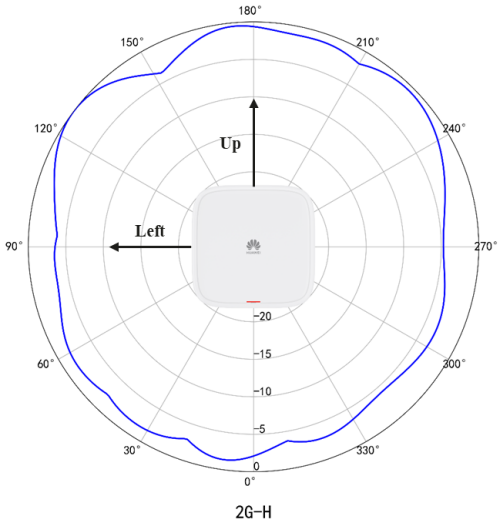
5GHz_1 (Vertical)



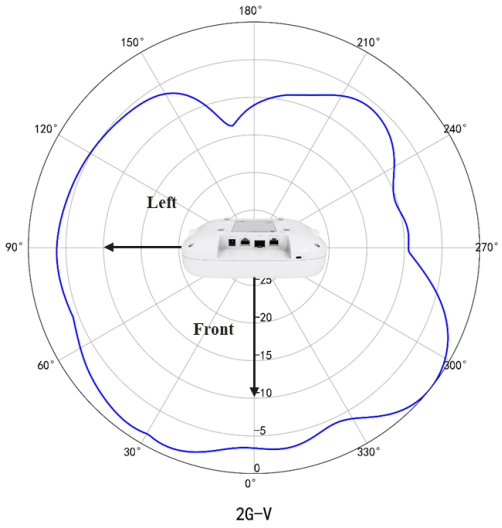
5GHz_1 (Horizontal)

5GHz_1 (Vertical)

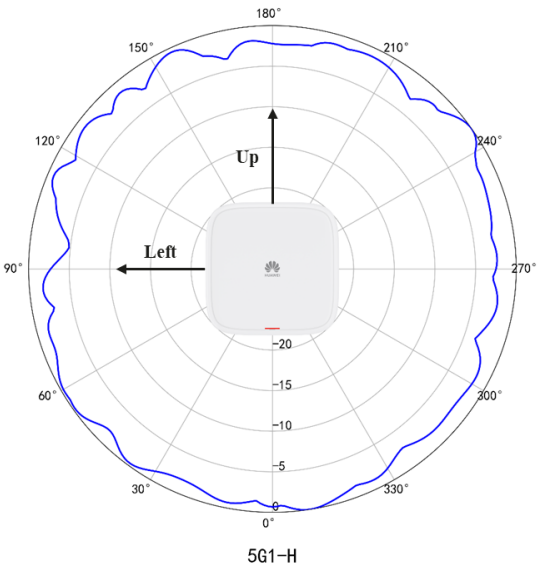
Model 3: 2.4GHz+5GHz

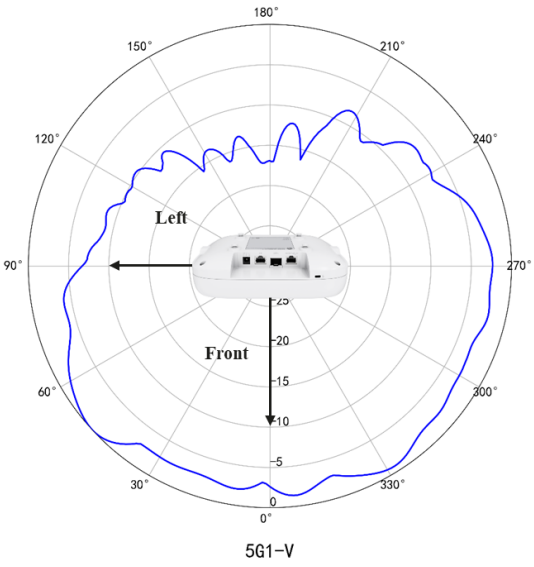


2.4GHz (Horizontal)



2.4GHz (Vertical)





5GHz (Horizontal) 5GHz (Vertical)

Disclaimer

Camera Detection is a function provided by Huawei Technologies Co., Ltd. (hereinafter referred to as "Huawei") for APs in commercial scenarios (such as enterprises and hotels). It protects natural persons in commercial facilities from infringement of legitimate rights and interests, including privacy rights, caused by illicit filming. Using wireless radio frequency technologies and camera detection algorithms, this function detects whether there are cameras in the surroundings and warns users of related risks.

This Camera Detection Disclaimer (hereinafter referred to as "this Disclaimer") is applicable to all commercial users (hereinafter referred to as "you") who use this function. By using this function, you acknowledge that you have read and agree to all the content of this Disclaimer. Please be aware that this function is purchased and installed by you. Huawei shall not be held liable for any adverse consequences caused by your installation.

1. The use of any hardware and software is subject to certain restrictions of the physical environment, software performance, and hardware capabilities. This function is no exception. When using this function, Huawei will do its best to ensure the detection accuracy, but does not guarantee that all cameras can be detected. Huawei shall not be held liable for any loss, damage, or expense caused by the use of this function. Therefore, the camera detection capability of this function cannot replace manual inspection and cannot 100% confirm or rule out the possibility that any camera exists within the monitoring scope. In addition, Huawei does not guarantee that all cameras detected by this function can be 100% confirmed or ruled out as possible infringement on legitimate rights and interests, including privacy rights.

2. Huawei promises to continuously improve the service quality, but cannot guarantee that the services provided are free of any problems. If problems that cannot be avoided by the existing technologies in the industry occur, Huawei will try its best to assist you in solving the problems. However, the service interruption does not constitute a defect of Huawei products, and Huawei shall not be held liable for any compensation arising out of or in connection with such problems.

3. Huawei will perform software/code upgrades from time to time. You shall ensure that you obtain related updates from Huawei website. Huawei shall not be liable for any responsibility arising from your failure to update.

4. Huawei shall not be liable for any direct, indirect, special, accidental, or consequential losses caused by your use of this function, including but not limited to financial losses, data losses, business interruptions, opportunity losses, and device damages. You shall be responsible for your behavior when using this function. If any loss is caused by improper use of this function, you shall be liable for the loss.

5. You may encounter force majeure or unforeseeable circumstances when using this product, including but not limited to:

   a. Data being obtained or tampered with by unauthorized individuals, groups, or organizations through certain channels;

   b. Delays due to busy communication, or interruptions, pauses, incomplete data, or data errors due to other reasons, causing errors, delays, interruptions, or pauses in transactions;

   c. Power outages and network system failures caused by earthquakes, fires, hurricanes, and other force majeure factors;

   d. Performance defects, quality problems, computer viruses, hardware faults, hacker attacks, computer virus intrusion or outbreak, and other problems in computer systems that are not attributable to Huawei;

   e. Government control, network faults, changes in government policies, and changes in laws and regulations. In case of force majeure or unforeseeable circumstances, Huawei will try its best to remedy the situations. However, Huawei shall not be held liable for any direct or indirect losses caused by force majeure or unforeseeable circumstances.

6. Huawei cannot guarantee that the software obtained from channels other than those specified by Huawei is free from computer viruses, Trojans, or hacker software. Using such products may cause unpredictable risks. You are advised not to download, install, or use such products. Huawei does not assume any legal liability arising therefrom.

7. The interpretation, validity, and enforcement of this disclaimer shall be governed by the laws of the People's Republic of China. If any dispute arises from this statement, the parties shall attempt to resolve it through friendly consultation. If consultation fails, either party may submit the dispute to the People's Court of Longgang District, Shenzhen, Guangdong Province, China for litigation.

8. The Company reserves the right to amend this statement from time to time in accordance with changes in relevant laws and regulations, as well as adjustments to the Company's operating conditions and business strategies. You may review the latest version of this statement at any time through this software, and you will receive a notification from the Company before

your first use following any modification. If you do not agree to the revised content, you should immediately stop using this function. If you continue to use this function, you will be deemed to have accepted the amended statement.

Copyright © Huawei Technologies Co., Ltd. 2026. 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

 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:www.huawei.com