Huawei AC6605-26-PWR
Brochure-Detailed

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Huawei AC6605-26-PWR Brochure-Detailed

Huawei AC6605-26-PWR is a high-performance wireless Access Controller (AC) with advanced features. By providing uniform forwarding, control, and policies for wired and wireless data, the AC6605 helps enterprises to build a wired and wireless converged network.
The AC6605 features good scalability and offers users considerable flexibility in configuring the number of managed APs. When used with Huawei's latest-generation 802.11ac and 802.11n APs, the AC6605-26-PWR delivers an adaptable solution for medium- to large-sized campus and enterprise office networks by extending wireless Metropolitan Area Network (MAN) and hotspot coverage.

Multiple port support

- Two 10GE optical ports
- 20 GE + four GE combo ports
- One RJ-45 serial port
- One RJ-45 network port
- One mini-USB serial port

Large-capacity, high-performance design with proven reliability

- Manages a maximum of 1024 APs and 10K STAs
- Backplane capacity of 128 Gbit/s with non-blocking data switching
- Port backup using Link Aggregation Control Protocol (LACP) or Multiple Spanning Tree Protocol (MSTP)
- Dual hot-swappable AC/DC power supplies

Easy to install and easy to maintain

- Convenient size (442 mm x 420 mm x 43.6 mm): small enough to fit a standard cabinet
- Hot swappable power supplies for easy maintenance
- Boolean port support for environmental monitoring and intra-board temperature probes for monitoring the AC operating environment in real time

Dynamic energy management

- Low-noise fans dynamically adjust to load changes to keep equipment noise and power consumption low.
- Automatic power-saving mode engages during idle operation (when no peer device is connected).
- Highly integrated, energy-saving design provides even higher performance and lower power consumption when coupled with an intelligent device management system.

Advanced Network Features

- Application scenarios: medium- to large-sized enterprises; campus and hospital networks
- Scalable licensing options
- Flexible networking and forwarding
- 128 Gbit/s switching capacity, eliminating the traffic -forwarding bottleneck at the WLAN core layer.
- Compatibility with 802.11a/b/g/n/ac
- Comprehensive user policy management and authorization controls
- Secure and reliable 1+1 hot backup and N+1 backup
- Graphics-based, real-time, and efficient WLAN management and maintenance for optimum network performance
- Power over Ethernet (PoE) power supply for up to 24 ports
- IPv6 support

Typical Networking

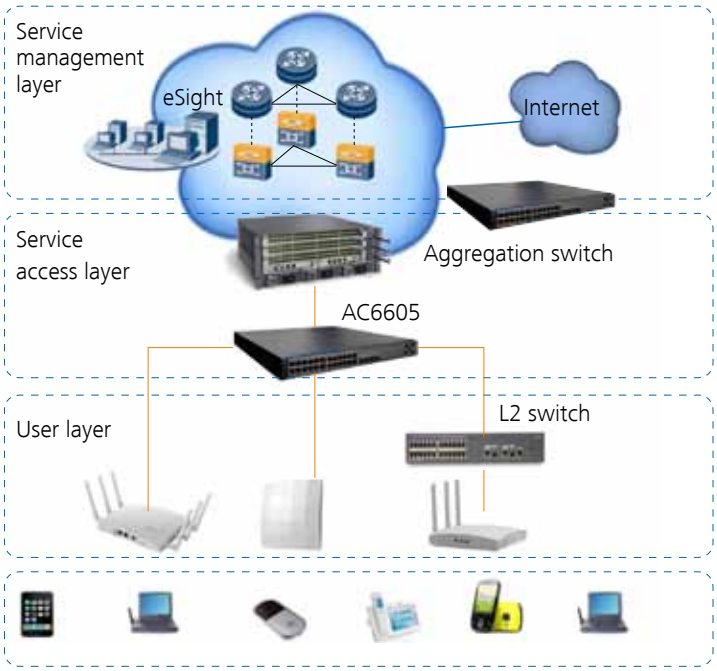
The AC6605-26-PWR can be deployed in inline, bypass, Wireless Distribution System (WDS), or Wireless Mesh Network (WMN) mode.

1. Inline Networking

In inline networking, APs or access switches directly connect to the AC6605, which functions as both an AC and an aggregation switch to forward and process data and management services for the APs.

In this scenario, the AC6605 sets up Control and Provisioning of Wireless Access Points (CAPWAP) tunnels with the APs for configuration and management. Service data from wireless users can be forwarded between APs and the AC6605 over CAPWAP data tunnels or be directly forwarded by the APs.

Direct forwarding is typically used with large-scale and centralized WLANs in inline networking scenarios to simplify network architecture.

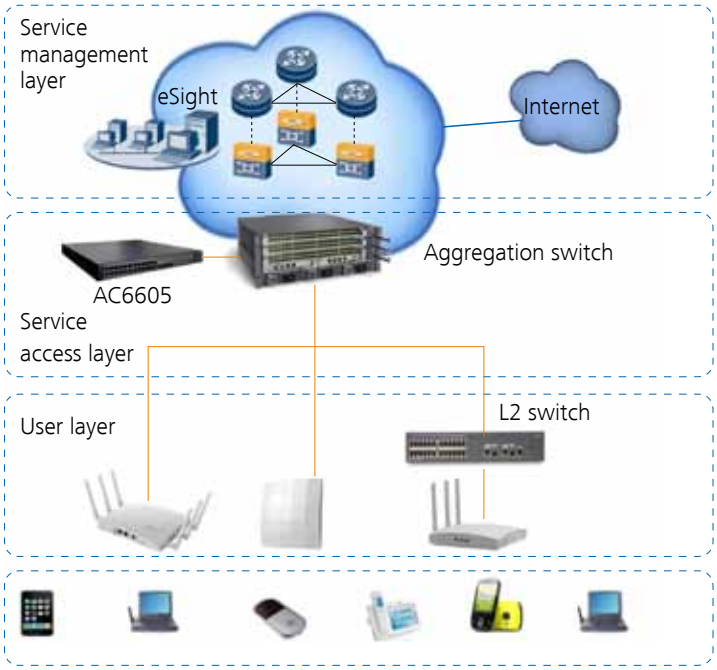


The AC6605 provides powerful access, aggregation, and switching capabilities and can provide PoE/PoE+ connections to APs.

2. Bypass Networking

In bypass networking, the AC6605 connects to a network device (usually an aggregation switch) to manage APs. The AC6605 manages all the APs connected to the aggregation switch. Management flows are transmitted in CAPWAP tunnels. Data flows can be forwarded by the AC over CAPWAP tunnels or forwarded to the upper layer network by the aggregation switch without passing through the AC6605.

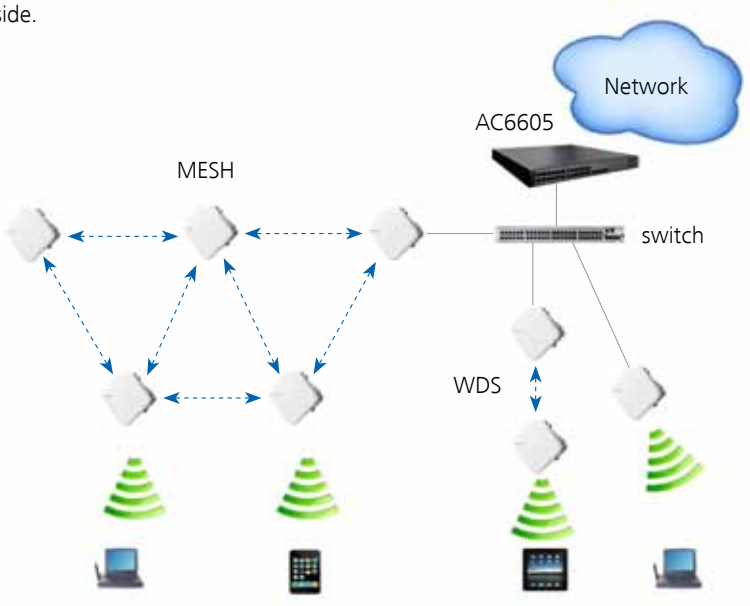
This network topology works well where APs are scattered across hotspots.



Bypass mode deployments require only a small modification to the existing network. You can select direct forwarding or tunnel forwarding mode according to networking requirements. Because tunnel forwarding is commonly used for overlay network deployments, Huawei recommends tunnel forwarding for most enterprise networks.

3. WDS and Mesh Networking

The WDS and WMN modes allow multiple APs to be connected wirelessly in a distributed system that extends the range of wireless network coverage. The WDS and Mesh networks connect to an AC through a switch, and the AC connects to the network through a network device, such as a gateway or an aggregation switch. The WDS and Mesh networks connect to user Stations (STAs) or PCs on the user side.



WDS and Mesh networking are used to expand outdoor wireless coverage areas.

Physical Specifications

Item		Description
Dimensions (width x depth x height)		43.6 mm x 442 mm x 420 mm
Maximum power consumption		85 W
Weight		Net weight: 5.48 kg Fully configured with 150 W power supplies: 7.16 kg Fully configured with 500 W power supplies: 7.48 kg
Operating temperature		-5°C to +50°C
Relative humidity		5% RH to 95% RH, noncondensing
Operating altitude		150 W DC power supply: 0 m to 2000 m Others: 0 m to 3000 m
AC input voltage	Rated voltage	100 V AC to 240 V AC, 50/60 Hz
	Voltage range	90 V AC to 264 V AC, 47 to 63 Hz
DC input voltage	Rated voltage	-48 V DC to -60 V DC
	Voltage range	-36 V DC to -72 V DC

Performance Specifications

Parameter	Specifications
Forwarding capability	10 Gbit/s
Number of managed APs	1K
Number of access users	• Entire device: 10K • Single AP: a maximum of 256 (depending on the AP model)
Number of MAC address entries	16K
Number of VLANs	4K
Number of routing entries	10K
Number of ARP entries	16K
Number of multicast forwarding entries	4K
Number of DHCP IP address pools	128 IP address pools, each of which contains a maximum of 16K IP addresses
Number of local users	1000

Item	Specifications
Number of ACLs	8K
Number of ESSIDs	4K
User group management	• 128 user groups • Each user group can reference a maximum of eight ACLs. • Each user group can associate with a maximum of 128 ACL rules.

Feature List

Switching and forwarding features

Feature		Description
Ethernet features	Ethernet	• Operating modes of full duplex, half duplex, and auto-negotiation • Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation • Flow control on interfaces • Jumbo frames • Link aggregation • Load balancing among links of a trunk • Interface isolation and forwarding restriction • Broadcast storm suppression
	VLAN	• Access modes of access, trunk, and hybrid • Default VLAN
	MAC	• Automatic learning and aging of MAC addresses • Static, dynamic, and blackhole MAC address entries • Packet filtering based on source MAC addresses • Interface-based MAC learning limiting
	ARP	• Static and dynamic ARP entries • ARP in a VLAN • Aging of ARP entries
	LLDP	• LLDP
Ethernet loop protection	MSTP	• STP • RSTP • MSTP • BPDU protection, root protection, and loop protection • Partitioned STP

Feature		Description
IPv4 forwarding	IPv4 features	• ARP and RARP • ARP proxy • Auto-detection • NAT • Bonjour Protocol
	Unicast routing features	• Static route • RIP-1 and RIP-2 • OSPF • BGP • IS-IS • Routing policies and policy-based routing • URPF check • DHCP client, server and relay • DHCP snooping
	Multicast routing features	• IGMPv1, IGMPv2, and IGMPv3 • PIM-SM • Multicast routing policies • RPF
IPv6 forwarding	IPv6 features	• ND Protocol
	Unicast routing features	• Static route • RIPng • OSPFv3 • BGP4+ • IS-IS IPv6 • DHCPv6 • DHCPv6 Snooping
	Multicast routing features	• MLD • MLD Snooping
Device reliability	BFD	• BFD
Layer 2 multicast features	Layer 2 multicast	• IGMP snooping • Prompt leave • Multicast traffic control • Inter-VLAN multicast replication
Ethernet OAM	EFM OAM	• Neighbor discovery • Link monitoring • Fault notification • Remote loopback

Feature		Description
QoS features	Traffic classification	• Traffic classification based on the combination of the L2 protocol header, IP 5-tuple, and 802.1p priority
	Action	• Access control after traffic classification • Traffic policing based on traffic classification • Re-marking packets based on traffic classifiers • Class-based packet queuing • Associating traffic classifiers with traffic behaviors
	Queue scheduling	• PQ scheduling • DRR scheduling • PQ+DRR scheduling • WRR scheduling • PQ+WRR scheduling
	Congestion avoidance	• SRED • WRED
Configuration and maintenance	Terminal service	• Configurations using command lines • Error message and help information in English • Login through console and Telnet terminals • Send function and data communications between terminal users
	File system	• File systems • Directory and file management • File uploading and downloading using FTP and TFTP
	Debugging and maintenance	• Unified management over logs, alarms, and debugging information • Electronic labels • User operation logs • Detailed debugging information for network fault diagnosis • Network test tools such as traceroute and ping commands • Interface mirroring and flow mirroring
	Version upgrade	• Device software loading and online software loading • BIOS online upgrade • In-service patching
Security and management	System security	• Different user levels for commands, preventing unauthorized users from accessing device • SSHv2.0 • RADIUS and HWTACACS authentication for login users • ACL filtering • DHCP packet filtering (with the Option 82 field) • Defense against control packet attacks • Defenses against attacks such as source address spoofing, Land, SYN flood (TCP SYN), Smurf, ping flood (ICMP echo), Teardrop, and Ping of Death attacks • IPSec
	Network management	• ICMP-based ping and traceroute • SNMPv1, SNMPv2c, and SNMPv3 • Standard MIB • RMON

Wireless networking capabilities

Feature	Description
Networking between APs and ACs	• APs and ACs can be connected through a Layer 2 or Layer 3 network. • APs can be directly connected to an AC. • APs are deployed on a private network, while ACs are deployed on the public network to implement NAT traversal. • ACs can be used for Layer 2 bridge forwarding or Layer 3 routing.
Forwarding mode	• Direct forwarding (distributed forwarding or local forwarding) • Tunnel forwarding (centralized forwarding) • Centralized authentication and distributed forwarding • In direct forwarding mode, user authentication packets support tunnel forwarding.
Wireless networking mode	WDS bridging: • Point-to-point (P2P) wireless bridging • Point-to-multipoint (P2MP) wireless bridging • Automatic topology detection and loop prevention (STP) Wireless mesh network • Access authentication for mesh devices • Mesh routing algorithm • Go-online without configuration

AC discovery	• An AP can obtain the device's IP address in any of the following ways:
	  - Static configuration
	  - DHCP
	  - DNS
	• The AC uses DHCP or DHCPv6 to allocate IP addresses to APs.
	• DHCP or DHCPv6 relay is supported.
	• On a Layer 2 network, APs can discover the AC by sending broadcast CAPWAP packets.

CAPWAP tunnel	• Centralized CAPWAP • CAPWAP control tunnel and data tunnel (optional) • CAPWAP tunnel forwarding and direct forwarding in an extended service set (ESS) • Datagram Transport Layer Security (DTLS) encryption, which is enabled by default for the CAPWAP control tunnel • Heartbeat detection and tunnel reconnection
Active and standby ACs	• Enables and disables the switchback function. • Supports load balancing. • Supports 1+1 hot backup. • Supports N+1 backup.

AP management

Feature	Description
AP access control	• Displays MAC addresses or SNs of APs in the whitelist. • Adds a single AP or multiple APs (by specifying a range of MAC addresses or SNs) to the whitelist. • Automatically discovering and manually confirming APs. • Automatically discovering APs without manually confirming them.
AP region management	• Supports three AP region deployment modes: - Distributed deployment: APs are deployed independently. An AP is equivalent to a region and does not interfere with other APs. APs work at the maximum power and do not perform radio calibration. - Common deployment: APs are loosely deployed. The transmit power of each radio is less than 50% of the maximum transmit power. - Centralized deployment: APs are densely deployed. The transmit power of each radio is less than 25% of the maximum transmit power. • Specifies the default region to which automatically discovered APs are added.
AP profile management	• Specifies the default AP profile that is applied to automatically discovered APs.
AP type management	• Manages AP attributes including the number of interfaces, AP types, number of radios, radio types, maximum number of virtual access points (VAPs), maximum number of associated users, and radio gain (for APs deployed indoors). • Provides default AP types. • Supports user-defined AP types.
Network topology management	Supports LLDP topology detection.

Radio management

Feature	Description
Radio profile management	• The following parameters can be configured in a radio profile: - Radio working mode and rate - Automatic or manual channel and power adjustment mode - Radio calibration interval • The radio type can be set to 802.11b, 802.11b/g, 802.11b/g/n, 802.11g, 802.11n, 802.11g/n, 802.11a, 802.11a/n, or 802.11ac. • You can bind a radio to a specified radio profile.
Unified static configuration of parameters	Radio parameters such as the channel and power of each radio are configured on the AC and then delivered to APs.

Item	Specifications

Dynamic management	• APs can automatically select working channels and power when they go online.
	• In an AP region, APs automatically adjust working channels and power in the event of signal interference:
	  - Partial calibration: The optimal working channel and power of a specified AP can be adjusted.
	  - Global calibration: The optimal working channels and power of all the APs in a specified region can be adjusted.
	• When an AP is removed or goes offline, the AC increases the power of neighboring APs to compensate for the coverage hole.
	• Automatic selection and calibration of radio parameters in AP regions are supported.

Enhanced service capabilities	• The AC supports 802.1a/b/g/n/ac. These modes can be used independently or jointly (a\n, b\g, b\g\n, and g\n). • The AC preferentially uses the 5 GHz frequency band for STAs. • 2.4 GHz and 5 GHz frequency load balancing

WLAN service management

Feature	Description
ESS management	• Allows you to enable SSID broadcast, set the maximum number of access users, and set the association aging time in an ESS. • Isolates APs at Layer 2 in an ESS. • Maps an ESS to a service VLAN. • Associates an ESS with a security profile or a QoS profile. • Enables IGMP for APs in an ESS.
VAP-based service management	• Adds multiple VAPs at a time by binding radios to ESSs. • Displays information about a single VAP, VAPs with a specified ESS, or all VAPs. • Supports configuration of offline APs. • Creates VAPs according to batch delivered service provisioning rules in automatic AP discovery mode.
Service provisioning management	• Supports service provisioning rules configured for a specified radio of a specified AP type. • Adds automatically discovered APs to the default AP region. The default AP region is configurable. • Applies a service provisioning rule to a region to enable APs in the region to go online.
Multicast service management	• Supports IGMP snooping. • Supports IGMP proxy.

Load balancing	• Performs load balancing among radios in a load balancing group.
	• Supports two load balancing modes:
	  - Based on the number of STAs connected to each radio
	  - Based on the traffic volume on each radio

Item	Specifications
BYOD (Bring Your Own Device)	• Identification of device types according to the OUI in the MAC address • Identification of device types according to the user agent (UA) field in an HTTP packet • Identification of device types according to DHCP Option information • Carrying of device type information in RADIUS authentication and accounting packets
Positioning services	• Locating AeroScout and Ekahau tags • Locating Wi-Fi terminals
Spectrum analysis	• Identification of the following interference sources: bluetooth, microwave ovens, cordless phones, ZigBee, game controller, 2.4 GHz/5 GHz wireless audio and video devices, and baby monitors. • Working with the eSight to locate the interference sources and display spectrum.

WLAN user management

Feature	Description
Address allocation of wireless users	Functions as a DHCP server to assign IP addresses to wireless users.
WLAN user management	• Supports user blacklist and whitelist. • Controls the number of access users: - Based on APs - Based on SSIDs • Logs out users in any of the following ways: - Using RADIUS DM messages - Using commands • Supports various methods to view information: - Allows you to view the user status by specifying the user MAC address, AP ID, radio ID, or WLAN ID. - Displays the number of online users in an ESS, AP, or radio. - Collects packet statistics on air interface based on user.
WLAN user roaming	• Supports intra-AC Layer 2 roaming. **NOTE** Users can roam between APs connected to different physical ports on an AC. • Supports inter-VLAN Layer 3 roaming on an AC. • Supports fast key negotiation in 802.1x authentication. • Authenticates users who request to reassociate with the AC and rejects the requests of unauthorized users. • Delays clearing user information after a user goes offline so that the user can rapidly go online again.
User group management	• Supports ACLs. • Supports user isolation: - Inter-group isolation - Intra-group isolation

WLAN security

Feature	Description
WLAN security profile management	• Manages authentication and encryption modes using WLAN security profiles. • Binds security profiles to ESS profiles.

Authentication modes	• Open system authentication with no encryption
	• WEP authentication/encryption
	• WPA/WPA2 authentication and encryption:
	  - WPA/WPA2-PSK+TKIP
	  - WPA/WPA2-PSK+CCMP
	  - WPA/WPA2-802.1x+TKIP
	  - WPA/WPA2-802.1x+CCMP
	  - WPA/WPA2-PSK+TKIP-CCMP
	  - WPA/WPA2-802.1x+TKIP-CCMP
	• WAPI authentication and encryption:
	  - Supports centralized WAPI authentication.
	  - Supports three-certificate WAPI authentication, which is compatible with traditional two-certificate authentication.
	  - Issues a certificate file together with a private key.
	• Allows users to use MAC addresses as accounts for authentication by the RADIUS server.
	• Portal authentication:
	  - Authentication through an external Portal server
	  - Built-in Portal authentication and authentication page customization

Combined authentication	• Combined MAC authentication:
	  - PSK+MAC authentication
	• MAC+portal authentication:
	  - MAC authentication is used first. When MAC authentication fails, portal authentication is used.
	  - This type of authentication applies only to centralized forwarding.

AAA	• Local authentication/local accounts (MAC addresses and accounts)
	• RADIUS authentication
	• Multiple authentication servers:
	  - Supports backup authentication servers.
	  - Specifies authentication servers based on account.
	  - Configures authentication servers based on account.
	  - Binds user accounts to SSIDs.

Security isolation	• Port-based isolation • User group-based isolation
WIDS	Rouge device scan, identification, defense, and countermeasures, which includes dynamic blacklist configuration and detection of rogue APs, STAs, and network attacks.
Authority control	ACL limit based on the following: • Port • User group • User

Item	Specifications

Other security features	• SSID hiding
	• IP source guard:
	  - Configures IP and MAC binding entries statically.
	  - Generates IP and MAC binding entries dynamically.

WLAN QoS

Feature	Description
WMM profile management	• Enables or disables Wi-Fi Multimedia (WMM). • Allows a WMM profile to be applied to radios of multiple APs.
Traffic profile management	• Manages traffic from APs and maps packet priorities according to traffic profiles. • Applies a QoS policy to each ESS by binding a traffic profile to each ESS.
AC traffic control	• Manages QoS profiles. • Uses ACLs to perform traffic classification. • Limits incoming and outgoing traffic rates for each user based on inbound and outbound CAR parameters. • Limits the traffic rate based on ESSs or VAPs.
AP traffic control	• Controls traffic of multiple users and allows users to share bandwidth. • Limits the rate of a specified VAP.

Packet priority configuration	• Sets the QoS priority (IP precedence or DSCP priority) for CAPWAP control channels.
	• Sets the QoS priority for CAPWAP data channels:
	  - Allows you to specify the CAPWAP header priority.
	  - Maps 802.1p priorities of user packets to ToS priorities of tunnel packets.

Airtime scheduling	• Allocates equal time to users for occupying the channel, which improves users' Internet access experience.

Standards Compliance

Environmental standards compliance

Item	Description
MIL-HDBK-217F	Electronic Product Reliability Estimation Manual
ETS EN 300 019 1-1 V.2.1.4. Class 1.2	Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-1: Classification of environmental conditions; Storage
ETS EN 300 019-1-2 V.2.1.4. Class 2.2	Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-2: Classification of environmental conditions; Transportation

Item	Specifications
ETSI EN 300 019-1-3	Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-3: Classification of environmental conditions; Stationary use at weatherprotected locations
ETSI EN 300 019-2-1	Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 2-1: Specification of environmental tests; Storage
ETSI EN 300 019-2-2	Equipment Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 2-2: Specification of environmental tests; Transportation
ETSI EN 300 019-2-3	Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 2-3: Specification of environmental tests; Stationary use at weatherprotected locations 6
IEC 60721-3-3	Classification of environmental conditions Part3: Classification of groups of environmental parameters and their severities- Section 3: Stationary use at weatherprotected locations

EMC standards compliance

Item	Description
ETSI EN 300 386 V1.4.1(2008-04)	Electro Magnetic Compatibility test specification
IEC61000-4-11,2004	Electromagnetic compatibility(EMC)-Part 4-11:Testing and measurement techniques-Voltage dips, short interruptions and voltage variations immunity tests
IEC 61000-4-4	Electromagnetic compatibility(EMC)-Part 4-4:Testing and measurement techniques-Electrical fast transient/burst immunity test
IEC61000-4-2, 2009	Electromagnetic compatibility(EMC) Section 4.2 Electrostatic discharge immunity test- Basic EMC Publication
IEC61000-4-3, 2006	Electromagnetic compatibility Part4-3:Testing and measurement techniques-Radiated, radio-frequency, electromagnetic field immunity test
IEC61000-4-5, 2005	Electromagnetic compatibility(EMC)- Part4-5:Testing and measurement techniques-Surge immunity test
IEC61000-4-6, 2006	Electromagnetic compatibility(EMC) Part4:Testing and measurement techniques Section 6:immunity to conducted disturbance,induced by radio-frequency fields
IEC61000-4-29, 2000	Electromagnetic compatibility(EMC)-Part4-29: Testing and measurement techniques-Voltage dips,shot interruptions and voltage variations on d.c. input power port immunity tests

Item	Specifications
IEC 61000-3-2	Electromagnetic compatibility(EMC)-Part3-2: Limits-Limits for harmonic current emissions(equipment input current ≤16A per phase)
IEC 61000-3-3	Electromagnetic compatibility(EMC)-Part3-3: Limits-Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems, for equipment with rated current ≤16A per phase and not subject to conditional connection
ETSI EN 300 132-2	Environmental Engineering (EE);Power supply interface at the input to telecommunications equipment; Part 2: Operated by direct current (dc)
AS/NZS CISPR 22:2006	Information technology Equipment - Radio disturbance characteristics - Limits and methods of measurement
EN55022/EN55024-ITE	Information technology Equipment - Radio disturbance characteristics - Limits and methods of measurement Information technology Equipment - Immunity characteristics - Limits and methods of measurement
ITU-T K.20	Recommendation K.20 (02/00) - Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents
ITU-T K.21	SERIES K:PROTECTION AGAINST INTERFERENCE Resistibility of telecommunication equipment installed in a customer premises to overvoltages and overcurrents
ITU-T K.45	Resistibility of telecommunication equipment installed in the access and trunk networks to overvoltages and overcurrents
ITU-T K.44	SERIES K:PROTECTION AGAINST INTERFERENCE Resistibility test for telecommunication equipment exposed to overvoltages and overcurrents - Basic recommendation
ICES-003	Digital Apparatus
GB9254	Information technology equipment--Radio disturbance characteristics--Limits and methods of measurement

Safety standards compliance

Item	Description
IEC60950-1: 2005	Safety of information technology equipment including Electrical Business Equipment
IEC 529	Classification of degrees of protection provided by enclosures
UL60950-1: 2007	Safety of information technology equipment including Electrical Business Equipment
CSA C22.2 NO.950 UL	Standard for Safety Communications Cables
EN60950	Safety of Information technology equipment
EN41003	Safety of Information technology equipment

Item	Specifications
AS 3260	Approval and Test Specification - Safety of information technology Equipment including electronic business Equipment
ETS 300 119	European telecommunication standard for equipment practice
GB 4943	Safety of information technology equipment including electrical business equipment

RoHS

Item	Description
Directive 2002/95/EC & 2011/65/EU	Restriction of Hazardous Substances Directive

Reach

Item	Description
Regulation 1907/2006/EC	Registration, Evaluation, Authorization, and Restriction of Chemicals

WEEE

Item	Description
Directive 2002/96/EC & 2012/19/EU	Waste Electrical and Electronic Equipment Directive

Professional Service and Support

Huawei WLAN planning tools deliver expert network design and optimization services using the most professional simulation platform in the industry. Backed by fifteen years of continuous investment in wireless technologies, extensive network planning and optimization experience, as well as rich expert resources, Huawei helps customers:

- Design, deploy, and operate a high-performance network that is reliable and secure.
- Maximize return on investment and reduce operating expenses.

More Information

For more information, please visit http://e.huawei.com or contact your local Huawei office.

Enterprise Services

Product Overview

Marketing Documentation

HUAWEI TECHNOLOGIES CO.,LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129,P.R.China
Tel: +86 755 28780808

www.huawei.com