Huawei

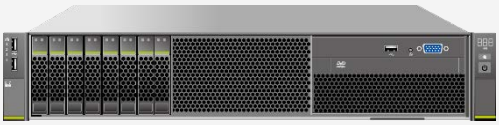
AC6800V

Wireless Access Controller

Datasheet

Product Overview

The AC6800V is a high-specification wireless access controller (AC) for large enterprise campuses, enterprise branches, and school campuses. Based on the Huawei-developed server platform, the AC6800V can manage up to 10K access points (APs) and provide 60 Gbit/s forwarding performance. It features high scalability and offers users considerable flexibility in configuring the number of managed APs. When used with Huawei's full series 802.11ac and 802.11n APs, the AC6800V delivers an adaptable solution for large campus networks, enterprise office networks, wireless Metropolitan Area Network (MAN), and hotspot coverage.



Huawei AC6800V wireless access controller

Product Features.

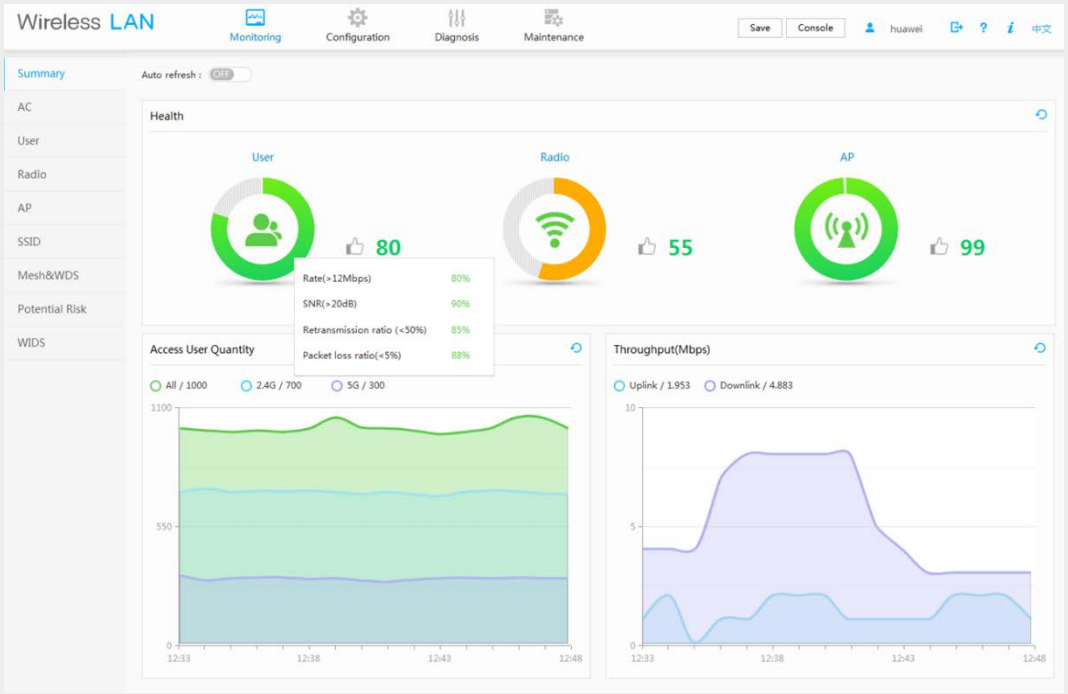
- Large-capacity and high-performance design
  - The AC6800V is capable of supporting medium and large campuses with up to 10K APs.
  - Provides 6x10GE optical interfaces and 6xGE electrical interfaces, providing 60 Gbit/s forwarding performance.
  - The AC6800V can manage up to 100K users.
- Various roles
  - The AC6800V has a built-in Portal/AAA server and can provide Portal/802.1X authentication for users, reducing customer investment.
- Flexible networking
  - The AC can be deployed in inline, bypass, bridge, and Mesh network modes, and supports both centralized and local forwarding.
  - The AC and APs can be connected across a Layer 2 or Layer 3 network. In addition, NAT can be deployed when APs are deployed on the private network and the AC is deployed on the public network.
  - The AC is compatible with Huawei full-series 802.11n and 802.11ac APs and supports hybrid networking of 802.11n and 802.11ac APs for simple scalability.
- Built-in application identification server
  - Supports Layer 4 to Layer 7 application identification and can identify over 1600 applications, including common office applications and P2P download applications, such as Lync, FaceTime, YouTube, and Facebook.
  - Supports application-based policy control technologies, including traffic blocking, traffic limit, and priority adjustment policies.
  - Supports automatic application expansion in the application signature database.
- Comprehensive reliability design
  - Supports redundant AC power supplies and hot swappable power supplies.
  - Supports AC 1+1 HSB, and N+1 backup, ensuring uninterrupted services.
  - Supports port backup based on the Link Aggregation Control Protocol (LACP) or Multiple Spanning Tree Protocol (MSTP)..
  - Supports WAN authentication escape between APs and ACs. In local forwarding mode, this feature retains the online state of existing STAs and allows access of new STAs when APs are disconnected from ACs, ensuring service continuity.

Built-in visualized network management platform

The AC6800V has a built-in web system that is easy to configure and provides comprehensive monitoring and intelligent diagnosis.

- Health-centric one-page monitoring, visualized KPIs

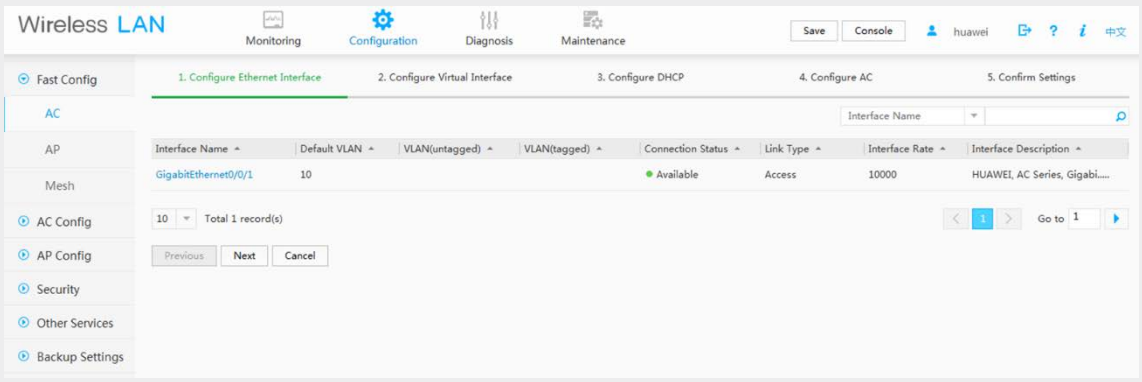
One page integrates the summary and real-time statistics. KPIs are displayed in graphs, including user performance, radio performance, and AP performance, enabling users to extract useful information from the massive amounts of monitored data, while also knowing the device and network status instantly.



Monitoring interface

- Profile-based configuration by AP group simplifies configuration procedure and improves efficiency.

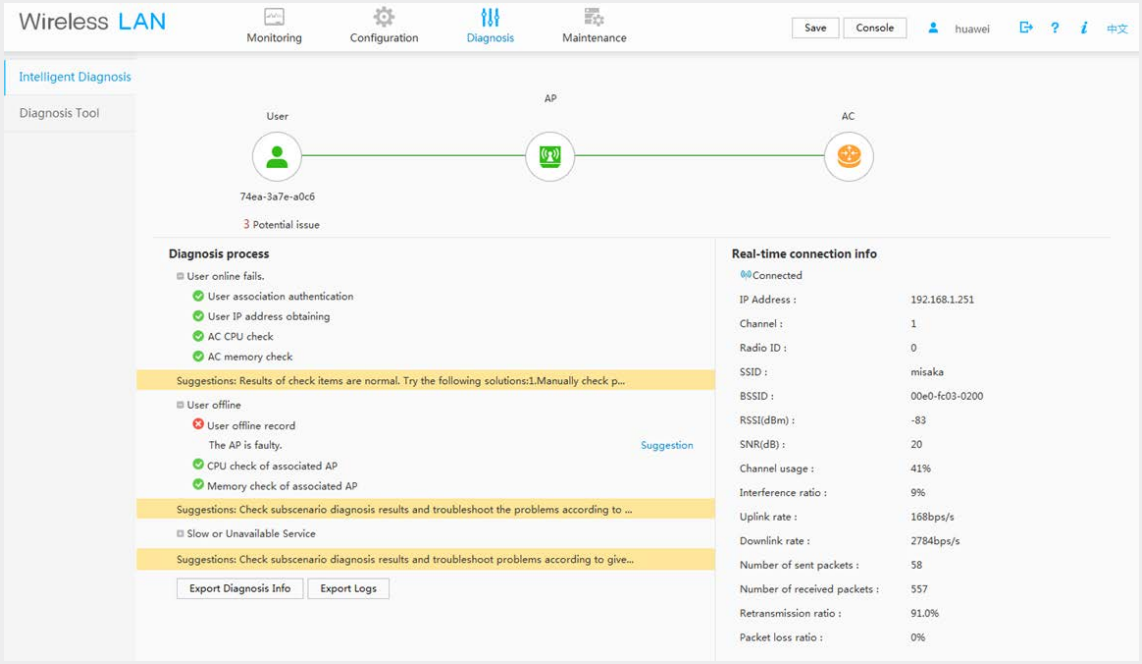
The web system supports AP group-centric configuration and automatically selects the common parameters for users, meaning that users do not need to pre-configure the common parameters, simplifying the configuration procedure.
If two AP groups have small configuration differences, users can copy the configurations of one AP group to the other. This improves configuration efficiency because users only need to modify the original configurations, not create entirely new ones each time.



Configuration interface

- One-click diagnosis solves 80% of common network problems.

The web system supports real-time and periodic one-click intelligent diagnosis from the dimensions of users, APs, and ACs, and provides feasible suggestions for troubleshooting the faults.



Intelligent diagnosis

AC6800V features

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 VLAN pool
	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
IPv4 forwarding	IPv4 features	ARP and RARP ARP proxy Auto-detection NAT mDNS

Feature		Description
IPv4 forwarding	Unicast routing features	Static route RIP-1 and RIP-2 OSPF BGP IS-IS Routing policies and policy-based routing URPF check DHCP 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
	Application control	Smart Application Control (SAC)
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 Intelligent diagnosis Interface mirroring and flow mirroring Syslog
	Version upgrade	Device software loading and online software loading BIOS online upgrade In-service patching
Security and management	Network management	ICMP-based ping and traceroute SNMPv1, SNMPv2c, and SNMPv3 Standard MIB RMON NetStream

Feature		Description
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) Local attack defense function that can protect the CPU and ensure that the CPU can process services Defense against control packet attacks Defenses against attacks such as source address spoofing, Land, SYN flood (TCP SYN), Smurf, ping flood (ICMP echo), Teardrop, broadcast flood, and Ping of Death attacks IPSec URL filtering Antivirus Intrusion prevention

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. WAN authentication escape is supported between APs and ACs. In local forwarding mode, this feature retains the online state of existing STAs and allows access of new STAs when APs are disconnected from ACs, ensuring service continuity.
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. Soft GRE forwarding. Tunnel forwarding + EoGRE tunnel
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.

Feature	Description
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 • Mesh network with multiple MPPs • Vehicle-ground fast link handover • Mesh client mode
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. Supports wireless configuration synchronization between ACs.

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 profile management	Specifies the default AP profile that is applied to automatically discovered APs.
AP group management	The AP group function is used to configure multiple APs in batches. When multiple APs managed by an AC require the same configurations, you can add these APs to one AP group and configure the AP group to complete AP configuration.

Feature	Description
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 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.
Network topology management	Supports LLDP topology detection.
AP working mode management	Supports AP working mode switchover. The AP working mode can be switched to the Fat or cloud mode on the AC.

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, 802.11ac Wave1, or 802.11ac Wave2. You can bind a radio to a specified radio profile. Supports MU-MIMO.
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.
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). Band steering: Enables terminals to preferentially access the 5G frequency band, achieving load balancing between the 2.4G and 5G frequency bands. Smart roaming: Enables sticky terminals to roam to APs with better signals.

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. Supports Chinese SSIDs.
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
Bring Your Own Device (BYOD)	Identifies device types according to the OUI in the MAC address. Identifies device types according to the user agent (UA) field in an HTTP packet. Identifies device types according to DHCP Option information. Carries device type information in RADIUS authentication and accounting packets.
Location services	Locates AeroScout and Ekahau tags. Locates Wi-Fi terminals. Locates Bluetooth terminals. Locates Bluetooth tags.
Spectrum analysis	Identifies 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. Works with the eSight to display spectrums of interference sources.
Hotspot2.0	Supports a Hotspot2.0 network.
Internet of Things (IoT)	Supports IoT cards on the AP to converge the WLAN and IoT.

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 roaming between ACs. 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.
Authentication modes	Open system authentication with no encryption WEP authentication/encryption WPA/WPA2 authentication and encryption: • WPA/WPA2-PSK+TKIP • WPA/WPA2-PSK+CCMP

Feature	Description
Authentication modes	• 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.
AAA	Local authentication/local accounts (MAC addresses and accounts) RADIUS authentication, LDAP/AD, Multiple authentication servers: • Supports backup authentication servers. • Specifies authentication servers based on the account. • Configures authentication servers based on the account. • Binds user accounts to SSIDs.
Security isolation	Port-based isolation User group-based isolation
Security standards	802.11i, Wi-Fi Protected Access 2 (WPA2), WPA 802.1x Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP), and Extensible Authentication Protocol (EAP) types: • EAP-Transport Layer Security (TLS) • EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) • Protected EAP (PEAP) v0 or EAP-MSCHAPv2 • EAP-Flexible Authentication via Secure Tunneling (FAST) • PEAP v1 or EAP-Generic Token Card (GTC) • EAP-Subscriber Identity Module (SIM)

Feature	Description
WIDS	Rogue 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
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 fair scheduling	Allocates equal time to users for occupying the channel, which improves users' Internet access experience.

Physical Specifications

Feature		Description
Dimensions (height x width x depth)		86.1 mm x 447 mm x 708 mm **Note:** The AC6800V should be installed in a standard IEC cabinet (19-inch).
Maximum power consumption		350 W
Weight		Net weight:21 kg
Operating temperature and altitude		5°C to 45°C (41°F to 113°F) (meeting the ASHRAE CLASS A3 and A4 standards). 900m～3048m：the operating temperature decreases by 1°C (1.8°F) every 300 m (984.24 ft).
Relative humidity		Operating humidity: 8% RH to 90% RH (non-condensing) Storage humidity: 5% to 95% RH (non-condensing) Humidity change rate: < 20% RH/h
Power modules		550W Dual Power Supply, 1+1 Redundant Backup
AC input voltage	Rated voltage	100V AC～240V AC，50/60Hz

Performance Specifications

Performance Specifications

Feature	Description
Number of managed APs	Central APs：1280 Common APs and RUs：10K
Number of access users	100K
Number of SSIDs	80K
Number of VLANs	4K
Number of routing entries	16K
Number of multicast forwarding entries	2K
Number of DHCP IP address pools	256 IP address pools, each of which contains a maximum of 64K IP addresses
Number of local accounts	1000
Number of ACLs	32K
User group management	128 user groups Each user group can reference a maximum of 8 ACLs. A maximum number of ACL rules that can be associated with each user group: 512

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, and 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

Trademark Notice


, HUAWEI, and 
are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, product, service and company names mentioned are the property of their respective owners.

General Disclaimer

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

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

www.huawei.com