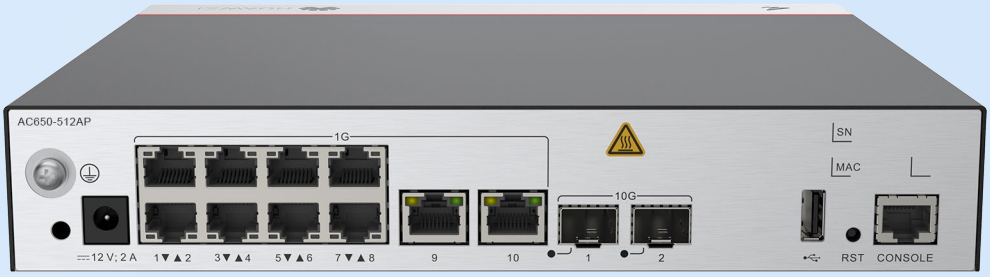
HUAWEI eKit

HUAWEI eKitEngine AC650-512AP Wireless Access Controller Datasheet



Make SME Network Easier and Smarter

HUAWEI

www.huawei.com

Product Overview

The eKitEngine AC650-512AP is a small-capacity box wireless access controller (AC) for small and medium enterprises. It can manage up to 512 access points (APs) and integrates the GE Ethernet switch function, achieving integrated access for wired and wireless users. The WLAN AC features high scalability and offers users considerable flexibility in configuring the number of managed APs. When used with Huawei's full series 802.11ax, 802.11ac,802.11n and 802.11be APs, the eKitEngine AC650-512AP can be used to construct small and medium campus networks, enterprise office networks, wireless Metropolitan Area Networks (MANs), and hotspot coverage networks.

Product Features

Large-capacity and high-performance design

- The eKitEngine AC650-512AP can manage up to 512 APs, meeting requirements of small and medium campuses.
- Provides 2 x 10GE optical interfaces and 10 x GE electrical interfaces, supporting up to 10 Gbit/s forwarding performance.

SmartRadio for air interface optimization

- Load balancing during smart roaming: The load balancing algorithm can work during smart roaming for load balancing detection among APs on the network after STA roaming to adjust the STA load on each AP, improving network stability.
- Intelligent DFA technology: The dynamic frequency assignment (DFA) algorithm is used to automatically detect adjacent-channel and co-channel interference, and identify any 2.4 GHz redundant radio. Through automatic inter-AP negotiation, the redundant radio is automatically switched to another mode (dual-5G AP models support 2.4G-to-5G switchover) or is disabled to reduce 2.4 GHz co-channel interference and increase the system capacity.
- Intelligent conflict optimization technology: The dynamic enhanced distributed channel access (EDCA) and airtime scheduling algorithms are used to schedule the channel occupation time and service priority of each user. This ensures that each user is assigned relatively equal time for using channel resources and user services are scheduled in an orderly manner, improving service processing efficiency and user experience.

Various roles

- The eKitEngine AC650-512AP has a built-in Portal/AAA server and can provide Portal/802.1X authentication for users, reducing customer investment.

Flexible networking

- The WLAN AC can be deployed in inline, bypass, bridge, and Mesh network modes, and supports both centralized and local forwarding.
- The WLAN 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 WLAN AC is deployed on the public network.
- The WLAN AC is compatible with Huawei full-series 802.11n, 802.11ac, 802.11ax and 802.11be APs and supports hybrid networking of 802.11n, 802.11ac, 802.11ax and 802.11be APs for simple scalability.

Built-in application identification server

- Supports Layer 4 to Layer 7 application identification and can identify over 6000 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 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 WLAN 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 WLAN ACs, ensuring service continuity.

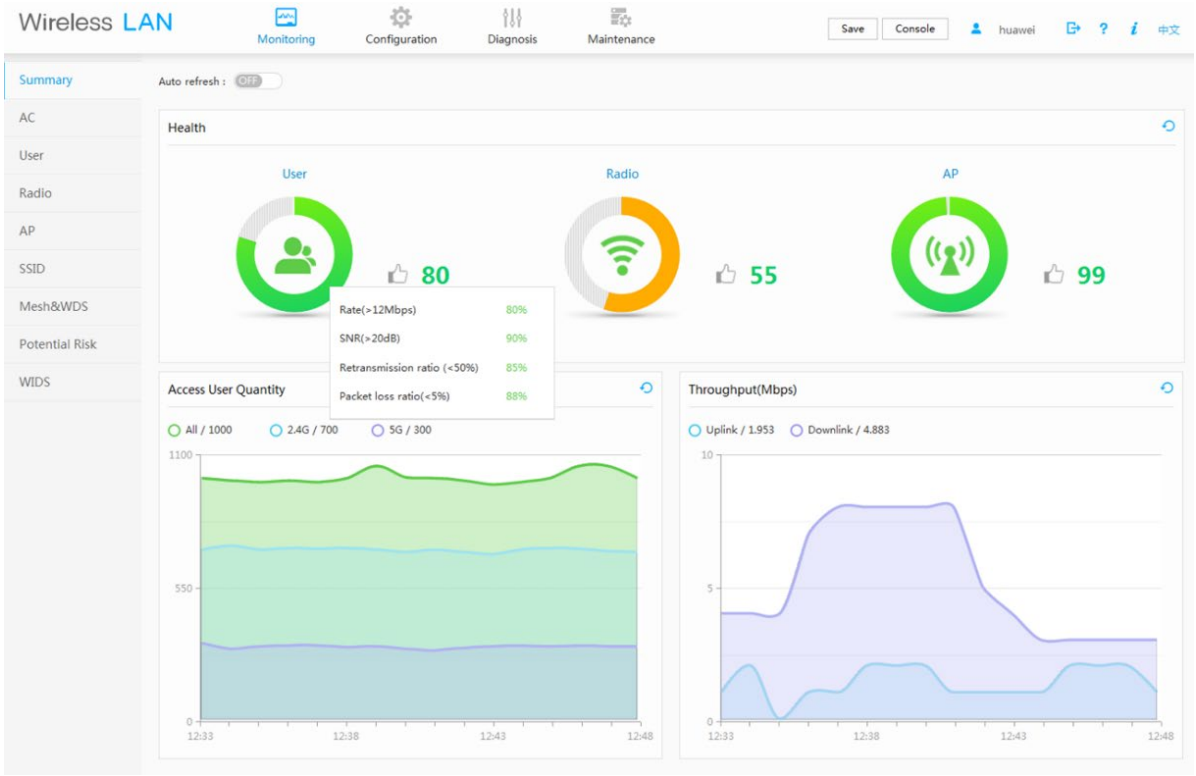
Built-in visualized network management platform

The eKitEngine AC650-512AP 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.

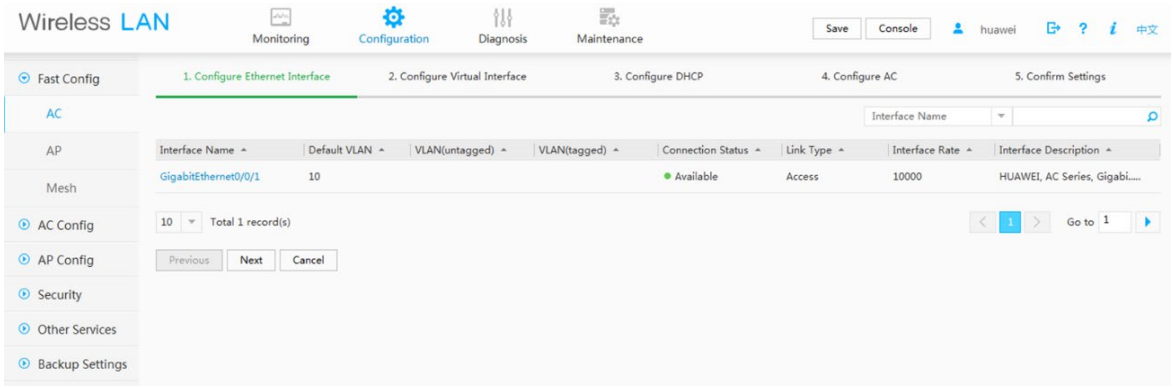
Monitoring interface



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.

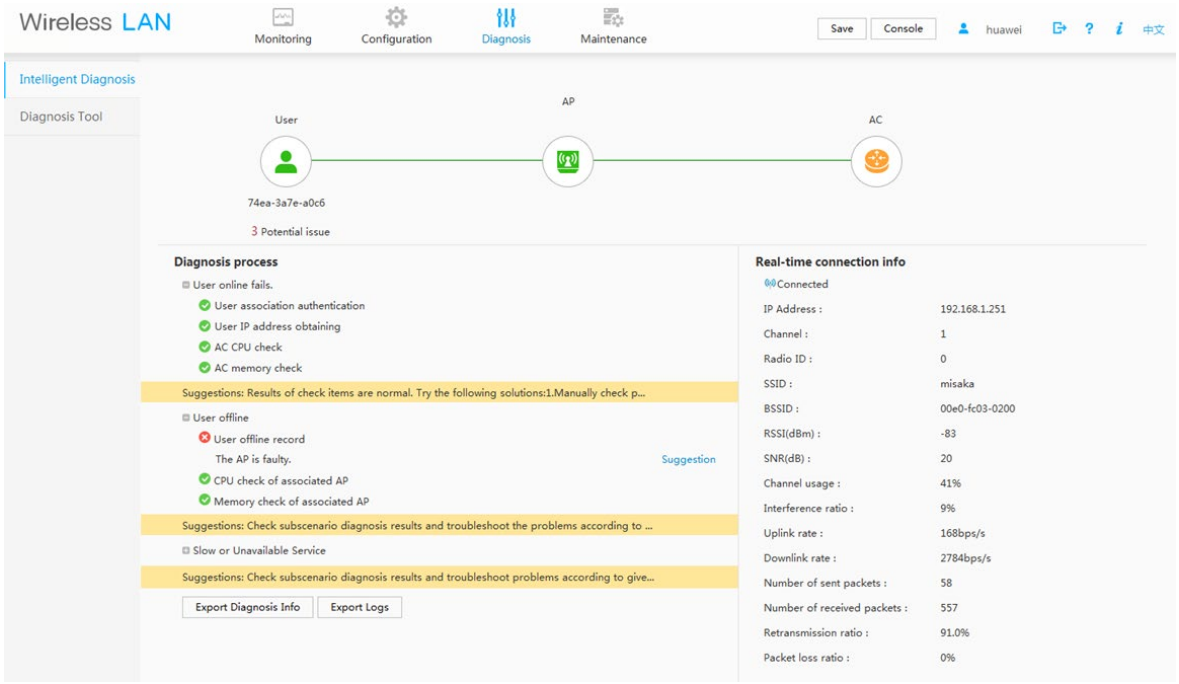
Configuration interface



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 WLAN ACs, and provides feasible suggestions for troubleshooting the faults.

Intelligent diagnosis



eKitEngine AC650-512 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

Feature		Description
		• 802.3az Energy Efficient Ethernet (EEE)
	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 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 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

Feature		Description
		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
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

Feature		Description
		Interface mirroring and flow mirroring
	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 Packet Conservation Algorithm for Internet 2.0 (iPCA 2.0) ,flow detection based on applications, 5-tuple, and flows
	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 WLAN ACs	APs and WLAN ACs can be connected through a Layer 2 or Layer 3 network. APs can be directly connected to a WLAN AC. APs are deployed on a private network, while WLAN ACs are deployed on the public network to implement NAT traversal. WLAN ACs can be used for Layer 2 bridge forwarding or Layer 3 routing. WAN authentication escape is supported between APs and WLAN 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 WLAN 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.

Feature	Description
	Soft GRE forwarding. Tunnel forwarding + EoGRE tunnel
WLAN AC discovery	An AP can obtain the device's IP address in any of the following ways: • Static configuration • DHCP • DNS The WLAN 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 WLAN AC by sending broadcast CAPWAP packets.
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 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 WLAN ACs	Enables and disables the switchback function. Supports load balancing. Supports 1+1 hot backup. **NOTE** *In 1+1 VRRP HSB mode, WLAN ACs share one virtual IP address, simplifying the network topology.* Supports N+1 backup. Supports wireless configuration synchronization between WLAN 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.

Feature	Description
AP group management	The AP group function is used to configure multiple APs in batches. When multiple APs managed by a WLAN AC require the same configurations, you can add these APs to one AP group and configure the AP group to complete AP configuration.
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, 802.11ax, or 802.11be. 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 WLAN 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 WLAN 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	Band steering: Enables terminals to preferentially access the 5G frequency band, achieving load balancing between the 2.4G and 5G frequency bands.

Feature	Description
	Smart roaming: Enables sticky terminals to roam to APs with better signals. • 802.11k and 802.11v smart roaming • 802.11r fast roaming (≤ 50 ms)

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.
Rogue device monitoring	Supports WIDS/WIPS attack detection to monitor, identify, prevent, and take

Feature	Description
	countermeasures against rogue devices and implement refined management and control.
Hotspot2.0	Supports a Hotspot2.0 network.
Navi WLAN AC	Supports remote STA access on the Navi WLAN AC.
Centralized license control	Supports a license server as the centralized AP license control point. Allows a license server to manage license clients. Supports license synchronization between a license server and clients.

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 a WLAN AC.* Supports inter-VLAN Layer 3 roaming on a WLAN AC. Supports roaming between WLAN ACs. Supports fast key negotiation in 802.1X authentication. Authenticates users who request to reassociate with the WLAN 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/WPA3 authentication and encryption: • WPA/WPA2-PSK+TKIP • WPA/WPA2-PSK+CCMP • WPA/WPA2-802.1X+TKIP • WPA/WPA2-802.1X+CCMP • WPA3-802.1X+GCMP512 • WPA/WPA2-PSK+TKIP-CCMP • WPA/WPA2-802.1X+TKIP-CCMP WPA/WPA2-PPSK authentication and encryption WPA3-SAE+CCMP authentication and encryption 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 802.1X authentication: • Authentication through an external 802.1X server. • Built-in 802.1X authentication.
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 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

Feature	Description
	• 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)
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 (H x W x D)	43.6 mm x 250 mm x210 mm
Interface type	2 x 10G (SFP+) + 10 x GE
Maximum power consumption	21 W
Weight	1.47 kg
Operating temperature and altitude	-60 m to +1800 m: 0°C to 45°C 1800 m to 5000 m: Temperature decreases by 1°C every time the altitude increases 220 m.
Relative humidity	5% RH to 95% RH, noncondensing
Power modules	AC/DC adapter

Performance Specifications

Feature	Description
Number of managed APs	512 **NOTE** *The RUs managed by the WLAN AC do not occupy the AC's license resources. However, the total number of managed common APs and RUs cannot exceed the upper limit allowed by the AC.*
Number of access users	4096 **NOTE** *The maximum number of access users varies depending on the authentication mode.*
Number of MAC address entries	8192
Forwarding capability	10 Gbit/s **NOTE** • *The value is the maximum forwarding capability supported by the device. The actual performance varies with the enabled functions of the device and the network environment. For details, see the product specifications.* • *Packet length: 1514 bytes.*
Number of VLANs	4096
Number of routing entries	• IPv4: 8192 • IPv6: 2048
Number of ARP entries	6144
Number of multicast forwarding entries	2048
Number of DHCP IP address pools	64 IP address pools, each of which contains a maximum of 8192 IP addresses
Number of local accounts	1000
Number of ACLs	4096

Standards compliance

Item	Description
Safety standards	IEC60950-1 UL60950-1 CSA C22.2#60950-1 EN60950-1 AS/NZS 60950.1 GB 4943
EMC standards	FCC Part15B ETSI EN 300 386 IEC61000-4-11 IEC 61000-4-4 IEC61000-4-2 IEC61000-4-3 IEC61000-4-5 IEC61000-4-6 IEC 61000-3-2 IEC 61000-3-3 AS/NZS CISPR 32 EN55032/EN55024 ICES-003 GB9254
RoHS	Directive 2002/95/EC & 2011/65/EU
Reach	Regulation 1907/2006/EC
WEEE	Directive 2002/96/EC & 2012/19/EU

More Information

For more information about Huawei WLAN products, visit http://e.huawei.com or contact us in the following ways:

- Global service hotline: http://e.huawei.com/en/service-hotline
- Logging in to the Huawei Enterprise technical support web: http://support.huawei.com/enterprise/
- Sending an email to the customer service mailbox: support_e@huawei.com

Huawei Technologies Co., Ltd.

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

Website:www.huawei.com