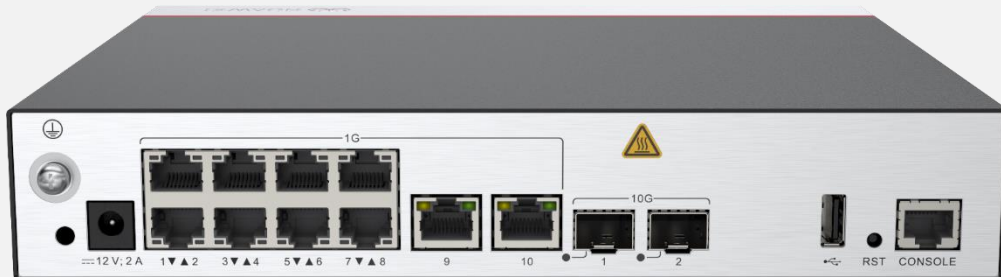


Huawei AC650-128AP Wireless Access Controller Datasheet



Large-capacity
Manages 128 APs for free



Super speed
forwarding performance:10Gbps
Interfaces:2*10GE SFP, 10*GE

The AC650-128AP is a small-capacity box wireless access controller (WAC) for small office home office (SOHO) enterprises. It can manage up to 128 access points (APs) and integrates the GE Ethernet switch function, achieving integrated access for wired and wireless users. Also, the AC650-128AP features high scalability and offers users considerable flexibility in configuring the number of managed APs. With these strengths, this WAC can be used to construct small and medium campus networks, enterprise office networks, wireless metropolitan area networks (MANs), and hotspot coverage networks

Feature Descriptions

Large-capacity and high-performance design

- Manages up to 128 APs, meeting requirements of SOHO campuses.
- Provides 2 x 10GE optical interfaces and 10 x GE electrical interfaces, supporting up to 10 Gbps forwarding performance.

SmartRadio for AP air interface optimization

- Load balancing during smart roaming: The load balancing algorithm enables load balancing detection between APs on the network after STA roaming to adjust the STA load on each AP, improving network stability.
- Intelligent dynamic frequency assignment (DFA) technology: The DFA algorithm is used to automatically detect adjacent-channel and co-channel interference, and identify any redundant 2.4 GHz radios. Through automatic inter-AP negotiation, a 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: 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 a relatively equal amount of time for using channel resources and user services are scheduled in an orderly manner, improving service processing efficiency and user experience.

Various roles

- The WAC has a built-in Portal/AAA server and can provide Portal/802.1X authentication for users, protecting customer investment.

Flexible networking

- The WAC can be deployed in in-path, off-path, bridge, or mesh network mode, and supports both centralized and local forwarding modes.
- The WAC and APs can be connected across a Layer 2 or Layer 3 network. In addition, network address translation (NAT) can be deployed when APs are deployed on the private network and the WAC is deployed on the public network.
- The WAC is compatible with Huawei's 802.11n, 802.11ac and 802.11ax APs and supports the hybrid networking of 802.11n, 802.11ac and 802.11ax 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 limiting, and priority adjustment policies.
- Supports automatic application expansion in the application signature database, without the need of a software upgrade.

Comprehensive reliability design

- Supports WAC 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 WACs. In local forwarding mode, this feature keeps existing STAs online and allows for the access of new STAs when APs are disconnected from WACs, ensuring service continuity.

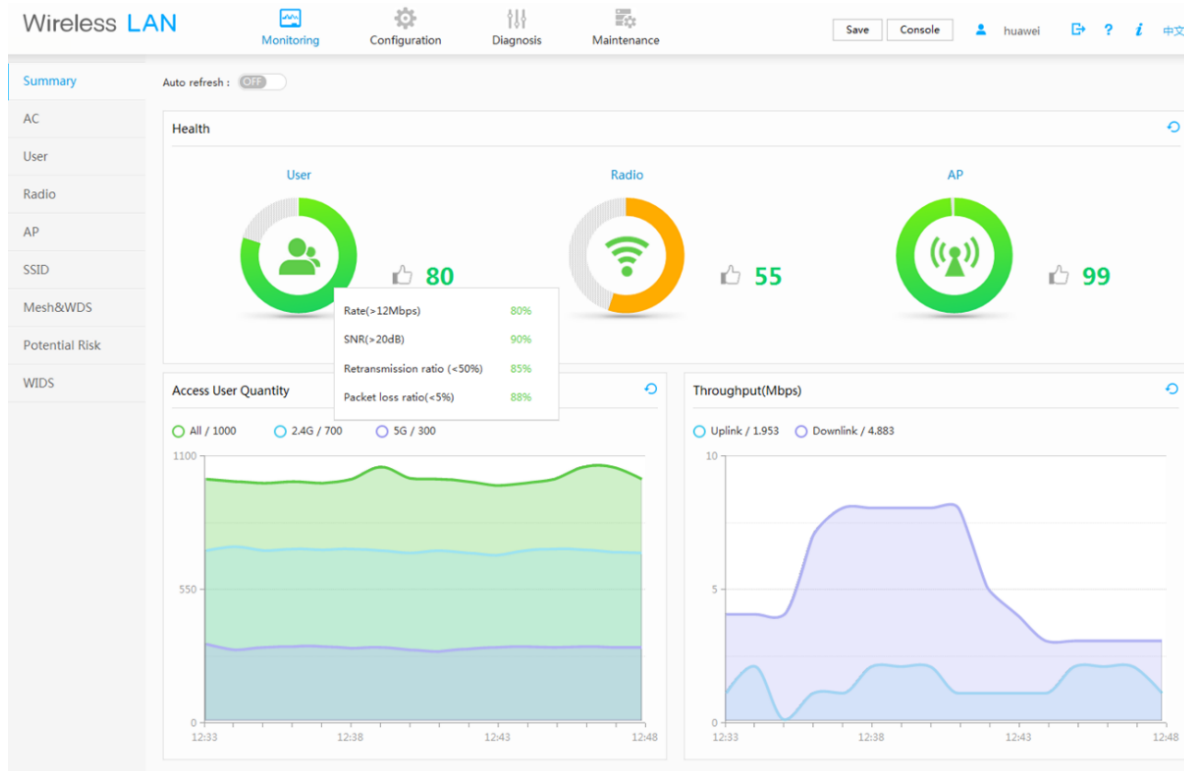
Built-in visualized network management platform

- The AC650-128AP 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 on graphs, including user, radio and AP performance, enabling users to extract useful information from the massive amount of data, while also being instantly aware of the device and network status.

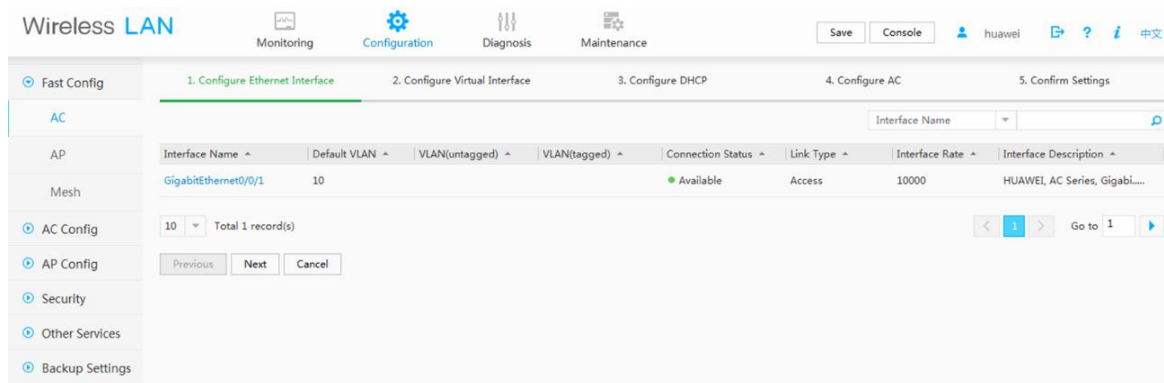
Monitoring web page



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

- The web system supports AP group-centric configuration and automatically selects common parameters for users, simplifying configuration.
- 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 need only modify the original configurations rather than creating entirely new ones each time.

Configuration web page



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 WACs, and provides feasible suggestions for troubleshooting.

Diagnosis web page

The screenshot displays the 'Intelligent Diagnosis' interface. At the top, there are navigation tabs: Monitoring, Configuration, Diagnosis (selected), and Maintenance. Below these are utility buttons: Save, Console, and user information (huawei). The main content area shows a network topology diagram with three nodes: User (74ea-3a7e-a0c6), AP, and AC. The 'Diagnosis process' section is expanded to show 'User offline' with a red error icon. It lists several checks: 'User association authentication', 'User IP address obtaining', 'AC CPU check', and 'AC memory check', all of which are marked as successful with green checkmarks. A suggestion box indicates that the results are normal and suggests manual checks. Another section shows 'User offline' with a red error icon, stating 'The AP is faulty' and suggesting a CPU and memory check of the associated AP. The 'Real-time connection info' section provides detailed statistics: Connected status, IP Address (192.168.1.251), Channel (1), Radio ID (0), SSID (misaka), BSSID (00e0-fc03-0200), RSSI (-83 dBm), SNR (20 dB), Channel usage (41%), Interference ratio (9%), Uplink rate (168 bps/s), Downlink rate (2784 bps/s), Number of sent packets (58), Number of received packets (557), Retransmission ratio (91.0%), and Packet loss ratio (0%).

Basic Specifications

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 Mbps, 100 Mbps, 1000 Mbps, and auto-negotiation <ul style="list-style-type: none"> • 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

Feature		Description
Ethernet loop protection	MSTP	STP RSTP MSTP BPDU protection, root protection, and loop protection Partitioned STP
IPv4 forwarding	IPv4 features	ARP and RARP Proxy ARP 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 DHCPv6 DHCPv6 snooping
	Multicast routing features	MLD MLD snooping
Device reliability	BFD	BFD
Layer 2 multicast features	Layer 2 multicast features	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 of 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
	Version upgrade	Device software loading and online software loading BIOS online upgrade In-service patching
Network management	Network management	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

Feature		Description
		flood, and Ping of Death attacks IPsec URL filtering Antivirus Intrusion prevention
	Network management	ICMP-based ping and traceroute SNMPv1, SNMPv2c, and SNMPv3 Standard MIB RMON NetStream

Wireless networking capabilities

Feature	Description
Networking between APs and WACs	APs and WACs can be connected through a Layer 2 or Layer 3 network. APs can be directly connected to a WAC. APs are deployed on a private network, while WACs are deployed on the public network to implement NAT traversal. WACs can be used for Layer 2 bridge forwarding or Layer 3 routing. WAN authentication escape is supported between APs and WACs. In local forwarding mode, this feature retains the online state of existing STAs and allows access of new STAs when APs are disconnected from WACs, 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
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 Zero-configuration provisioning (ZTP) Mesh network with multiple MPPs Vehicle-ground fast link handover Mesh client mode
WAC discovery	An AP can obtain the WAC's IP address in any of the following ways: <ul style="list-style-type: none"> • Static configuration • DHCP • DNS

Feature	Description
	<p>The WAC uses DHCP or DHCPv6 to allocate IP addresses to APs.</p> <p>DHCP or DHCPv6 relay is supported.</p> <p>On a Layer 2 network, APs can discover a WAC by sending broadcast CAPWAP packets.</p>
CAPWAP tunnel	<p>Centralized CAPWAP</p> <p>CAPWAP control tunnel and (optional) data tunnel</p> <p>CAPWAP tunnel forwarding and direct forwarding in an extended service set (ESS)</p> <p>Datagram Transport Layer Security (DTLS) encryption, which is enabled by default for the CAPWAP control tunnel</p> <p>Heartbeat detection and tunnel reconnection</p>
Active and standby WACs	<p>Enables and disables the switchback function.</p> <p>Supports load balancing.</p> <p>Supports 1+1 HSB.</p> <p>NOTE</p> <p><i>In 1+1 VRRP HSB mode, WACs share one virtual IP address, simplifying the network topology.</i></p> <p>Supports N+1 backup.</p> <p>Supports wireless configuration synchronization between WACs.</p> <p>Supports license sharing between WACs</p>

AP management

Feature	Description
AP access control	<p>Displays MAC addresses or SNs of APs in the whitelist.</p> <p>Adds a single AP or multiple APs (by specifying a range of MAC addresses or SNs) to the whitelist.</p> <p>Automatically discovers and manually confirms APs.</p> <p>Automatically discovers APs without manually confirming them.</p>
AP region management	<p>Supports three AP region deployment modes:</p> <ul style="list-style-type: none"> • 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. <p>Specifies the default region to which automatically discovered APs are to be added.</p>
AP profile management	<p>Specifies the default AP profile that is applied to automatically discovered APs.</p>
AP type management	<p>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 some APs deployed indoors).</p> <p>Provides built-in default AP types.</p>
Network topology management	<p>Supports LLDP topology detection.</p>
AP working mode management	<p>Supports AP working mode switchover. The AP working mode can be switched to the Fat or cloud mode on the WAC.</p>

Radio management

Feature	Description
Radio profile management	<p>Supports the following parameter settings in a radio profile:</p> <ul style="list-style-type: none"> • Radio working mode and rate • Automatic or manual channel and power adjustment mode • Radio calibration interval • Radio type, which 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, or 802.11ax <p>Allows you to bind a radio to a specified radio profile.</p> <p>Supports MU-MIMO.</p>
Unified static configuration of parameters	Configures radio parameters such as the channel and power of each radio on the WAC and delivers the configurations to APs.
Dynamic management	<p>APs can automatically select working channels and power when they go online.</p> <p>In an AP region, APs automatically adjust working channels and power in the event of signal interference:</p> <ul style="list-style-type: none"> • 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. • The DFA function automatically identifies, switches, or disables redundant radios, reducing 2.4 GHz co-channel interference and increasing system capacity. <p>When an AP is removed or goes offline, the WAC increases the power of neighboring APs to compensate for the coverage hole.</p> <p>Automatic selection and calibration of radio parameters in AP regions are supported.</p>
Enhanced service capabilities	<p>Band steering: enables terminals to preferentially access the 5 GHz frequency band, achieving load balancing between the 2.4 GHz and 5 GHz frequency bands.</p> <p>Smart roaming: enables sticky terminals to roam to APs with better signals.</p> <ul style="list-style-type: none"> • 802.11k and 802.11v smart roaming • 802.11r fast roaming (≤ 50 ms)

WLAN service management

Feature	Description
ESS management	<p>Allows you to enable SSID broadcast, set the maximum number of access users, and set the association aging time in an ESS.</p> <p>Isolates APs at Layer 2 in an ESS.</p> <p>Maps an ESS to a service VLAN.</p> <p>Associates an ESS with a security profile or a QoS profile.</p> <p>Enables IGMP for APs in an ESS.</p> <p>Supports Chinese SSIDs.</p>
VAP-based service management	<p>Adds multiple VAPs at a time by binding radios to ESSs.</p> <p>Displays information about a single VAP, VAPs with a specified ESS, or all VAPs.</p> <p>Supports configuration of offline APs.</p> <p>Creates VAPs according to batch delivered service provisioning rules in automatic AP discovery mode.</p>

Feature	Description
Automatic 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 can be pre-configured. 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: <ul style="list-style-type: none"> • 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.
Navi WAC	Supports remote STA access on the Navi WAC.
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: <ul style="list-style-type: none"> • Based on APs • Based on SSIDs Logs out users in any of the following ways: <ul style="list-style-type: none"> • Using RADIUS DM messages • Using commands Supports various methods to view information:

Feature	Description
	<ul style="list-style-type: none"> Allows you to view the user status based on the user MAC address, AP ID, radio ID, or WLAN ID. Displays the number of online users by ESS, AP, or radio. Collects STA-based packet statistics on the air interface.
WLAN user roaming	<p>Supports intra-AC Layer 2 roaming.</p> <p>NOTE <i>Users can roam between APs connected to different physical ports on a WAC.</i></p> <p>Supports inter-VLAN Layer 3 roaming on a WAC.</p> <p>Supports roaming between WACs.</p> <p>Supports fast key negotiation in 802.1X authentication.</p> <p>Authenticates users who request to reassociate with the WAC and rejects the requests of unauthorized users.</p> <p>Delays clearing user information after a user goes offline so that the user can rapidly go online again.</p>
User group management	<p>Supports ACLs.</p> <p>Supports user isolation:</p> <ul style="list-style-type: none"> Inter-group isolation Intra-group isolation

WLAN security

Feature	Description
WLAN security profile management	<p>Manages authentication and encryption modes using WLAN security profiles.</p> <p>Binds security profiles to ESS profiles.</p>
Authentication modes	<p>Open system authentication with no encryption</p> <p>WEP authentication/encryption</p> <p>WPA/WPA2 authentication and encryption:</p> <ul style="list-style-type: none"> WPA/WPA2-PSK+TKIP WPA/WPA2-PSK+CCMP WPA/WPA2-802.1X+TKIP WPA/WPA2-802.1X+CCMP WPA/WPA2-802.1X+ CCMP WPA/WPA2-PSK+TKIP-CCMP WPA/WPA2-802.1X+TKIP-CCMP <p>WPA/WPA2-PPSK authentication and encryption</p> <p>WAPI authentication and encryption:</p> <ul style="list-style-type: none"> 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. <p>Allows users to use MAC addresses as accounts for authentication by the RADIUS server.</p> <p>Portal authentication:</p> <ul style="list-style-type: none"> Authentication through an external Portal server Built-in Portal authentication and authentication page customization <p>802.1X authentication:</p>

Feature	Description
	<ul style="list-style-type: none"> • Authentication through an external 802.1X server. • Built-in 802.1X authentication.
Combined authentication	Combined MAC authentication: <ul style="list-style-type: none"> • PSK+MAC authentication MAC+Portal authentication: <ul style="list-style-type: none"> • MAC address-prioritized Portal authentication
AAA	Local authentication/local accounts (MAC addresses and accounts) RADIUS authentication Multiple authentication servers: <ul style="list-style-type: none"> • 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
WIDS	Rogue device scan, identification, defense, and containment, which includes dynamic blacklist configuration and detection of rogue APs, STAs, and network attacks.
Authority control	ACL limit based on the following: <ul style="list-style-type: none"> • 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.

Feature	Description
	Sets the QoS priority for CAPWAP data channels: <ul style="list-style-type: none"> • 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

Item	Description
Dimensions (H x W x D)	43.6 mm x 210 mm x 250 mm
Interface type	2 x 10GE optical ports +10 x GE electrical ports 1 x Console (RJ45), 1 x USB
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

Technical Specifications

Performance specifications

Item	Description
Number of managed APs	128
Number of access users	1024 NOTE <i>The maximum number of access users varies depending on the authentication mode.</i>
Number of MAC address entries	8192
Forwarding capability	10 Gbps
Number of VLANs	4096
Number of routing entries	<ul style="list-style-type: none"> • IPv4: 4096 • IPv4: 2048
Number of ARP entries	4096
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	1024

Item	Description
Number of ACLs	4096

Ordering Information

Product Model	Description
AC650-128AP	AC650-128AP (10*10/100/1000BASE-T ports, 2*10GE SFP+ port, AC/DC power)

More Information

For more information about Huawei WLAN products, visit <http://e.huawei.com> or contact the local Huawei sales office. Alternatively, you can 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

Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: www.huawei.com