H3C New Generation

Access Controller Modules

Release Date: October, 2019

New H3C Technologies Co., Limited

H3C New Generation Access Controller Modules

Overview

H3C new-generation access controller modules (referred to as ACs in this document) are high-performance, service-rich modules for wireless networking. They provide outstanding services for WLAN access in large and medium-sized campuses, wireless coverage in MAN, Wi-Fi hotspot coverage, and branch deployment. They can work seamlessly with the S10500X switch hardware and software to deliver an ideal wired and wireless unified solution.

S10500X 20G access controller module

S10500X 40G access controller module

Features and benefits

Management of all H3C Aps

In addition to 802.11a/b/g/n/ac APs, the module can also set up networks with 802.11ac Wave2 and 802.11ax APs. This overcomes the limitation of the traditional wireless serial communication mechanism, exponentially increases the wireless spectrum usage, and significantly improves user experience in high-density access scenarios and increases user access number.

Cutting-edge operating system

The module runs the H3C's state-of-the-art Comware V7 network operating system. This system greatly improves product performance and can keep up with the increasingly complicated enterprise network applications. This system offers the following advantages:

- Multi-core control—Comware V7 can adjust the ratio of the control cores to forwarding cores in the CPU as demanded to achieve an optimal balance, remarkably improving the CPU control capabilities and computing capabilities while providing strong concurrent computing capabilities.
- User-mode multitasking—In Comware V7, most network applications run in user mode. When you start an application, the system creates a task for the application and provides the task with private resources. If a task error occurs, the error is limited to this task and does not affect other applications and the operating system.
- User-mode task monitoring—Comware V7 monitors each task running in user mode. When a task error occurs, the system will reload the task to ensure quick recovery of the application.
- Independent application upgrade—Comware V7 can upgrade a single module independently instead of the whole system, which enhances upgrade security and network stability significantly.

IRF fabric in start topology

The module supports the H3C Intelligent Resilient Framework (IRF) technology that can virtualize multiple modules into a logical module called an IRF fabric, which provides the following benefits:

- **Simplified topology**—You can set up an IRF fabric simply by connecting the ACs through a switch. No dedicated cable or port is required.
- **Simplified configuration**—The configuration on the IRF fabric (master AC) will be automatically synchronized to the member ACs.
- **1+1 redundancy**—Failure of one AC does not affect the operation of the IRF fabric.
- **Flexible license control**—The ACs in the IRF fabric in star topology share their licenses.

AC hierarchy architecture

AC hierarchy architecture is a brand new networking model engineered by H3C to cater for the need of hierarchy network construction in the market. An AC hierarchy network contains a central AC, local ACs, and APs. The central AC manages all local ACs, and local ACs connect APs to the network and provide traffic forwarding.

- The central AC typically has a high processing capacity and is deployed at the distribution layer. It focuses on performing global services such as network management and control and centralized authentication. It can also connect APs to the network and provide traffic forwarding.
- The local ACs can be medium- or low-end ACs, all-in-one ACs (with routing and DPI features), or unified wired and wireless switches.

AC hierarchy architecture can be used for large-scale wireless network deployment and is well suited for headquarters and branch network deployments. The link bandwidth at the core layer and forwarding capacity of the central AC are no longer the bottleneck. Through centralized management on the central AC, this architecture enables automatic and convenient version upgrade and configuration synchronization of local ACs and APs. The local ACs control client roaming between APs, significantly improving roaming performance.

CUPID location

The AC module supports CUPID location, which is similar to radar probing and provides high positioning accuracy. It enables an AP to proactively send a probe packet to a client and locate the client by calculating the time difference between the probe and response packets.

Flexible forwarding modes

The module supports centralized forwarding, distributed forwarding, and policy-based forwarding, and users can choose the forwarding mode flexibly according to service requirements and network conditions.

The module also supports local forwarding in conjunction with centralized authentication. It can perform 802.1X and Portal authentications for data streams that are forwarded locally.

Carrier-class wireless access control and management

The module supports the following access control methods:

- User profile-based access behavior control

A user profile is a configuration template that saves predefined configurations such as Committed Access Rate (CAR) and QoS policies. When a user passes authentication, the AC applies the parameters in the user profile to the user to restrict the user behavior. When the user logs out, the AC automatically disables the user profile parameters.

- MAC authentication access control

MAC authentication allows you to configure and modify the access rights of a group of clients or a particular client on the AAA server. The refined access control method enhances the availability of WLANs and facilitates access right assignment.

- MAC-based VLAN access control

The administrator can assign users (or MAC addresses) with the same attributes to the same VLAN and configure a VLAN-based security policy on the AC. This simplifies system configuration and refines user management to the per-user granularity.

- AP-based access control.

The AC gets a list of permitted APs from the authentication server during client authentication, and then selects an optimal AP for the client. This allows you to control the APs that wireless clients can associate for security or accounting purposes.

Dynamic frequency selection (DFS)

In a WLAN, adjacent APs must work in non-overlapping channels to avoid channel interference. However, the non-overlapping channels in a WLAN are limited. For example, the 2.4 GHz band has only three non-overlapping channels. Meanwhile, there are many possible interference sources such as radars and microwave ovens that can affect the operation of APs in a WLAN.

DFS can ensure that each AP operates in the optimal channel, thereby minimizing adjacent channel interference. In addition, the real-time interference detection function can help keep APs away from interference sources.

Intelligent AP load balancing

In a WLAN, clients prefer to associate with an AP that has a higher RSSI. As a result, a large number of clients might associate with the same AP because it has stronger signal strength. Because these clients share the wireless media, the throughput for each client will be reduced.

The module provides session-based load balancing and traffic-based load balancing. It analyzes AP loads, determines which APs can balance loads for each other, and dynamically adjusts loads among APs to ensure adequate bandwidth for clients.

Wireless intrusion detection and prevention system (WIDS/WIPS)

The module provides the following WIDS/WIPS features: blacklist, whitelist, rogue detection, malformed packet detection, illegal client logoff, and MAC layer attack detection and countermeasures through predefined signatures. MAC layer attacks include DDoS attacks, flood attacks, and man-in-the-middle attacks.

For an identified attack source, such as an AP or terminal, the AC can visually track and monitor physical locations of the attacker and shut down the physical port on the switch.

Cooperating with H3C professional core-layer firewall/IPS devices, the AC can achieve complete security protection from Layer 1 through Layer 7, fulfilling the end-to-end security requirements of both 802.11 and 802.3 standards.

802.1X, MAC, and portal authentications

The module supports the following authentication methods:

- 802.1X authentication—The module supports local and remote 802.1X authentication and multiple 802.1X authentication methods, such as TLS, PEAP, TTLS, MD5, and SIM card. In local authentication mode, the AC acts as the authentication server and no additional AAA server is required. The module also supports dynamic VLAN assignment and ACL through predefined user profiles.

- MAC authentication—The module supports MAC address authentication to authenticate hand-held terminals such as Wi-Fi phones and hand-held mobile terminals. On the module or AAA server, you can specify MAC addresses allowed to access a WLAN. MAC addresses not specified are identified as illegal and cannot access the WLAN. This authentication method is widely used in the wireless healthcare system.

- Portal authentication—The module provides an embedded portal server. This authentication method allows users to initiate authentication through a Web browser without installing client software. After a client passes authentication, the AC redirects the client to the specified website and simultaneously starts authorization and accounting. Customized portal pages can also be pushed to the clients for advertisement and message delivery. This is widely used for guest access in various scenarios like wireless campus, hotel, and commercial chain stores.

IPv4/IPv6 dual stack (Native IPv6)

The module supports both IPv4 and IPv6 client accesses. When the AC is deployed on an IPv4 network, APs connected to the AC can identify IPv6 packets and map IPv6 priorities to the tunnel priority. After receiving packets sent from APs, the AC can also use ACLs to control and filter IPv6 packets. When the AC is deployed on an IPv6 network, it will automatically negotiate with APs and establish an IPv6 tunnel with each AP and can still correctly identify and process IPv4 packets from wireless clients.

Excellent IPv4/IPv6 adaptability enables the module to provide services to various complicated applications during migration from IPv4 to IPv6.

The module also supports IPv6 Source Address Validation (SAVI) to address emerging IPv6 forged packet attacks on campus networks. Through address allocation protocol snooping, the AC obtains clients' IP addresses and ensures that clients use the correct address when they come online, eradicating the possibility of IP address forging and guaranteeing the reliability of source IP addresses. IPv6 SAVI in conjunction with portal authentication further guarantees the integrity and security of network packets.

End-to-end QoS

Developed based on the H3C's cutting-edge Comware V7 operating system, the module supports the QoS Diff-Serv model perfectly. It also supports IPv6 QoS.

The QoS Diff-Serv model mainly includes traffic classification, traffic policing, queue management, and queue scheduling, completely supporting the six kinds of PHB services: EF, AF1 through AF4, and BE. This enables service providers to provide services with different qualities to clients, making the Internet a truly integrated network carrying data, voice, and video services at the same time.

Fast Layer 2 and Layer 3 roaming

The module improves both Layer 2 and Layer 3 roaming performance significantly and enables inter-subnet roaming. This benefit greatly simplifies early wireless network planning and reduces network planning costs.

The module uses key caching to implement fast roaming of clients. The key caching function allows clients to fast roam from one AP to another without performing the complete 802.1X authentication process while ensuring user identification and the continuity of keys. With fast roaming, an intra-AC roaming will take no more than 50ms, which ensures transmission of speed-demanding voice traffic.

Remote access for branches

The module can be deployed to implement the following features for remote branch access:

- Performance improvement of services such as printer access and terminal communication in branch LANs by choosing centralized forwarding mode or local forwarding mode.
- Client access to local resources in case of WAN or AC failure and the AC escape function.
- Communication between an AC and APs in a private network through NAT.

Technical specifications

Hardware specifications

Item	LSUM1WCMX20RT (20G AC module) LSUM1WCMX40RT (40G AC module)
Applicable device	H3C S10500X switch series
Dimensions (H × W × D)	40 × 399 × 355 mm (1.57 × 15.71 × 13.98 in)
Weight	3.8 kg (8.38 lb)
Management port	1 × console port 1 × out-of-band management (OOBM) GE port
Power consumption	< 180 W
Temperature	Operating temperature: 0°C to 45°C (32°F to 113°F) Storage temperature: –40°C to +70°C (–40°F to +158°F)
Relative humidity (non-condensing)	Operating and storage humidity: 5% to 95%
Safety standard	UL 60950-1 CAN/CSA C22.2 No 60950-1 IEC 60950-1 EN 60950-1/A11 AS/NZS 60950 EN 60825-1 EN 60825-2 FDA 21 CFR Subchapter J
EMC standards	ETSI EN 300 386 V1.3.3:2005 EN 55024: 1998+ A1: 2001 + A2: 2003 EN 55022 :2006 VCCI V-3:2007 ICES-003:2004 EN 61000-3-2:2000+A1:2001+A2:2005 EN 61000-3-3:1995+A1:2001+A2:2005 AS/NZS CISPR 22:2004 FCC PART 15:2005 GB 9254:1998 GB/T 17618:1998
MTBF	≥ 55.6 years

Software specifications

Item		LSUM1WCMX20RT	LSUM1WCMX40RT
Basic capabilities	Supported APs without a license	0	
	License type	1/4/8/16/32/64/128/512/1024	
	Max number of manageable APs	1024	4096
	Max number of configurable APs	4096	16384
	Max number of SSIDs	1024	4096
	Forwarding capacity	20 Gbps	40 Gbps
802.11 MAC	802.11 protocol suite	Supported	
	Hide SSID	Supported	
	802.11g protection	Supported	
	802.11n only	Supported	
	Client quantity limit	SSID-based client quantity limit Radio-based client quantity limit	
	Online client detection	Supported	
	Automatic client aging	Supported	
	Multi-country code	Supported	
	User isolation	VLAN-based user isolation SSID-based user isolation	
	20 MHz/40 MHz auto-switch in 40 MHz mode	Supported	
CAPWAP	Local forwarding	Local forwarding based on SSID+VLAN	
	Auto AP	Supported	
	AC discovery (DHCP option 43 and DNS)	Supported	
	IPv6 tunnel	Supported	
	Network synchronization	Supported	
	Jumbo frame forwarding	Supported	
	AP preprovisioning	AP basic network settings such as static IP, VLAN, and AC's IP address	
	NAT traversal between AP and AC	Supported	
Roaming	Intra-AC Layer 2 and Layer 3 roaming	Supported	
	Inter-AC Layer 2 and Layer 3 roaming	Supported	

Item		LSUM1WCMX20RT	LSUM1WCMX40RT
Access control	Open system, shared key authentication	Supported	
	WEP-64/128, dynamic WEP	Supported	
	WPA, WPA2	Supported	
	TKIP	Supported	
	CCMP	Supported (11n recommended)	
	SSHv1.5/v2.0	Supported	
	Wireless End-point Access Domination (EAD)	Supported	
	Portal authentication	Supported, remote or external server	
	Portal webpage redirection	SSID-based portal webpage redirection AP-based portal webpage redirection	
	Portal by-pass proxy	Supported	
	802.1X authentication	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5, EAP-SIM, LEAP, EAP-FAST, EAP offload (TLS, PEAP only)	
	Local authentication	802.1X authentication, portal authentication, MAC authentication	
	LDAP authentication	802.1X and portal access 802.1X EAP-GTC and EAP-TLS	
	AP-based access control	Supported	
	Guest access control	Supported	
	VIP tunnel	Supported	
	ARP anti-attack	Wireless SAVI	
	SSID anti-spoofing	Username and SSID binding	
	Domain- and SSID-based AAA server selection	Supported	
	AAA server backup	Supported	
	Local AAA server for wireless clients	Supported	
	TACACS+	Supported	
QoS	Priority mapping	Supported	
	Layer 2 to Layer 4 traffic classification	Supported	
	Rate limit	Granularity of 8 Kbps	
	802.11e/WMM	Supported	
	User profile-based access control	Supported	

Item		LSUM1WCMX20RT	LSUM1WCMX40RT
	Intelligent bandwidth limit (equal bandwidth share algorithm)	Supported	
	Intelligent bandwidth limit (user specific)	Supported	
	Intelligent bandwidth guarantee	Free flow for packets coming from every SSID when traffic is not congested, and minimum bandwidth specified for each SSID when traffic is congested	
	QoS optimization for SVP phone	Supported	
	Call Admission Control (CAC)	CAC based on client quantity or bandwidth	
	End-to-end QoS	Supported	
	AP uplink rate limit	Supported	
WLAN resource management	Country code lock	Supported	
	Dynamic frequency selection (DFC) and transmit power control (TPC)	Supported	
	Dynamic transmit rate control	Supported	
	Coverage hole detection and correction	Supported	
	Load balancing mode	Traffic-based load balancing Session-based load balancing Radio group based load balancing (dual-band supported)	
	Intelligent load balancing	Supported	
	AP load balancing group	Auto-discovery and flexible setting	
Security	Static blacklist	Supported	
	Dynamic blacklist	Supported	
	Whitelist	Supported	
Others	Bonjour gateway	Supported	
	Hotspot 2.0	Supported	
	AC hierarchy	Central AC	
	HA	IRF, license sharing, AC dual-link backup	
	Third-party application	Facebook authentication, WeChat authentication	

Ordering information

Product ID	Product Description
LSUM1WCMX40RT	H3C S10500 40G Access Controller Module
LSUM1WCMX20RT	H3C S10500 20G Access Controller Module

The Leader in Digital Solutions

New H3C Technologies Co., Limited

Beijing Headquarters
Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang District, Beijing, China
Zip: 100102
Hangzhou Headquarters
No.466 Changhe Road, Binjiang District, Hangzhou, Zhejiang, China
Zip: 310052
Tel: +86-571-86760000

Disclaimer: Though H3C strives to provide accurate information in this document, we cannot guarantee that details do not contain any technical error or printing error. Therefore, H3C cannot accept responsibility for any inaccuracy in this document. H3C reserves the right for the modification of the contents herein without prior notification

http://www.h3c.com