

H3C WX2520X-LI Next-Generation Enterprise-Class Gateway Wireless Controller

Product Overview

The H3C WX2520X-LI is a gateway-type wireless access controller (AC) independently developed by H3C Technologies Co., Ltd. (hereinafter referred to as H3C).

The WX2520X-LI wireless controller has rich service types, integrating fine user control management, comprehensive radio frequency resource management, 7X24 hour wireless security control, and Layer 2 and Layer 3 fast roaming.

It integrates multiple functions such as mobile browsing, flexible QoS control, IPv4&IPv6 dual stack, etc.

The H3C WX2520X-LI wireless controller is designed specifically for branch offices and small campus wireless network requirements. It integrates gateway and AC functions and works with H3C Fit AP products.

The series supports functions such as WIPS and firewall, making it a versatile tool for enterprise networking. It also has a rich variety of port types, especially the built-in USB interface, which can connect to relevant enterprise peripherals.

Overall, it reduces the types and quantities of equipment that enterprises need to purchase when building networks, helping enterprises save investment.

*H3C WX2520X-LI wireless controller works with H3C Fit AP product series to meet the needs of wireless scenarios such as small enterprise campus WLAN access and branch office hotspot coverage.

Typical applications.



WX2520X-LI Next-Generation Enterprise-Class Gateway Wireless Controller Appearance

*For detailed purchasing information, please contact your local H3C office.

Features

Provides management of 802.11ax APs

The WX2520X-LI wireless controller not only supports the management of traditional 802.11a/b/g/n/ac APs, but can also cooperate with H3C's 802.11ax-based APs to form a network, thus breaking through the traditional wireless network serial communication mechanism,

promoting the exponential increase in wireless spectrum resource utilization, greatly increasing the number of effective access users, and effectively reducing wireless network

It reduces the network deployment overhead and greatly improves the user experience in high-density user environments.

Provide flexible data forwarding mode

Traditional wireless controller deployment generally adopts centralized forwarding mode. AC can fully control and supervise the messages, but all wireless service traffic needs to go to AC for forwarding.

In the case of unified processing, the core link bandwidth and AC forwarding capacity can easily become bottlenecks. Especially when the AP and AC are connected via a WAN, the AP acts as a data access device.

Deployed in branch offices, while AC is deployed in headquarters, all user data is sent from AP to AC, which then forwards it centrally, resulting in low forwarding efficiency.

LI wireless controller can support centralized forwarding, distributed forwarding, and policy forwarding. Users can flexibly set the forwarding method according to business needs and actual network conditions.

The WX2520X-LI wireless controller also supports centralized authentication and local forwarding networking. When data flows are forwarded locally, it provides centralized authentication of 802.1X and Portal.

and management.

Supports carrier-grade wireless user access control and management

User-based access control is a key feature of the WX2520X-LI wireless controller. A User Profile provides a configuration template that can store preset configurations (a collection of configurations). Users can configure different User Profile attributes based on different application scenarios, such as Committed Access Rate (CAR) policies and Quality of Service (QoS) policies.

When a user accesses a device, they must first authenticate their identity. During the authentication process, the authentication server will send the User Profile name to the device, and the device will immediately activate the User Profile.

When a user passes the authentication and accesses the device, the device will use these specific contents to restrict the user's access behavior. When the user goes offline, the system will automatically disable

Configuration items under the User Profile remove the restrictions placed on users by the User Profile. Therefore, the User Profile is used to restrict the access behavior of online users. When no users are online (perhaps because no

users have accessed, the user has not passed authentication, or the user is offline), the User Profile is the default configuration and does not take effect.

In addition, the WX2520X-LI wireless controller also supports MAC-based authentication access control, which not only allows customers to perform authentication on user groups on the AAA server, but also allows users to authenticate users on the AAA server.

The configuration and modification of row permissions are supported, and the configuration of permissions for specific users is also supported. This fine-grained user permission control greatly enhances the availability of wireless networks, and network administrators can

This method can easily assign access rights to people or groups at different levels.

MAC-based VLAN is also a major feature of the WX2520X-LI wireless controller. In terms of control strategy, administrators can assign users of the same nature (MAC) to the same VLAN and configure VLAN-based security policies on

the controller. This can not only simplify system configuration but also achieve fine-grained management at the user level.

For security or billing reasons, the system administrator may want to control the location where wireless users can access the network.

User access control. When a wireless user accesses the network, the authentication server can send the list of APs that allow the user to access to the AC, and perform access control on the AC, thereby

The purpose is to limit wireless users to access APs in designated locations.

Provide reliable gateway functionality

The WX2520X-LI is targeted at small and medium-sized enterprises. It combines the functions of a wireless controller with branch office gateway functionality. Its dual WAN ports provide the foundation for uplink backup. Furthermore, the WX2520X-LI supports common gateway features such as PPPoE, NAT gateway, and dynamic and static IP address configuration.

Support Bonjour Gateway

The WX2520X-LI wireless controller supports the Bonjour Gateway function, allowing small businesses to easily use Apple devices such as printers, TVs, and tablets.

Support intelligent channel switching

In wireless LAN, channels are very scarce resources. Each AP can only work on a very limited number of non-overlapping channels. For example, for a 2.4G network, there are only three non-overlapping channels.

Channels, so how to intelligently allocate channels to APs is the key to wireless applications.

There are many possible interference sources in the frequency band of wireless LAN, such as radar and microwave ovens, which will interfere with the normal operation of AP.

function, which can ensure that each AP can be assigned to the optimal channel, reduce and avoid adjacent channel interference as much as possible, and through real-time channel interference detection, it can enable AP to

Avoid interference sources such as radar and microwave ovens.

Support intelligent AP load sharing

The 802.11 protocol leaves wireless roaming decisions to wireless clients. Wireless clients typically select APs based on their signal strength (RSSI). This can easily lead to a large number of clients connecting to the same AP simply because it has a stronger signal. Because these clients share the wireless medium, network throughput for each client is significantly reduced.

The intelligent load sharing method can analyze the location of wireless clients in real time and dynamically determine which APs can share the load with each other at the current time and current location.

The system supports load balancing based on the number of online user sessions and the number of user traffic.

Load sharing.

Support 7-layer mobile security detection/defense (WIDS/WIPS)

The WX2520X-LI wireless controller supports mobile security defense modes including blacklist, whitelist, rogue defense, malformed packet detection, illegal user offline, and pre-configured and upgradeable Signature MAC layer attack detection and countermeasures (e.g., DoS, Flood, and man-in-the-middle attacks). Combined with the wireless application console's built-in intelligent expert knowledge base, it provides flexible wireless security policy decisions. For clearly identified illegal attack sources (APs or terminals), it enables visual physical location tracking and removal of physical switch ports.

By cooperating with H3C's professional core layer firewall/IPS equipment, a 7-layer three-dimensional security defense can be achieved for the mobile campus, meeting the true end-to-end security protection needs from wireless (802.11) to wired (802.3).

Support RealTime Spectrum Guard (real-time spectrum protection) mode

RealTime Spectrum Guard (RTSG) is an innovative, professional monitoring solution for wireless spectrum status. H3C's full range of wireless controllers can be combined with Sensor APs with built-in RF acquisition modules to achieve deeply integrated RF monitoring and real-time spectrum protection.

The RTSG console is integrated and deployed in the H3C iMC intelligent management center. It communicates and collects data with the Sensor AP through the CAPWAP management tunnel, achieving 7X24

24/7 wireless environment quality monitoring, wireless network capability trend assessment, and unlicensed interference alerts. Graphically, it proactively detects and identifies all RF interference sources (Wi-Fi and non-Wi-Fi) in the 2.4GHz/5GHz bands, providing real-time FFT graphs, spectrum density graphs, spectrum graphs, duty cycle graphs, event spectrum graphs, channel power, interference power, and more.

It can automatically identify interference sources and locate problematic wireless devices to ensure optimal wireless network performance. Combined with H3C iAR intelligent reporting components, it can achieve full coverage.

Storage, tracing, and playback of RF quality history records within the zone, automatically generating customized trend, compliance, and audit reports.

In response to different levels of user wireless environment supervision requirements, the RTSG solution can be deployed flexibly in Local Mode or Monitor Mode.

When , normal user access and data packet forwarding can be maintained under the premise of obtaining effective spectrum protection.

Built-in RF Optimization Engine (ROE)

The WX2520X-LI wireless controller features a built-in RF Optimizing Engine for APs. Through signature- and protocol-based RF optimization, it effectively improves application acceleration and quality assurance in wireless deployments, such as high-density access and streaming media transmission. This includes features such as multi-user fair scheduling, hybrid access fairness, interference filtering, rate optimization, spectrum navigation, multicast enhancements (IPv4/IPv6), per-packet power control, and intelligent bandwidth assurance.

Support 802.1x authentication, MAC address authentication, Portal authentication, etc.

The WX2520X-LI wireless controller supports multiple authentication methods:

- 802.1x authentication: WX2520X-LI wireless controller supports multiple 802.1x authentication methods such as TLS, PEAP, TTLS, MD5, SIM card, etc.
802.1x local authentication method provides support for mainstream authentication methods such as MD5, TLS, and PEAP, and users no longer need to configure additional AAA servers.
The WX2520X-LI wireless controller also supports dynamic authorization of VLAN and ACL functions after 802.1x authentication. The user policy can be set in advance.
The system automatically configures customer permissions.
- MAC address authentication: WX2520X-LI wireless controller supports MAC address authentication. For some handheld terminals (such as Wi-Fi Phone, handheld mobile terminals, etc.), it is not convenient to use the computer authentication method. MAC address authentication can easily solve this problem and configure a valid address on the controller or AAA server.
MAC addresses, terminals corresponding to these MAC addresses are allowed to access the network, while illegal terminals that have not been configured in advance cannot access the wireless network.
This function greatly facilitates applications such as wireless medical systems. MAC address authentication can ensure that only the hospital's PDA work terminals can access the wireless network.
Deny patients' wireless PDAs access to private wireless networks.
- Portal authentication: WX2520X-LI wireless controller provides a built-in Portal authentication server. This authentication method does not require client cooperation and is directly connected to the web browser.
The portal page is used as an authentication channel. Once the user passes the authentication, they can flexibly jump to the designated access homepage and start the corresponding authorization and billing.
Requirements, flexible push customized Portal page, to achieve the purpose of advertising and information transmission, widely used in wireless campus, wireless city, visitor access and other application scenarios scene.

Support IPv4/IPv6 dual stack (Native IPv6)

The WX2520X-LI wireless controller supports IPv6 access for wireless clients. At the tunnel starting point AP, since the device is IPv6 aware, it can prioritize IPv6 traffic to the tunnel.

Priority mapping, etc.; on the AC side, complex control and filtering such as ACL filtering can also be performed on IPv6 packets.

WX2520X-LI wireless controller can also be deployed in IPv6 network, and the AC and AP will automatically negotiate to form an IPv6 tunnel. When AC and AP are fully working in IPv6 state,

The wireless controller can still correctly perceive IPv4 and process IPv4 packets of wireless customers. The flexible adaptability of WX2520X-LI wireless controller IPv4/6 can meet customers' needs.

Various complex applications in IPv4 to IPv6 network migration can provide customers with IPv4 services in IPv6 islands, and also allow users to easily

Log in to the network via IPv6 protocol.

In response to the endless stream of IPv6 forged message attacks on campus networks, the WX2520X-LI wireless controller supports IPv6 SAVI (Source Address Validation) technology. By intercepting the address allocation protocol, it obtains the user's IP address, ensuring that the correct address can be used to access the Internet in subsequent applications, and that the IP address of others cannot be forged.

The reliability of the source address is guaranteed. At the same time, the combination of IPv6 SAVI and Portal technology further guarantees the authenticity and security of all Internet user messages.

Provide end-to-end QoS

The WX2520X-LI wireless controller is developed based on the Comware platform. It not only fully supports the Diff-Serv standard, but also adds QoS support for the IPv6 protocol.

The QoS Diff-Serv model mainly includes flow classification, traffic policing (Policing), queue management, queue scheduling (Scheduling), etc., which fully implements the EF,

AF1-AF4, BE and other six groups of PHB and services, so that network operators can provide users with different service quality levels of service guarantees, making the Internet truly a

An integrated network that carries data, voice, and video services.

Support fast Layer 2 and Layer 3 roaming

H3C's centralized wireless architecture can not only easily implement Layer 2 roaming, but also facilitates cross-layer roaming.

The information transmitted between APs is limited, which makes roaming across three layers very difficult to implement. The centralized architecture can easily solve the problem of roaming across three layers.

The controller supports Layer 2 and Layer 3 roaming, and the roaming domain is not restricted by the subnet. This excellent roaming feature allows customers to plan wireless networks without having to consider the existing network.

Planning, more attention should be paid to the coverage of wireless signals. This approach greatly simplifies the early network planning and reduces the network planning cost.

In traditional mode, when wireless user terminals use 802.1x as a means of 802.11 access authentication and key interaction, the interaction messages between wireless user terminals and APs will be very long. When a wireless user terminal roams between two APs, if the wireless user terminal follows the complete 802.1x interaction process when accessing the new AP, roaming will inevitably occur. The roaming handover time is too long. For some services that are sensitive to roaming handover time (such as voice services), such a long handover time is unbearable. The WX2520X-LI wireless controller uses key caching technology to complete the fast handover of users during roaming. Key caching technology makes a good balance between user secure access and fast roaming. This allows wireless user terminals to roam between two APs without having to re-do the complete 802.1x authentication interaction process, while ensuring user identity recognition and password integrity. Wireless users use fast roaming, with roaming time within a single AC not exceeding 50ms, meeting the stringent requirements of voice services.

Product Specifications

Hardware specifications

project	WX2520X-LI
Overall dimensions (width x depth x height)	440 mm *250 mm *43.6 mm
Fully equipped weight	3.1 kg
Throughput	4Gbps
interface	WAN 2*GE & LAN 6*GE+ 2* SFP+
power supply	Built-in open-frame power supply
Operating/storage ambient temperature	0°C~45°C/-40°C~70°C
Working/storage environment relative humidity (non-condensing)	5%~95%
Safety regulations	FDA 21 CFR Subchapter J GB 4943.1 UL 62368-1 CAN/CSA C22.2 No 62368-1 IEC 62368-1 EN 62368-1 AS/NZS 62368-1
EMC	CISPR 35:2016 EN 61000-3-2:2014 EN 61000-3-3:2013 ETSI EN 300 386 V1.6.1(2012-09) ETSI EN 300 386 V2.1.1(2016-07) EN 55032:2015+A1:2020 EN 55032:2015+A11:2020 EN 55035:2017+A11:2020 CISPR 32:2015+AMD1:2019 AS/NZS CISPR 32:2015+AMD1:2020 EN IEC 61000-3-2:2019 EN IEC 61000-3-2:2019+A1:2021 EN 61000-3-3:2013+A1:2019 EN 61000-3-3:2013+A1:2019+A2:2021 EN 61000-3-3:2013+A2:2021+AC:2022

project	WX2520X-LI
	ETSI EN 300 386 V2.2.1(2022-09) GB/T 9254.1-2021
MTBF	≥145 years

Software Specifications

project	Maximum	WX2520X-LI
	number of managed APs supported	128
	Default number of managed APs	0
	License Step	1/4/8/16/32/64/128
	Maximum number of configured APs	256
	Maximum number of users	2048
	ARP entries	4096
	ND entry	4096
Basic performance	IPv4 routing table	4096
	IPv6 routing table	4096
	VLAN Table	4096
	MAC table	4096
	Maximum number of users for Portal authentication	2048
	Maximum number of 802.1x authentication users	2048
	802.11 protocol suite	support
	Maximum number of SSIDs on the device	128
	Hiding SSID	support
	User limit	Support: User limit based on SSID and Radio
	User online detection	support
	Automatic aging of users without traffic	support
802.11MAC	Multi-country code deployment	support
	Wireless user isolation	support: 1. Wireless VLAN wireless user layer 2 isolation 2. SSID-based wireless user layer 2 isolation
	20MHz/40MHz automatic in 40MHz mode Switch	support
	Local forwarding	support
	Automatically enter AP serial number	support
CAPWAP	AC discovery (DHCP option43, DNS method Mode)	support
	IPv6 tunneling	support
	Clock synchronization	support
	AP dual uplink tunnel links	support

project	Supported Features	WX2520X-LI
	Configure AP basic network parameters through AC Support: configure static IP, VLAN, connected AC address, etc.	
	Support L2 and L3 layer networking between AC and AP	
	NAT traversal between AP and AC	support
Roaming capability	In the same AC, different APs have two or three layers of flooding, tour	support
	Different ACs, different APs, second and third layer flooding tour	support
Routing Features	NAT	support
	PPPoE	support
	DDNS	support
	SSL VPN	support
	IPSEC VPN	support
	RIP/RIPNG	support
	GRE	support
Access Control	Open system/Shared-Key	support
	WEP-64/128, Dynamic WEP	support
	WPA/WPA2/WPA3	support
	TKIP	support
	CCMP	support
	WHERE	support
	SSH v2.0	support
	Wireless EAD (Terminal Access Control)	support
	Local authentication	Support: 802.1X, Portal, MAC authentication
	LDAP authentication	support
	Guest access	support
QoS	Priority Mapping	support
	L2-L4 traffic classification	support
	Traffic speed limit	support
	802.11e/WMM	support
	User Profile-based Access control	support
	Intelligent bandwidth speed limit	support
	Intelligent bandwidth guarantee	support:
	Voice optimization (WMM, SVP mapping)	support
	WMM CAC	support
	End-to-end QoS	support
Radio Resource Management	Country code lock	support
	Static channel and power settings	support

project	Supported Features	WX2520X-LI
	Dynamic channel and power settings	support
	Dynamic rate adjustment	support
	Air interface black hole detection and compensation	support
	Load balancing dimensions	Support: Based on traffic, user, frequency band (dual-band support)
	Intelligent load balancing	support
Security Defense	Static blacklist	support
	Dynamic blacklist	support
	Whitelist	support
	Rogue AP Detection	Support: Based on SSID, BSSID, device OUI, etc.
	Illegal AP Countermeasures	support
	Wireless flooding attack prevention (Flooding Attack) support	
	Spoof Attack Prevention	support
	Prevent Weak IV attacks	support
	WIPS	Support: 7-layer mobile security defense
Layer 2 protocol	ARP proxy	support
	802.1p	support
	802.1q	support
	802.1x	support
	Broadcast storm suppression	support
IP protocol	IPv4 protocol	support
	Native IPv6	support
	IPv6 SAVI	support
	IPv6 Portal	support
Multicast Protocol	MLD Snooping	support
	IGMP Snooping	support
	Number of multicast groups	256
	Multicast to unicast (IPv4, IPv6)	Support: Unicast access threshold can be set according to the environment
Network management and configuration	Management methods	Support: WEB, SNMP v1/v2/v3, RMON, etc.
	Configuration method	Support: WEB, CLI, TELNET, FTP, etc.
Green and energy-saving	Shut down AP radio ports on demand	support
	Shut down wireless services on demand	support
	Per-packet power control (PPC)	support
WLAN Comprehensive Application	RF Ping	support
	Remote Probe Analysis	support
	Real-time spectrum guard (RTSG)	support
	Intelligent Wireless Application Awareness (wIAA)	Support/Stateful Firewall
	Fair scheduling mechanism for message sending	support

project	Supported Features	WX2520X-LI
	802.11n message transmission suppression	support
	Traffic shaping based on connection status	support
	Adjust channel sharing between APs	support
	Adjust channel reuse between APs	support
	Radio interface transmission rate adjustment algorithm	support
	Ignore weak signal wireless messages	support
	Prohibit weak signal client access	support
	Disable multicast packet caching	support
	Blink status detection (partial AP)	support



New H3C Technologies Co., Ltd.

Beijing Headquarters
 Building 1, Lixing Center, No. 8 Guangshun South Street, Chaoyang District, Beijing
 Zip code: 100102

Hangzhou Headquarters
 No. 466, Changhe Road, Binjiang District, Hangzhou
 Zip code: 310052
 Tel: 0571-86760000
 Fax: 0571-86760001

<http://www.h3c.com>

Customer Service Hotline
400-810-0504

Copyright ©2021 H3C Technologies Co., Ltd. All rights reserved.
 Disclaimer: Although H3C attempts to provide accurate information in this document, it does not guarantee that the content of this document is free of technical errors or typographical errors. Therefore, H3C assumes no responsibility for any inaccuracies in this document.
 H3C reserves the right to modify the contents of this document without any notice or reminder.