H3C WX5860X New Generation High Performance Multi-Service Access Controller

Release Date: July 2022

New H3C Technologies Co., Limited

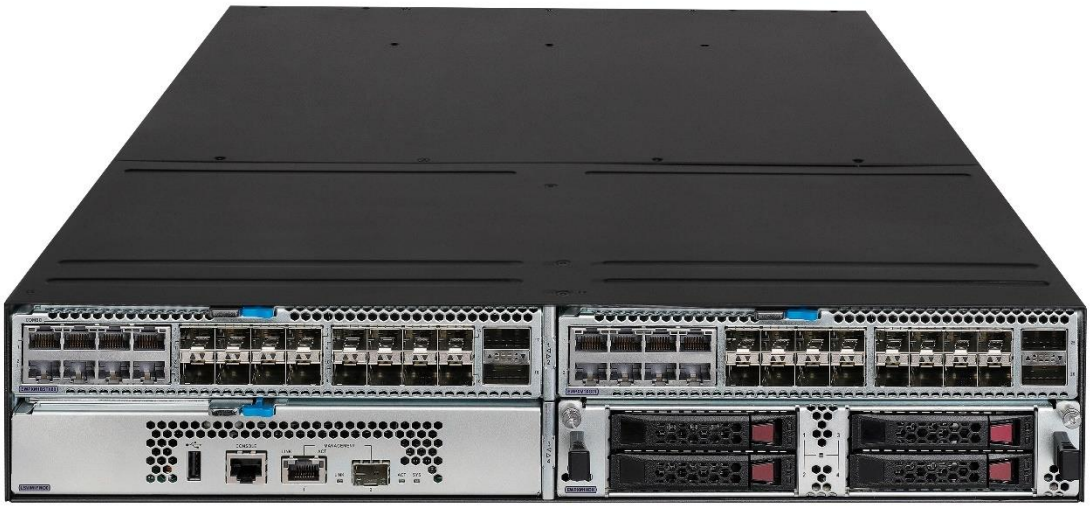
H3C WX5860X New-Generation High-Performance Multiservice Access Controller

Overview

H3C WX5860X access controller is a new generation of high-performance multiservice unified wired and wireless access controller intended for high-end enterprise networks. It features large capacity, high availability, and rich services. Equipped with a high-performance multi-core CPU and a FPGA card, it is even capable of forwarding packets of 64 bytes at line rate over wireless channels. Running H3C's state-of-the-art Comware 7 network operating system, the WX5860X supports not only granular user control and management, comprehensive RF resource management, 7×24 wireless security control, fast Layer 2 and Layer 3 roaming, flexible QoS management, and IPv4/IPv6 dual stack, but also emerging wireless features including multi-core control plane, next-generation wireless location, Bonjour, and Hotspot 2.0.

The WX5860X greatly facilitates network deployment, configuration, and maintenance. It supports multiple flexible networking methods, including Oasis cloud management, IRF, and license synchronization. Also, it provides wired and wireless access on a single platform and enables configuration and management of wired and wireless features in one system.

Working together with H3C fit AP product series, it is an ideal access controller option for large enterprise campuses to provide wireless services such as WLAN access, wireless coverage in MAN, and Wi-Fi hotspot coverage.



WX5860X multiservice access controller

Features and benefits

802.11ax AP management

In addition to 802.11a/b/g/n/ac APs, the WX5860X can work together with H3C 802.11ax APs to provide multiple times faster wireless access rate over larger area. This feature improves user experience and ensures the application of wireless multimedia technology that requires high transmission rate.

Cutting-edge operating system

The WX5860X runs H3C's state-of-the-art Comware 7 network operating system. This system significantly improves product performance and reliability, and supports the increasingly complicated network applications in the enterprise market. This system offers the following advantages:

- **Multi-core control**—Comware 7 can adjust the ratio of the control cores to forwarding cores in the CPU to achieve an optimal balance as demanded, remarkably improving the CPU control capabilities and computing capabilities while providing strong concurrent computing capabilities.
- **User-mode multitasking**—In Comware 7, most network applications are executed 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 7 monitors each task executed 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 7 can upgrade a single module independently instead of the whole system, which enhances upgrade security and network stability significantly.

Powerful wired and wireless processing capability

Equipped with robust hardware, the WX5860X delivers strong concurrent computing capabilities and industry-leading wireless packet processing capabilities:

- Lately-developed high-performance multicore CPU, with 8 independent cores that can be virtualized to 32 logical cores
- High-bandwidth switching chips
- High-performance programmable FPGA card

High-density port access

The WX5860X offers multiple port types and high port density, significantly facilitating wired and wireless accesses and improving networking agility.

License synchronization

H3C license synchronization technology enhances availability of a network with multiple ACs and provides agility for network deployment.

The following two license synchronization modes are available:

- Dual-link backup mode (two ACs)—The two ACs back up licenses for each other. When an AC fails, the other AC takes over the service and APs will be reassociated with the backup AC.
- N+1 backup mode (N ≤ 4)—An AC backs up licenses for other ACs. When one or more of the other ACs fail, the backup AC will take over the service and APs will be reassociated with the backup AC.

Intelligent Resilient Framework (IRF)

The H3C Intelligent Resilient Framework (IRF) technology can virtualize two WX5860X ACs into a logical device called an IRF fabric, which delivers the following benefits:

- Simplified topology—To set up an IRF fabric, you can connect the ACs directly or through an switch. No

dedicated cable or port is required.

- Simplified configuration—The configurations on the IRF fabric (master AC) will be automatically synchronized to the member AC.
- 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 share their licenses. The number of APs that can be connected to the IRF fabric is the sum of licenses installed on the ACs. Licenses installed on an AC can be easily unloaded or migrated.

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 provide network access to APs and process client traffic.

- The central AC 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 provide network access to APs and process client traffic.
- The local ACs can be standard ACs, all-in-one ACs (with routing and DPI features), or unified wired and wireless switches.

AC hierarchy architecture is well suited for large-scale wireless network deployment. It supports headquarter and branch networking applications. 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 allows automatic and convenient version upgrade and configuration synchronization of local ACs and APs. The local ACs are responsible for AP switching, significantly improving roaming performance.

CUPID location

The WX5860X 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.
CUPID is superior to RF fingerprinting in the following aspects:

Item	Description	CUPID	RF fingerprinting
Obstacles	For example, moving people	Almost not affected	Large signal strength attenuation
Multipath effect	For example, signals have been reflected and dispersed during the transmission	Not affected	Greatly affected
Workload	Field survey and signal feature investigation	Small workload	Large workload. It is required to set up a fingerprint database by collecting signal strengths and client locations.
Accuracy	Positioning accuracy	2 m (6.56 ft)	5 to 15 m (16.40 to 49.21 ft), typically 10 m (32.81 ft)
Stability	Positioning stability under interference of environmental factors	Stable positioning result	Positioning result susceptible to obstacles, multipath effect, deployment density, and environment changes.

New-generation Wireless Intelligent Application Aware

Wireless Intelligent Application Aware (wIAA) provides user role-based application-layer security, QoS, and forwarding policies for wired and wireless users. With wIAA, you can control user access and specify networks available for applications such as HTTP and FTP and the allowed bandwidth.

The last-generation wIAA identifies packets based on the fourth-layer port number (such as port number 80 for HTTP, 20/21 for FTP). Users can bypass access restrictions simply by setting up a proxy.

The new-generation wIAA integrates message depth analysis (DPI) and improves application identification and statistical functions. Based on the 7-layer model characteristics of Ethernet packets, as well as the typical packet signature, the new-generation wIAA implements a more precise recognition and complete restriction. With DPI, you can set up a rule to control access to certain types of websites, instead of denying each website individually. This feature simplifies network configuration and improves efficiency.

Flexible forwarding modes

Traditional ACs typically use the centralized forwarding mode. The AC performs centralized control and security monitoring and all user data is sent from APs to the AC for processing and forwarding. This might result in inefficient forwarding. The uplink bandwidth and the forwarding capability of the AC might become the bottleneck, especially when APs are deployed at branches, the AC is deployed at the headquarters, and APs and the AC are connected over a WAN.

The WX5860X supports centralized forwarding, distributed forwarding, and policy-based forwarding, and users can choose the forwarding mode flexibly according to service needs and network conditions.

The WX5860X 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 WX5860X supports the following access control methods:

User profile-based access control

A user profile is a configuration template that saves predefined configurations such as Committed Access Rate (CAR) and QoS policies for clients. When a client passes authentication, the authentication server sends the related user profile to the AC. The AC uses the configuration in the user profile to restrict the client's access. When the client goes offline, the AC disables the user profile. You can configure several user profiles for different clients to achieve user profile-based access control.

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.

Smart Roaming Features

- Supports intra-AC roaming, cross-AC roaming, and cross-VLAN Layer 3 roaming
- Portal roaming information synchronization function: AC and AP support Portal users' non-perceived roaming between ACs on a large-scale network, without the Portal mac-trigger server. The wireless controller can independently assume the mac-trigger server function. This reduces the pressure on the portal server and prevents the portal server from becoming a performance bottleneck. When the Portal server is done, the online terminal can still roam without authentication between no less than 10 wireless controllers.
- 802.1X roaming information synchronization function: AC and AP support 802.1X users for fast roaming between ACs on a large-scale network. Support dot1x authentication for fast roaming between ACs. Terminals do not need to do authentication again after roaming to a new AC. Alleviate server pressure and ensure fast access of terminals, and support fast roaming between more than 10 ACs.
- Support 802.11k/v/r fast roaming protocols

Intelligent dynamic frequency selection (DFS)

In a WLAN, adjacent APs need to 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 WX5860X provides session-based load balancing and traffic-based load balancing during roaming. 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.
Support SSID automatic hiding function based on radio resource utilization. When the radio resource reaches or exceeds the configured threshold, the SSID automatically hides to provide users with stable and reliable wireless services.

Wireless intrusion detection and prevention system (WIDS/WIPS)

The WX5860X 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 DoS attacks, flood attacks, and man-in-the-middle attacks.
With the huge intelligent expert information base built in the wireless application center, the AC can visually track and monitor physical locations of attackers and shut down a physical port.
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 WX5860X supports the following authentication methods:

- 802.1X authentication—The WX5860X 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 WX5860X also supports dynamic VLAN assignment and ACL through predefined user profiles.

- MAC authentication—The WX5860X supports MAC address authentication to authenticate hand-held terminals such as Wi-Fi phones and hand-held mobile terminals. On the WX5860X or AAA server, you can specify MAC addresses allowed to access a WLAN. MAC addresses not specified are considered illegal and cannot access the WLAN. This function facilitates some wireless applications such as the wireless healthcare system where MAC authentication can ensure that only the PDAs of the hospital can access the dedicated WLAN but not those owned by patients.
- Portal authentication—The WX5860X 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 in various scenarios like wireless campus, wireless city, and guest access.

IPv4/IPv6 dual stack (native IPv6)

The WX5860X 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 WX5860X to provide services to various complicated applications during migration from IPv4 to IPv6.
The WX5860X 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 7 operating system, the WX5860X 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 WX5860X under H3C fit AP+AC architecture 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 WX5860X 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 50 ms, which ensures transmission of speed-demanding voice traffic.

Remote access for branches

The WX5860X 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	Specification
Dimensions (H × W × D)	88.1 × 440 × 660 mm (3.47 ×17.32×25.98 in)
Weight (full configuration)	22.9 kg
Throughput	80/160Gbps
Ports	Support 2 interface cards at most. The specification of each card: 2 x 40G（QSFP+） 8 x 10G（SFP+） 8 x GE Combo (2×40G and 8×10G are mutually exclusive) 1*Console 3*USB 1*OOBM
Power supply	Removable AC or DC power modules Support for 1+1 or 1+3 power module redundancy (Power module should be purchased separately.)
Maximum power consumption	< 502 W
Temperature	Operating temperature: 0°C to +45°C (+32°F to +113°F)

Item	Specification
	Storage temperature: –40°C to +70°C (–40°F to +158°F)
Relative humidity (non-condensing)	Operating and storage humidity: 5% to 95%
Safety standards	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 EN60601-1-2 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	≥ 50, 000 hours

Software specifications

Item	Specification	
Basic capabilities	Supported APs without license	0
	License type	1/4/8/16/32/64/128/512/1024
	Max. manageable number of APs	6656/8192
	Max. configurable number of APs	32768
	Max. manageable number of wireless users	81920
802.11 MAC	802.11 protocol suite	
	Hide SSID	
	802.11g protection	
	802.11n only	
	Client quantity limit	SSID-based client quantity limit Radio-based client quantity limit

Item	Specification	
	Online client detection	
	Automatic client aging	
	Multi-country code	
	User isolation	VLAN-based user isolation SSID-based user isolation
	20 MHz/40 MHz auto-switch in 40 MHz mode	
	Local forwarding	Local forwarding based on SSID+VLAN
CAPWAP	Auto AP	
	AC discovery (DHCP option 43 and DNS)	
	IPv6 tunnel	
	Network synchronization	
	Jumbo frame forwarding	
	AP preprovisioning	AP basic network settings such as static IP, VLAN, and AC's IP address
	NAT traversal between AP and AC	
Roaming	Intra-AC Layer 2 and Layer 3 roaming	
	Inter-AC Layer 2 and Layer 3 roaming	
Access control	Open system, shared key authentication	
	WEP-64/128, dynamic WEP	
	WPA, WPA2,WPA3	
	TKIP	
	CCMP (802.11n recommended)	
	WAPI (optional)	
	SSH1.5/2.0	
	Wireless End-point Access Domination (EAD)	
	Oasis cloud authentication	
	Portal authentication	Transparent authentication, remote or external server
	Portal webpage redirection	SSID-based portal webpage redirection AP-based portal webpage redirection
	Portal by-pass proxy	
	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, portal authentication, MAC authentication
	LDAP authentication	Portal access 802.1X access with EAP-GTC or EAP-TLS
	AP-based access control	
	Guest access control	

Item	Specification	
	VIP tunnel	
	ARP anti-attack	Wireless SAVI
	SSID anti-spoofing	Username and SSID binding
	Domain- and SSID-based AAA server selection	
	AAA server backup	
	Local AAA server for wireless clients	
	TACACS+	
QoS	Priority mapping	
	Layer 2 to Layer 4 traffic classification	
	Rate limit	Granularity of 8 Kbps
	802.11e/WMM	
	User profile-based access control	
	Intelligent bandwidth limit (equal bandwidth share algorithm)	
	Intelligent bandwidth limit (user specific)	
	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	
	Call Admission Control (CAC)	CAC based on client quantity or bandwidth
	End-to-end QoS	
	Coupled with H3C WLAN APs, the AC can identify variety of applications and policy control can be implemented including priority adjustment, scheduling, blocking, and rate limiting on users	
	AP uplink rate limit	
WLAN radio resource management (RRM)	Country code lock	
	Static channel and power configuration	
	Dynamic channel and power configuration	
	Transmit power control (TPC)	
	Coverage hole detection and correction	
	Load balancing mode	Traffic-based load balancing Session-based load balancing Radio group based load balancing (dual-band supported)
	Intelligent load balancing	
	AP load balancing group	Auto-discovery and flexible setting
Security	Static blacklist	
	Dynamic blacklist	
	Whitelist	
	Rogue AP detection	Rogue AP detection based on SSID, BSSID, or device OUI

Item	Specification	
	Countermeasures against rogue APs	
	Anti-flooding	
	Anti-spoofing	
	Anti-weak IV attack	
	WIPS	7-layer mobile security protection
Layer 2 protocols	ARP proxy	
	802.1p	
	802.1q	
	802.1X	
	Broadcast storm suppression	
IP protocols	IPv4	
	Native IPv6	
	IPv6 SAVI	
	IPv6 Portal	
Multicast	MLD Snooping	
	IGMP Snooping	
	Number of multicast groups	256
	Multicast-to-unicast conversion (IPv4/IPv6)	Support for unicast threshold setting
Backup	1+1, N+1, N+N AC backup	Support for license sharing
	AP load balancing	
	Remote AP	
Network management and configuration	Management	WEB, SNMPv1/v2/v3, RMON
	Configuration	Web, CLI, Telnet, FTP
Wireless location	CUPID location	
Wireless Gateway	VPN	IPSEC, GRE
	NAT, NPAT	
Power save	Scheduled radio shutdown	
	Scheduled wireless service shutdown	
	Per-packet power control (PPC)	
WLAN application	RF Ping	
	Remote probing and analysis	
	RealTime Spectrum Guard (RTSG)	
	Wireless Intelligent Application Aware (wIAA)	Based on stateful firewall
	Packet forwarding fairness scheduling	
	802.11n packet forwarding suppression	

Item	Specification
	Connection status-based traffic shaping
	AP channel sharing
	AP channel reusing
	Radio transmission rate adjustment algorithm
	Ignore packets with low RSSI
	Forbid clients with low RSSI from accessing a WLAN
	Forbid multicast buffering
	Blink status detection

Ordering Information

Product ID	Product Description
EWP-WX5860X-GL	H3C WX5860X Access Controller
EWPXM1BSTX80	H3C WX5500X Hardware Acceleration Module
LSVM1DC650	650W DC Power Supply Module (Power Panel Side Intake Airflow)
PSR650B-12A1-D	650W AC Power Supply

LSWM1BFANSCB-SN	H3C Fan Module (Fan Panel Side Exhaust Airflow)
LIS-WX-1-BE	Enhanced Access Controller License, 1 AP, for V7
LIS-WX-4-BE	Enhanced Access Controller License,4 APs, for V7
LIS-WX-8-BE	Enhanced Access Controller License,8 APs, for V7
LIS-WX-16-BE	Enhanced Access Controller License,16 APs, for V7
LIS-WX-32-BE	Enhanced Access Controller License,32 APs, for V7
LIS-WX-64-BE	Enhanced Access Controller License,64 APs, for V7
LIS-WX-128-BE	Enhanced Access Controller License,128 APs, for V7
LIS-WX-512-BE	Enhanced Access Controller License,512 APs, for V7
LIS-WX-1024-BE	Enhanced Access Controller License,1024 APs, for V7
SFP-GE-LX-SM1310-A	1000BASE-LX SFP Transceiver, Single Mode (1310nm, 10km, LC)
SFP-GE-SX-MM850-A	1000BASE-SX SFP Transceiver, Multi-Mode (850nm, 550m, LC)
SFP-XG-LX-SM1310-E	SFP+ Module (1310nm,10km, LC)
SFP-XG-SX-MM850-E	SFP+ Module (850nm,300m, LC)
QSFP-40G-LR4-WDM1300	QSFP+ 40GBASE Optical Transceiver Module (1310nm,10km, LR4, LC)
QSFP-40G-BIDI-SR-MM850	QSFP+ 40GBASE BIDI Optical Transceiver Module (850nm,100m, SR)
QSFP-40G-LR4L-WDM1300	QSFP+ 40GBASE Optical Transceiver Module (1310nm,2km, LR4L, LC)

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

http://www.h3c.com