H3C WSG1840X Wireless Integrated Multi-Service Gateway

Release Date: October, 2023

New H3C Technologies Co., Limited

H3C WSG1840X Wireless Integrated Multi-Service Gateway

Overview

The H3C WSG1840X Wireless Integrated Multi-Service Gateway is well designed and positioned for SMB network. It features gateway, security and AC function integration, reducing the number of devices and TCO in network. It adopts the innovative Comware V7 platform (referred to as V7 hereafter). V7 comes with the standard granular user control management, comprehensive RF resource management, 7x24 wireless security control, fast layer-2 and layer-3 roaming, strong QoS and IPv4/IPv6 dual stack. V7 adds in various novel wireless technologies such as multi-core control plane, Bonjour and Hotspot 2.0. It also supports multiple network configurations such as cloud management. When paired with H3C SMB APs (See ordering information for details), it serves as an ideal access control solution for WLAN access of SMB network.

WSG1840X

Features

All Inclusive AP License

The WSG1840X Wireless Integrated Multi-Service Gateway includes AP license as following by default, which protects customer’ s investment to maximum, which also give SMB/SME a great opportunity to add new AP with the wireless network expansion without additional cost. The number of licenses is up to 128, and 64 licenses are built-in by default. Which means WSG1840X can manage 64 ordinary AP or 128 wall-plate AP by default. Need to purchase extra license to enlarge the ordinary AP number. (Version supported since WSG1800X-CMW710-E5623)

model	AP license by default
WSG1840X	64

AC Model	Max AP Qty.		License	
	WA6120/WA6126/WA6120X	WA6120H	Default	Add-on

WX1840X	128	0	64	64
	0	128	64	0
	64	64	64	32

All-in-one Gateway

The WSG1840X Wireless Integrated Multi-Service Gateway integrates, gateway, security and AC function in one box, which is perfect for SOHO, SMB and SME environment. WSG1840X supports full enterprise controller feature sets, in addition, WSG1840X supports gateway function, such as PPPOE, NAT, dynamic IP address, and static IP address setting function.

802.11ax AP Management

In addition to 802.11a/b/g/ac AP management, the WSG1840X can work together with H3C 802.11ax based SMB APs (See ordering information for details) to provide wireless access speed several times faster than a traditional 802.11a/b/g/ac/ network.

Flexible Forwarding Modes

In a wireless network of centralized forwarding mode, all wireless traffic is sent to an AC for processing which the forwarding capability of the AC may become a bottleneck. Especially on wireless networks where APs are deployed at branches, ACs are deployed at the headquarters, and APs and ACs are connected over a WAN. In this scenario, Distributed forwarding is more suitable. The WSG1840X supports both distributed forwarding modes and centralized forwarding mode and it can set SSID based forwarding as needed.

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 Channel Switching

- In a WLAN, adjacent wireless APs should work in different channels to avoid channel interference. However, channels are very rare resources for a WLAN. There are a small number of non-overlapping channels for APs. For example, there are only three non-overlapping channels for the 2.4GHz network. Therefore, the key to wireless applications is how to allocate channels for APs intelligently
- Meanwhile, there are many possible interference sources that can affect the normal operation of APs in a WLAN, such as rogue APs, radars and microwave ovens. The intelligent channel switching technique can ensure the allocation of an optimal channel to each AP, thereby minimizing adjacent channel interference. Besides, the real-time interference detection function can help keep APs away from interference sources such as radars and microwave ovens

Intelligent AP Load Sharing

- According to IEEE 802.11, wireless clients control wireless roaming in WLANs. Usually, a wireless client chooses an AP based on the Received Signal Strength Indication (RSSI). Therefore, many clients may choose the same AP with a high RSSI. As these clients share the same wireless medium, the throughput of each client is reduced greatly.
- The intelligent AP load sharing function can analyze the locations of wireless clients in real time, dynamically determine which APs at the current location can share load with one another, and implement load sharing among these APs. In addition to load sharing based on the number of online sessions, the system also supports load sharing based on the traffic of online wireless users
- 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.

Layer 4-7 Deep Packet Inspection

The WSG1840X can identify variety of applications and policy control can be implemented including priority adjustment, scheduling, blocking, and rate limiting to ensure efficient bandwidth resource and improve the network quality.

Layer 7 Wireless Intrusion Detection and Prevention Systems (WIDS / WIPS)

- The WSG1840X supports the blacklist, whitelist, rogue device defense, bad packet detection, illegal user removal, upgradeable Signature MAC layer attack detection (DoS attack, Flood attack or man-in-the-middle attack) and counter measures
- With the built-in knowledge base in WSG1840X, you can perform timely and accurate wireless security decisions. For determined attack sources such as rogue AP or terminals, you can perform visible physical location monitoring and switch physical port removing
- With H3C firewall/IPS device, network infrastructure can also implement layer 7 security defense in wireless campus, covering wired (802.11) and wireless (802.3) secure connections on an end-to-end basis

Comprehensive Network Security Protection Capabilities

The rich feature library can complete the detection of popular viruses. It supports anti-virus to botnets, Trojans, and worms. It can identify 1500+ high-profile applications. With rich attack prevention technology, it can support both IPv4 and IPv6. It can provide effective protection against the following attacks:
1) Abnormal packet attacks (such as illegal TCP packet flags, Land, smurf, WinNuke, Ping of Death, Large ICMP Traffic/Tiny Fragment, etc.);
2) Address spoofing attacks (such as IP address attacks, port attacks, etc.);
3) Abnormal traffic attacks (such as Ack Flood, DNS Flood, Fin Flood, HTTP Flood, HTTPS Flood,ICMP Flood, ICMPV6 Flood, SYNACK Flood, SYN Flood, UDP Flood, etc.);

- Security zone—Allows you to configure security zones based on interfaces and VLANs.
- Packet filtering—Allows you to apply standard or advanced ACLs between security zones to filter packets based on information contained in the packets, such as UDP and TCP port numbers. You can also configure time ranges during which packet filtering will be performed.
- Access control—Supports access control based on users and applications and integrates deep intrusion prevention with access control.
- ASPF—Dynamically determines whether to forward or drop a packet by checking its application layer protocol information and state. ASPF supports inspecting FTP, HTTP, SMTP, RTSP, and other TCP/UDP-based application layer protocols.
- AAA—Supports authentication based on RADIUS/HWTACACS+, CHAP, and PAP.
- Blacklist—Supports static blacklist and dynamic blacklist.
- NAT and VRF-aware NAT.

- Security logs—Supports operation logs, zone pair policy matching logs, attack protection logs, DS-LITE logs, and NAT444 logs.
- Routing—Supports static routing, RIP, OSPF, BGP, routing policies, and application- and URL-based policy-based routing.
- Traffic monitoring, statistics, and management.

Next-generation multi-service features

- Integrated link load balancing feature—Uses link state inspection and link busy detection technologies, and applies to a network egress to balance traffic among links.
- Integrated SSL VPN feature—providing secure access of mobile users to the enterprise network.

Flexible and extensible, integrated and advanced DPI security

- Integrated security service processing platform—Highly integrates the basic and advanced security protection measures to a security platform.
- Application layer traffic identification and management.Uses the state machine and traffic exchange inspection technologies to detect traffic of P2P, IM, network game, stock, network video, and network multi-media applications. It Uses the deep inspection technology to identify P2P traffic precisely and provides multiple policies to control and manage the P2P traffic flexibly.
- Categorized filtering of massive URLs—uses the local+cloud mode to provide basic URL filtering blacklist and whitelist and allows you to query the URL category filtering server on line.
- Complete and updated security signature database—H3C has a senior signature database team and professional attack protection labs that can provide a precise and up-to-date signature database.

Hardware Specifications

Item	WSG1840X
Dimensions (WxDxH)	440*165*43.6mm
Weight	1.8kg
Wireless throughput	4Gbps
Port	LAN：1*SFP Plus + 4*GE + 1*5GE WAN：2 GE + 1*USB
Power supplies	100V AC~240V AC:50/60Hz
Operating and storage temperature	0℃~45℃/-40℃~70℃
Operating and storage relative humidity	5%~95%

Item	WSG1840X
Safety Compliance	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	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	≥50000hours

Software specifications

Item	Feature	WSG1840X
Basic functions	Number of managed APs by default	64 ordinary AP or 128 wall-plate AP
	Maximum number of managed APs	128
	Maximum users of authentication	2048
802.11MAC	802.11 Protocols	√
	The number of SSID of whole machine	128
	SSID hiding	√
	11G protection	√
	11n only	√
	Use number limit	Supported: SSID based, per RF based
	Keepalive	√
	Idle	√
	Multi-country code assignment	√
	Wireless user isolation	Supported: VLAN based wireless users 2-layer isolation SSID based wireless user 2-layer isolation
	20MHz/40MHz auto-switch in 40MHz mode	√

Item	Feature	WSG1840X
	Local forwarding	Local forwarding based on SSID+VLAN
CAPWAP	Automatic AP registration	√
	AC discovery (DHCP option43, DNS)	√
	IPv6 tunnel	√
	Clock synchronization	√
	Jumbo frame forwarding	√
	Assign basic AP network parameter through AC	Supported: Static IP, VLAN, connected AC address
	L2/L3 connection between AP and AC	√
	NAT traversal between AP and AC	√
Roaming	Intra-AC, Inter-AP L2 and L3 roaming	√
	Inter-AC, Inter-AP L2 and L3 roaming	√
GW Features	NAT	√
	PPPoE	√
	DDNS	√
	SSL VPN	√
	IPSEC VPN	√
	RIP	√
	GRE	√
Access control	Open system, Shared-Key	√
	WEP-64/128, dynamic WEP	√
	WPA,WPA2,WPA3	√
	TKIP	√
	CCMP	√ (11n recommended)
	SSH v1.5/v2.0	√
	Portal authentication	Supported: Remote Authentication, external server
	Portal page redirection	Supported: SSID based, AP Portal page push
	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, MAC authentication
	LDAP authentication	802.1X and Portal EAP-GTC and EAP-TLS supported by 802.1X login
	AP location-based user access control	√
	Guest Access control	√
	VIP channel	√
	ARP attack detection	Supported: Wireless SAVI
	SSID anti-spoofing	SSID + user name binding
	AAA server selection based on SSID and domain	√
	AAA server back up	√
	Local AAA server for wireless user	√

Item	Feature	WSG1840X
	TACACS+	√
QoS	Priority mapping	√
	L2-L4 packet filtering and traffic classification	√
	Rate limit	Supported with granularity of 8Kbps
	802.11e/WMM	√
	Access control based on user profile	√
	Intelligent bandwidth limit (equal bandwidth share algorithm)	√
	Intelligent bandwidth limit (user specific)	√
	Intelligent bandwidth guarantee	Supported: Free flow for packets coming from every SSID When traffic is not congested, and guarantee a minimum bandwidth for each SSID when traffic is congested
	QoS Optimization for SVP phone	√
	CAC(Call Admission Control)	Supported: based on user number/bandwidth
	End-to-end QoS	√
	AP upload speed limit	√
RF management	Country code lock	√
	Static channel and power configuration	√
	Auto channel and power configuration	√
	Auto transmission rate adjustment	√
	Coverage hole detection and correction	√
	Load balancing	Supported: based on traffic, user & frequency (dual-frequency supported)
	Intelligent load balancing	√
	AP load balancing group	Supported: auto-discovery and flexible setting
Security	Static blacklist	√
	Dynamic blacklist	√
	White list	√
	Rogue AP detection	Supported: SSID based, BSSID, device OUI
	Rouge AP countermeasure	√
	Flooding attack detection	√
	Spoof attack detection	√
	Weak IV attack detection	√
	WIPS/WIDS	Supported: 7-layer mobile security
Layer 2 protocol	ARP (gratuitous ARP)	√
	802.1p	√
	802.1q	√ (Maximum VLANs: 4094)
	802.1x	√
IP protocol	IPv4 protocol	√
	Native IPv6	√
	IPv6 SAVI	√

Item	Feature	WSG1840X
	IPv6 Portal	√
Multicast	MLD Snooping	√
	IGMP Snooping	√
	Multicast group	256
	Multicast to Unicast (IPv4, IPv6)	Supported: Set unicast limit based on operating environment
Redundancy	1+1 failover between ACs	√
	Intelligent AP sharing among ACs	√
	Remote AP	√
Management and deployment	Network management	WEB, SNMP v1/v2/v3, RMON
	Network deployment	WEB, CLI, Telnet, FTP
Green features	Scheduled shutdown of AP RF interface	√
	Scheduled shutdown of wireless service	√
	Per-packet power adjustment (PPC)	√
WLAN Application	RF Ping	√
	Remote probe analysis	√
	Packet forwarding fairness adjustment	√
	802.11n packet forwarding suppression	√
	Access based traffic shaping	√
	Co-AP channel sharing	√
	Co-AP channel reuse	√
	RF interface transmission rate adjustment algorithm	√
	Drop wireless packet with weak signal	√
	Disable user access with weak signal	√
	Disable multicast packet caching	√
	Status blink(limited to some AP)	√
New added features	Policy forwarding	√
	VLAN pool	√
	Bonjour gateway	√
	802.11w	√
	802.11k,v,r	√
	Hotspot2.0 (802.11u)	√
	NAT	√
	VPN	√
Firewall	Attack protection against malicious attacks, such as land, smurf, fraggle, ping of death, teardrop, IP spoofing, IP fragmentation, ARP spoofing, reverse ARP lookup, invalid TCP flag, large ICMP packet, address/port scanning, SYN flood, ICMP flood, UDP flood, and DNS query flood	√

Item	Feature	WSG1840X
	ASPF application layer packet filtering	√
	Basic and advanced ACLs	√
	Time range-based ACL	√
	User-based and application-based access control	√
	Static and dynamic blacklist function	√
	MAC-IP binding	√
	MAC-based ACL	√
Antivirus	Signature-based virus detection	√
	Manual and automatic upgrade for the signature database	√
	Stream-based processing	√
	Virus detection based on HTTP, FTP, SMTP, and POP3	√
	Virus types include Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare, and Virus	√
	Virus logs and reports	√
	Signature-based virus detection	√
Deep intrusion prevention	Prevention against common attacks such as hacker, worm/virus, Trojan, malicious code, spyware/adware, DoS/DDoS, buffer overflow, SQL injection, and IDS/IPS bypass	√
	Attack signature categories (based on attack types and target systems) and severity levels (including high, medium, low, and notification)	√
	Manual and automatic upgrade for the attack signature database (TFTP and HTTP).	√
	P2P/IM traffic identification and control	√
Email/webpage/application layer filtering	Email filtering	√
	SMTP email address filtering	√
	Email subject/content/attachment filtering	√
	Webpage filtering	√
	HTTP URL/content filtering	√
	Java blocking	√
	ActiveX blocking	√
	SQL injection attack prevention	√
VPN	L2TP VPN	√
	IPSec VPN	√
	GRE VPN	√
	SSL VPN	√

Item	Feature	WSG1840X
NAT	Many-to-one NAT, which maps multiple internal addresses to one public address	√
	Many-to-many NAT, which maps multiple internal addresses to multiple public addresses	√
	One-to-one NAT, which maps one internal address to one public address	√
	NAT of both source address and destination address	√
	External hosts access to internal servers	√
	Internal address to public interface address mapping	√
	NAT support for DNS	√
	Setting effective period for NAT	√
	NAT ALGs for NAT ALG, including DNS, FTP, H.323, ILS, MSN, NBT, PPTP, and SIP	√

Ordering Information:

Product ID	**Product Description**
EWP-WSG1840X	H3C WSG1840X 8-Port (6*1000BASE-T, 1*5GE-T, and 1*SFP Plus) Wireless Integrated Services Gateway
LIS-WX-1-SME-OVS	H3C SME-OVS Access Controller 1-AP License
LIS-WX-4-SME-OVS	H3C SME-OVS Access Controller 4-AP License
LIS-WX-8-SME-OVS	H3C SME-OVS Access Controller 8-AP License
LIS-WX-16-SME-OVS	H3C SME-OVS Access Controller 16-AP License
Remarks	**Description**
Supporting SMB APs	WA6120/WA6126/WA6120X/WA6120H

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