# H3C WSG1812X-PWR Puerta de enlace multiservicio integrada inalámbrica

New H3C Technologies Co., Limited

# H3C WSG1812X-PWR Puerta de enlace multiservicio integrada inalámbrica

## Visión general

Diseña y posiciones la Puerta de enlace de servicios múltiples integrada inalámbrica H3C WSG1812X-PWR para redes de SMB. Características gateway, seguridad y función AC integración, reduciendo número dispositivos y TCO en red. Adopta la innovadora plataforma Comware V7 (denominada V7 de aquí en adelante). V7 viene con el estándar de control de usuarios granular, gestión integral de recursos RF, control de seguridad inalámbrica 7x24, roaming rápido de capa 2 y capa 3, fuerte QoS y pila dual IPv4 / IPv6. Agrega en diversas tecnologías inalámbricas como el control de plano multi-núcleo, Bonjour y Hotspot 2.0. Además, soporta múltiples configuraciones de red como gestión en la nube. Cuando se empareja con los AP de H3C SMB (consulte la información de pedido para obtener más detalles), se convierte en una solución de control de acceso ideal para el acceso WLAN de la red SMB.

WSG1812X-PWR

# Características

## Licencia de AP Todo Incluido

La Puerta de enlace de servicios múltiples integrada inalámbrica WSG1812X-PWR incluye la licencia AP como se indica a continuación, lo cual protege la inversión del cliente al máximo y también brinda a las PYMES una excelente oportunidad de agregar nuevos puntos de acceso para la expansión de la red inalámbrica sin costos adicionales.  El número de licencias es de hasta 64, y 32 licencias están incorporadas por defecto. Significa que WSG1812X-PWR puede gestionar 32 AP ordinarios o 64 AP de placa mural de forma predeterminada. Compra una licencia adicional para ampliar el número de AP ordinario. Versión admitida desde WSG1800X-CMW710-E5623

| modelo | Licencia AP por defecto. |
|---|---|
| WSG1812X-PWR | 32 |

| Modelo de AC | Cantidad máxima de AP | | Licencia | |
|---|---|---|---|---|
| | WA6120/WA6126/WA6120X | WA6120H | Defecto | Añádelo |
| WX1812X-PWR | 64 | 0 | 32 | 32 |
| | 0 | 64 | 32 | 0 |
| | 32 | 32 | 32 | 16 |

## Puerta de enlace todo en uno

El Gateway de Servicios Múltiples Integrado Inalámbrico WSG1812X-PWR integra PoE, gateway, seguridad y función AC en una sola caja, perfecta para entornos SOHO, SMB y SME. WSG1812X-PWR soporta todas las funciones de controlador empresarial, además, WSG1812X-PWR soporta funciones de gateway, como PPPOE, NAT, configuración de dirección IP dinámica y estática.

## Capacidad de PoE+ Incorporado

Todos los puertos LAN del WSG1812X-PWR admiten la función PoE 802.3af/802.3at, lo que ahorra TCO al entorno existente del cliente y reduce al mismo tiempo los puntos únicos de falla. Un solo puerto puede proporcionar un máximo de 30W (150W en total para toda la máquina) para alimentar los dispositivos conectados, como teléfonos IP, puntos de acceso inalámbricos y cámaras de alta potencia.

## Gestiona el punto de acceso 802.11ax

Además de la gestión de AP 802.11a/b/g/ac, el WSG1812X-PWR puede trabajar junto con los AP SMB basados en 802.11ax de H3C (consulte la información de pedido para obtener detalles) para proporcionar una velocidad de acceso inalámbrico varias veces más rápida que una red tradicional 802.11a/b/g/ac/.

## Modos de reenvío flexibles

En una red inalámbrica en modo de reenvío centralizado, todo el tráfico inalámbrico se envía a un AC para su procesamiento, lo cual puede convertirse en un cuello de botella debido a la capacidad de reenvío del AC. Especialmente en redes inalámbricas donde los AP se despliegan en las sucursales, los AC se despliegan en la sede central y los AP y AC se conectan a través de una WAN. En este escenario, la reenviación distribuida es más adecuada. El WSG1812X-PWR admite tanto los modos de reenvío distribuido como el modo de reenvío centralizado y puede configurar el reenvío basado en SSID según sea necesario.

## Características de Roaming Inteligente

- Compatible con roaming intra-AC, roaming cruzado AC y roaming cruzado de capa 3 VLAN.

- Función de sincronización de información itinerante del portal. AC y AP admiten el roaming no percibido de los usuarios del Portal entre los AC en una red a gran escala, sin el servidor mac-trigger del Portal. El controlador inalámbrico puede asumir de forma independiente la función del servidor de activación de MAC. Esto reduce la presión en el servidor del portal y evita que se convierta en un cuello de botella de rendimiento. Cuando el servidor Portal esté listo, la terminal en línea aún puede moverse libremente sin autenticación entre no menos de 10 controladores inalámbricos.
- 802.1X función de sincronización de información de roaming. AC y AP soportan usuarios 802.1X para una rápida itinerancia entre ACs en una red a gran escala. Soporte la autenticación dot1x para una itinerancia rápida entre los AC. Terminales no necesitan autenticar de nuevo después de migrar a un nuevo AC. Alivia la presión del servidor y asegura un acceso rápido de los terminales, y apoya el roaming rápido entre más de 10 ACs.
- Soporte los protocolos de roaming rápido 802.11k/v/r.

## Cambiate de canal inteligentemente.

- En una WLAN, los AP inalámbricos adyacentes deben trabajar en diferentes canales para evitar interferencias en el canal. Sin embargo, los canales son recursos muy escasos para una WLAN. Hay un pequeño número de canales no superpuestos para los AP. Por ejemplo, solo hay tres canales no superpuestos para la red de 2.4GHz. Por lo tanto, la clave para las aplicaciones inalámbricas es cómo asignar canales a los APs de manera inteligente.
- Mientras tanto, hay muchas fuentes posibles de interferencia que pueden afectar el funcionamiento normal de los AP en una WLAN, como APs fraudulentos, radares y hornos de microondas. La técnica de cambio de canal inteligente puede asegurar la asignación de un canal óptimo para cada AP, minimizando así la interferencia del canal adyacente. Además, la función de detección de interferencias en tiempo real puede ayudar a mantener los AP alejados de fuentes de interferencia como los radares y los hornos de microondas.

## Comparte la carga de los AP inteligentes

- De acuerdo con IEEE 802.11, controla el roaming inalámbrico en las WLANs. Normalmente, el cliente inalámbrico elige un AP basado en la Indicación de Fuerza de Señal Recibida (RSSI). Por lo tanto, muchos clientes eligen el mismo AP con un alto RSSI. Como estos clientes comparten el mismo medio inalámbrico, la velocidad de cada cliente se reduce considerablemente.
- La función de compartir carga AP inteligente puede analizar las ubicaciones de los clientes inalámbricos en tiempo real, determinar dinámicamente qué AP en la ubicación actual puede compartir carga entre sí y llevar a cabo la carga compartida entre estos AP. Además de compartir

la carga basado en el número de sesiones en línea, el sistema también admite compartir la carga basado en el tráfico de usuarios inalámbricos en línea.

- Apoya la función de ocultar automáticamente SSID basado en la utilización de recursos de radio. Cuando el recurso de radio alcance o supere el umbral configurado, el SSID se oculta automáticamente para brindar a los usuarios servicios inalámbricos estables y confiables.

## Realiza una inspección profunda del paquete en la capa 4-7.

Identifica una variedad de aplicaciones y aplica el control de políticas, ajustando prioridades, programando, bloqueando y limitando la velocidad para garantizar un uso eficiente del ancho de banda y mejorar la calidad de la red.

## Layer 7 Sistemas de Detección y Prevención de Intrusiones Inalámbricas (WIDS / WIPS)

- El WSG1812X-PWR soporta la lista negra, lista blanca, defensa de dispositivos maliciosos, detección de paquetes malos, eliminación de usuarios ilegales, detección de ataques de capa MAC con firma actualizable (ataque de DoS, ataque de inundación o ataque de hombre en el medio) y medidas de contraataque.
- Con la base de conocimientos incorporada en WSG1812X-PWR, realiza decisiones de seguridad inalámbrica de manera oportuna y precisa. Para fuentes de ataques determinadas como rogue AP o terminales, realiza monitoreo de ubicación física visible y desconecta el puerto físico del interruptor.
- Con el dispositivo firewall/IPS de H3C, también puedes implementar defensa de seguridad de capa 7 en la infraestructura de red en el campus inalámbrico, cubriendo conexiones seguras por cable (802.11) e inalámbricas (802.3) de extremo a extremo.

## Comprende capacidades de protección de seguridad de red.

Completa la detección de virus populares con la amplia biblioteca de características. Apoya el anti-virus contra botnets, troyanos y gusanos. Puede identificar más de 1500 aplicaciones destacadas. Con tecnología rica en prevención de ataques, soporta tanto IPv4 como IPv6. Puede proporcionar protección efectiva contra los siguientes ataques:

1) Ataques de paquetes anormales (como banderas ilegales de paquete TCP, Land, smurf, WinNuke, Ping of Death, tráfico ICMP grande/fragmento pequeño, etc.).

2) Ataques de suplantación de dirección (como ataques de dirección IP, ataques de puerto, etc.).

3) Ataques de tráfico anormal (como el Flood de Ack, el Flood de DNS, el Flood de Fin, el Flood de HTTP, el Flood de HTTPS, el Flood de ICMP, el Flood de ICMPV6, el Flood de SYNACK, el Flood de SYN, el Flood de UDP, etc.).

- Zona de seguridad: Permite configurar zonas de seguridad en base a interfaces y VLANs.
- Filtrado de paquetes: Aplica ACL estándar o avanzada entre zonas de seguridad para filtrar paquetes basándose en la información contenida en los paquetes, como los números de puerto UDP y TCP. Configura los rangos de tiempo durante los cuales se realizará el filtrado de paquetes.
- Aplicar control de acceso: Soporta control de acceso basado en usuarios y aplicaciones e integra prevención de intrusos profunda con control de acceso.
- ASPF: Determina dinámicamente si reenviar o desechar un paquete mediante la comprobación de la información del protocolo de capa de aplicación y el estado. APSF soporta la inspección de protocolos de capa de aplicación basados en TCP/UDP como FTP, HTTP, SMTP, RTSP y otros.
- Apoya la autenticación basada en RADIUS/HWTACACS+, CHAP y PAP.
- Lista negra: admite lista negra estática y lista negra dinámica.
- Traducción: NAT y NAT compatible con VRF.
- Registros de seguridad: admite registros de operación, registros de coincidencia de políticas de pares de zonas, registros de protección contra ataques, registros DS-LITE y registros NAT444.
- Routing—Soporta enrutamiento estático, RIP, OSPF, BGP, políticas de enrutamiento y enrutamiento basado en políticas de aplicaciones y URL.
- Monitoreo de tráfico, estadísticas y gestión.

## Características multi-servicio de próxima generación

- Característica integrada de equilibrio de carga de enlaces: utiliza tecnologías de inspección del estado del enlace y detección de enlace ocupado, y se aplica a una salida de red para equilibrar el tráfico entre los enlaces.
- Funcionalidad de VPN SSL integrada: proporciona acceso seguro de los usuarios móviles a la red de la empresa.

## Flexible y extensible, integrada y avanzada seguridad de DPI

- Integra las medidas de seguridad básicas y avanzadas en una plataforma de seguridad.
- Identificación y gestión del tráfico de la capa de aplicación: utiliza la máquina de estados y las tecnologías de inspección de intercambio de tráfico para detectar el tráfico de aplicaciones P2P, mensajes instantáneos, juegos en red, acciones, vídeos en red y aplicaciones multimedia en red.

Usa la tecnología de inspección profunda para identificar el tráfico P2P con precisión y proporciona múltiples políticas para controlar y gestionar el tráfico P2P de manera flexible.

- Filtrado categorizado de URL masivas: utiliza el modo local + nube para proporcionar una lista negra y una lista blanca de filtrado de URL básico y te permite consultar el servidor de filtrado de categorías de URL en línea.
- Base de datos de firma de seguridad completa y actualizada: H3C tiene un equipo senior de base de datos de firma y laboratorios de protección contra ataques profesionales que pueden proporcionar una base de datos de firma precisa y actualizada.

## Especificaciones de hardware

| Artículo | WSG1812X-PWR |
|---|---|
| Dimensiones (ancho × profundidad × altura) | 440×220×43.6mm |
| Peso | 2,9kg |
| Rendimiento inalámbrico | 4Gbps |
| Puerto | LAN: 2*SFP Plus + 12*PoE+<br>WAN: 2 GE<br>+ 1*USB |
| Fuentes de alimentación | 100V AC to 240V AC:50/60Hz |
| Operar y almacenar temperatura | 0ºC a 45ºC / -40ºC a 70ºC |
| Operar y almacenar la humedad relativa | 5% to 95% |
| Cumple con las normas de seguridad | UL 60950-1<br>CAN/CSA C22.2 No 60950-1<br>IEC 60950-1<br>EN 60950-1/A11<br>AS/NZS 60950<br>EN 60825-1<br>ES 60825-2<br>EN60601-1-2<br>FDA 21 CFR Subcapítulo J |

| | |
|---|---|
| EMC | ETSI EN 300 386 V1.3.3:2005<br>EN 55024: 1998+ A1: 2001 + A2: 2003<br>EN 55022 :2006<br>VCCI V-3:2007<br>ICES-003:2004<br>EN 61000-3-2:2000+A1:2001+A2:2005<br>EN 61000-3-3:1995+A1:2001+A2:2005<br>AS/NZS CISPR 22:2004<br>FCC PART 15:2005<br>GB 9254:1998<br>GB/T 17618:1998 |
| MTBF | ≥ 50000 horas |

## Especificaciones del software

| Artículo | Característica | WSG1812X-PWR |
|---|---|---|
| Funciones básicas | Número de AP gestionados por defecto | 32 AP ordinarios o 64 AP de placas de pared |
| | Número máximo de AP administrados. | 64 |
| | Usuarios máximos de autenticación | 1024 |
| 802.11MAC | Protocolos 802.11 | √ |
| | El número de SSID de la máquina completa. | 32 |
| | Oculta el SSID | √ |
| | Protección 11G | √ |
| | 11n solamente. | √ |
| | Usa límite de número. | Soportado. SSID basado, por RF basado |
| | Mantén vivo | √ |
| | Inactivo | √ |
| | Asignación de códigos multipaíses | √ |
| | Aislamiento de usuarios inalámbricos | Soportado. |

| | | |
|---|---|---|
| | | Basado en VLAN, aislamiento de usuarios inalámbricos de 2 capas<br>Basado en SSID, aísla a los usuarios inalámbricos en dos capas. |
| | Activar cambio automático de 20MHz/40MHz en modo 40MHz. | √ |
| | Reenvía localmente. | Reenvío local basado en SSID+VLAN |
| CAPWAP | Registro automático de AP | √ |
| | Descubre AC (opción DHCP43, DNS) | √ |
| | Túnel IPv6 | √ |
| | Sincroniza el reloj. | √ |
| | Reenviar Jumbo frame forwarding | √ |
| | Asigna los parámetros básicos de la red AP a través del AC. | Soportado. IP estática, VLAN, dirección MAC conectada |
| | Conectar el AP y el AC mediante una conexión L2/L3. | √ |
| | Trasladar a español: Travesía NAT entre AP y AC | √ |
| Roaming | Roaming Intra-AC, Inter-AP L2 y L3 | √ |
| | Roaming Inter-AC, Inter-AP L2 y L3 | √ |
| Características de GW | NAT | √ |
| | PPPoE | √ |
| | Configura DDNS en el router. | √ |
| | SSL VPN | √ |
| | VPN IPSEC | √ |
| | RIP | √ |
| | GRE | √ |
| Acceso control | Abrir sistema, Clave compartida. | √ |
| | WEP-64/128, WEP dinámico | √ |
| | WPA, WPA2, WPA3 | √ |
| | TKIP | √ |

| | | |
|---|---|---|
| | CCMP | √ (recomendado 11n) |
| | SSH v1.5/v2.0. | √ |
| | Autentica en el portal. | Soportado. Autenticación remota, servidor externo. |
| | Redirección de página del portal | Soportado. Basado en SSID, empuja la página del portal del AP. |
| | Portal by-pass Proxy | √ |
| | Autenticación 802.1x | EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5, EAP-SIM, LEAP, EAP-FAST, EAP offload (TLS, PEAP only) |
| | Au thentification locale. | 802.1X, Portal, autenticación MAC |
| | Autenticación LDAP | 802.1X y Portal<br>Soporte EAP-GTC y EAP-TLS para inicio de sesión 802.1X. |
| | Localización de AP control de acceso de usuario. | √ |
| | Control de acceso de invitados | √ |
| | Canal VIP | √ |
| | Detectar ataque ARP | Soportado. Inalámbrico SAVI |
| | SSID anti-spoofing | Vincula SSID y nombre de usuario. |
| | Selecciona el servidor AAA basado en el SSID y el dominio. | √ |
| | Respuesta: El servidor AAA está respaldando | √ |
| | Servidor AAA local para usuario inalámbrico. | √ |
| | TACACS+ | √ |
| QoS | Mapeo de prioridad | √ |
| | Filtrar y clasificar paquetes de nivel L2-L4. | √ |
| | Límite de tasa | Apoya con una granularidad de 8Kbps. |
| | 802.11e/WMM | √ |

| | | |
|---|---|---|
| | Control de acceso basado en el perfil de usuario. | √ |
| | Límite inteligente de ancho de banda (algoritmo de compartir ancho de banda igual) | √ |
| | Limita el ancho de banda de forma inteligente (usuario específico). | √ |
| | Garantiza ancho de banda inteligente. | Soportado. Flujo libre para paquetes provenientes de cada SSID. Garantiza un ancho de banda mínimo para cada SSID cuando hay congestión de tráfico. |
| | Optimiza la calidad de servicio para el teléfono SVP. | √ |
| | CAC (Control de Admisión de Llamadas) | Basado en el número de usuario / ancho de banda. |
| | End-to-end QoS | √ |
| | Límite de velocidad de carga AP. | √ |
| Gestión de la RF | Código de país bloquear | √ |
| | Configura el canal estático y la potencia | √ |
| | Configura el canal y la potencia automaticamente. | √ |
| | Ajusta la tasa de transmisión automática. | √ |
| | Detecta y corrige los agujeros de cobertura. | √ |
| | Carga balanceada | Basado en el tráfico, el usuario y la frecuencia (compatible con doble frecuencia) |
| | Equilibrio de carga inteligente | √ |
| | Grupo de balanceo de carga de AP | Soportado: auto-descubrimiento y configuración flexible. |
| Seguridad | Lista negra estática | √ |
| | Lista negra dinámica | √ |

| | | |
|---|---|---|
| | Lista blanca. | √ |
| | Detecta APs intrusos | Soportado. SSID basado, BSSID, OUI del dispositivo |
| | Medida para contrarrestar AP falsos | √ |
| | Detecta ataques de inundación. | √ |
| | Detecta ataques de suplantación | √ |
| | Detectar ataques de IV débiles. | √ |
| | WIPS/WIDS | Soportado. Seguridad móvil de 7 capas |
| Protocolo de Capa 2 | ARP (ARP gratuito) | √ |
| | 802.1p | √ |
| | 802.1q | √ (Máximo de VLANs: 4094) |
| | 802.1x | √ |
| Protocolo IP | Protocolo IPv4 | √ |
| | IPv6 nativo. | √ |
| | IPv6 SAVI | √ |
| | Portal de IPv6 | √ |
| Multicast | MLD Snooping | √ |
| | Activa el IGMP Snooping. | √ |
| | Grupo de multidifusión | 256 |
| | Multicasta a Unicast (IPv4, IPv6) | Soportado. Establece límite unicast basado en el entorno operativo. |
| Redundancia | 1+1 conmutación entre ACs. | √ |
| | Comparte inteligente de APs entre ACs. | √ |
| | AP Remota | √ |
| Gestiona y despliega. | Gestiona la red | WEB, SNMP v1/v2/v3, RMON. |
| | Despliega la red. | WEB, CLI, Telnet, FTP |
| Características verdes | Apaga programado de la interfaz inalámbrica del AP. | √ |
| | Cierre programado del servicio | √ |

| | | |
|---|---|---|
| | inalámbrico | |
| | Ajusta la potencia por paquete (APP) | √ |
| WLAN Aplicación | RF Ping | √ |
| | Análisis de la sonda remota | √ |
| | Ajustar equidad de reenvío de paquetes | √ |
| | Supresión de reenvío de paquetes 802.11n | √ |
| | Acceso basado en la modelación de tráfico | √ |
| | Comparte el canal Co-AP | √ |
| | Reutiliza el canal Co-AP. | √ |
| | Ajusta el algoritmo de tasa de transmisión de la interfaz RF. | √ |
| | Descarta el paquete inalámbrico con señal débil. | √ |
| | Deshabilita el acceso de usuario con señal débil. | √ |
| | Desactiva la caché de paquetes multicast. | √ |
| | Estado parpadeo (limitado a algunos AP) | √ |
| Nuevas características añadidas | Reenvía la política. | √ |
| | VLAN pool | √ |
| | ¡Hola! gateway | √ |
| | 802.11w | √ |
| | 802.11k,v,r | √ |
| | Hotspot2.0 (802.11u) | √ |
| | NAT | √ |
| | VPN | √ |
| Cortafuegos | Protección contra ataques maliciosos | √ |

| | | |
|---|---|---|
| | como land, smurf, fraggle, ping de la muerte, teardrop, IP spoofing, fragmentación de IP, ARP spoofing, búsqueda inversa de ARP, bandera TCP inválida, paquete ICMP grande, escaneo de dirección/puerto, inundación SYN, inundación ICMP, inundación UDP y DNS query flood. | |
| | Filtra los paquetes de la capa de aplicación de ASPF. | √ |
| | Básica y avanzada ACLs | √ |
| | ACL basada en rango de tiempo | √ |
| | Basado en usuarios y aplicaciones control de acceso | √ |
| | Función de lista negra estática y dinámica | √ |
| | Ligadura MAC-IP | √ |
| | Basado en MAC ACL | √ |
| Antivirus | Detéctalo por firmas de virus. | √ |
| | Manual y automática actualización para la base de datos de firmas | √ |
| | Procesamiento basado en stream | √ |
| | Detéctalo Virus basado en HTTP, FTP, SMTP y POP3. | √ |
| | Tipos de virus incluyen Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare y Virus. | √ |
| | Registros y reportes de virus | √ |
| | Detéctalo por firmas de virus. | √ |
| Prevención profunda de intrusión. | Prevención contra ataques comunes como hacker, gusano/virus, Troyano, código malicioso, spyware/adware, DoS/DDoS, desbordamiento de búfer, inyección SQL y bypass de | √ |

| | | |
|---|---|---|
| | IDS/IPS. | |
| | Categorías de firmas de ataque (basadas en tipos de ataque y sistemas objetivo) y niveles de gravedad (que incluyen alta, media, baja y notificación) | √ |
| | Actualiza manual o automáticamente la base de datos de firmas de ataque (TFTP y HTTP). | √ |
| | Identificación y control de tráfico P2P/IM. | √ |
| Filtrar capa de correo electrónico/ página web/aplicación | Filtrado de Correo Electrónico | √ |
| | Filtrar direcciones de correo electrónico SMTP | √ |
| | Filtrar el asunto/contenido/archivo adjunto del correo electrónico. | √ |
| | Filtración de páginas web | √ |
| | Filtra el contenido de la URL HTTP. | √ |
| | Bloqueo de Java. | √ |
| | Bloquea ActiveX | √ |
| | Prevención de ataques de inyección SQL. | √ |
| VPN | L2TP VPN | √ |
| | IPSec VPN | √ |
| | GRE VPN | √ |
| | SSL VPN | √ |
| NAT | Muchos a uno NAT, que asigna múltiples direcciones internas a una sola dirección pública | √ |
| | Muchos a muchos NAT, que asigna múltiples direcciones internas a múltiples direcciones públicas. | √ |
| | Uno a uno NAT, que mapea una | √ |

| | | |
|---|---|---|
| | dirección interna a una dirección pública. | |
| | NAT de la dirección de origen y de la dirección de destino | √ |
| | Acceso de los hosts externos a los servidores internos. | √ |
| | Mapea la dirección interna a la dirección de interfaz pública. | √ |
| | Soporte NAT para DNS. | √ |
| | Establece el período efectivo para NAT. | √ |
| | NAT ALGs para NAT ALG, incluyendo DNS, FTP, H.323, ILS, MSN, NBT, PPTP y SIP | √ |

## Información de pedido

| ID de producto | Descripción del producto |
|---|---|
| EWP-WSG1812X-PWR | H3C WSG1812X-PWR 16-Port (14*1000BASE-T and 2*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 |
| Comentarios | Descripción |
| Apoya a los AP de SMB. | WA6120/WA6126/WA6120X/WA6120H |

The Leader in Digital Solutions

**New H3C Technologies Co., Limited**

Sede de Beijing

Torre 1, Centro LSH, 8 Calle Guangshun Sur, Chaoyang Distrito, Beijing, China

Código postal: 100.102

Sede Hangzhou

No.466 Changhe Road, Distrito de Binjiang, Hangzhou, Zhejiang,

China

Código postal: 310.052