

# CloudEngine S6730-H Series 25GE Switches

Huawei CloudEngine S6730-H series 25GE switches are next-generation enterprise-class core and aggregation switches that provide 25GE downlink optical ports and 100GE uplink optical ports.

## Product Overview

Huawei CloudEngine S6730-H series switches are next-generation enterprise-class core and aggregation switches that offer high performance, high reliability, cloud management, and intelligent operations and maintenance (O&M). They build on an industry-leading Versatile Routing Platform (VRP) and are purpose-built with security, IoT, and cloud in mind. With these traits, CloudEngine S6730-H can be widely used in enterprise campuses, colleges/universities, data centers, and other scenarios.


CloudEngine S6730-H switches offer 10GE, 25GE, 40GE, and 100GE port types, flexibly adapting to diversified network bandwidth requirements. They also support cloud management and implement cloud-managed network services throughout the full lifecycle from planning, deployment, monitoring, experience visibility, and fault rectification, all the way to network optimization, greatly simplifying network management.

By integrating the native wireless access controller (WAC) capability, a single CloudEngine S6730-H switch can manage a vast number of wireless access points (APs). The results are simplified network architecture, fewer required devices, and lowered networking costs. Free mobility, another key differentiator of CloudEngine S6730-H, enables consistent user experience no matter the user location or IP address, fully meeting enterprises' demands for mobile offices.

CloudEngine S6730-H switches support VXLAN to implement network virtualization, achieving multi-purpose networks and multi-network convergence for greatly improved network capacity and utilization. As such, CloudEngine S6730-H switches are an ideal choice for building next-generation IoT converged networks in terms of cost, flexibility, and scalability.

The full series of CloudEngine S6730-H switches have built-in security probes to enable abnormal traffic detection, analysis of threats even in encrypted traffic, and network-wide threat deception. With such robust security features, CloudEngine S6730-H switches transform traditional passive security defense into proactive security protection, fully ensuring campus network security.

## Models and Appearance

Appearance	Description
 CloudEngine S6730-H28Y4C	<ul style="list-style-type: none"> <li>• 28 x 25 Gig SFP28, 4 x 100 Gig QSFP28</li> <li>• Dual pluggable power modules, 1+1 power backup</li> <li>• Switching capacity: 2.2Tbps/2.4Tbps</li> </ul> <p><b>NOTE</b></p> <p>25GE SFP28 interfaces support 10GE and 25GE optical module auto-sensing.</p> <p>100GE QSFP28 interfaces support 40GE and 100GE optical module auto-sensing.</p> <p>The value before the slash (/) refers to the device's switching capability, while the value after the slash (/) means the chip's switching capability.</p>

# Features and Highlights

## Abundant Convergence

- This CloudEngine S6730-H series provides the integrated WLAN AC function that can manage 1K APs, reducing the costs of purchasing additional WLAN AC hardware. With this switch series, customers can stay ahead in the high-speed wireless era.
- The CloudEngine S6730-H series supports SVF and functions as a parent switch. With this virtualization technology, a physical network with the "Small-sized core and aggregation switches + Access switches + APs" structure can be virtualized into a "super switch", greatly simplifying network management.
- The CloudEngine S6730-H series provides excellent QoS capabilities and supports queue scheduling and congestion control algorithms. Additionally, it adopts innovative priority queuing and multi-level scheduling mechanisms to implement fine-grained scheduling of data flows, meeting service quality requirements of different user terminals and services.

## Providing Granular Network Management

- The CloudEngine S6730-H series uses the Packet Conservation Algorithm for Internet (iPCA) technology that alters the traditional method of using simulated traffic for fault location. iPCA technology can monitor network quality for any service flow anywhere, anytime, without extra costs. It can detect temporary service interruptions in a very short time and can identify faulty ports accurately. This cutting-edge fault detection technology turns "extensive management" to "granular management."
- The CloudEngine S6730-H supports Two-Way Active Measurement Protocol (TWAMP) to accurately check any IP link and obtain the entire network's IP performance. This protocol eliminates the need of using a dedicated probe or a proprietary protocol.

## Flexible Ethernet Networking

- In addition to traditional Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP), the CloudEngine S6730-H supports Huawei-developed Smart Ethernet Protection (SEP) technology and the latest Ethernet Ring Protection Switching (ERPS) standard. SEP is a ring protection protocol specific to the Ethernet link layer, and applies to various ring network topologies, such as open ring topology, closed ring topology, and cascading ring topology. This protocol is reliable, easy to maintain, and implements fast service switching within 50 milliseconds. ERPS is defined in ITU-T G.8032. It implements millisecond-level protection switching based on traditional Ethernet MAC and bridging functions.
- The CloudEngine S6730-H supports Smart Link and Virtual Router Redundancy Protocol (VRRP), which implement backup of uplinks. One CloudEngine S6730-H switch can connect to multiple aggregation switches through multiple links, significantly improving reliability of access devices.

## Intelligent Stack (iStack)

- The CloudEngine S6730-H series supports the iStack function that combines multiple switches into a logical switch. Member switches in a stack implement redundancy backup to improve device reliability and use inter-device link aggregation to improve link reliability. iStack provides high network scalability. You can increase a stack's ports, bandwidth, and processing capability by simply adding member switches. iStack also simplifies device configuration and management. After a stack is set up, multiple physical switches can be virtualized into one logical device. You can log in to any member switch in the stack to manage all the member switches in it.

## Cloud-based Management

- The Huawei cloud management platform allows users to configure, monitor, and inspect switches on the cloud, reducing on-site deployment and O&M manpower costs and decreasing network OPEX. Huawei switches support both cloud management and on-premise management modes. These two management modes can be flexibly switched as required to achieve smooth evolution while maximizing return on investment (ROI).

## VXLAN Features

- VXLAN is used to construct a Unified Virtual Fabric (UVF). As such, multiple service networks or tenant networks can be deployed on the same physical network, and service and tenant networks are isolated from each other. This capability truly achieves 'one network for multiple purposes'. The resulting benefits include enabling data transmission of different services or customers, reducing the network construction costs, and improving network resource utilization.
- This series switches are VXLAN-capable and allow centralized and distributed VXLAN gateway deployment modes. These switches also support the BGP EVPN protocol for dynamically establishing VXLAN tunnels and can be configured using NETCONF/YANG.

## Link Layer Security

- This series switches support MACsec. MACsec protects transmitted Ethernet data frames through identity authentication, data encryption, integrity check, and anti-replay protection, reducing the risks of information leakage and malicious network attacks. With MACsec, these switch models are able to address strict information security requirements of customers in industries such as government and finance.

## Intelligent O&M

- This series switches provides telemetry technology to collect device data in real time and send the data to Huawei campus network analyzer(iMaster NCE-CampusInsight). The CampusInsight analyzes network data based on the intelligent fault identification algorithm, accurately displays the real-time network status, effectively demarcates and locates faults in a timely manner, and identifies network problems that affect user experience, accurately guaranteeing user experience.
- This series switches supports a variety of intelligent O&M features for audio and video services, including the enhanced Media Delivery Index (eMDI). With this eMDI function, the switch can function as a monitored node to periodically conduct statistics and report audio and video service indicators to the CampusInsight platform. In this way, the CampusInsight platform can quickly demarcate audio and video service quality faults based on the results of multiple monitored nodes.

## Intelligent Upgrade

- Switches support the intelligent upgrade feature. Specifically, switches obtain the version upgrade path and download the newest version for upgrade from the Huawei Online Upgrade Platform (HOUP). The entire upgrade process is highly automated and achieves one-click upgrade. In addition, preloading the version is supported, which greatly shortens the upgrade time and service interruption time.
- The intelligent upgrade feature greatly simplifies device upgrade operations and makes it possible for the customer to upgrade the version independently. This greatly reduces the customer's maintenance costs. In addition, the upgrade policies on the HOUP platform standardize the upgrade operations, which greatly reduces the risk of upgrade failures.

## Big Data-Powered Collaborative Security

- This series of switches supports encrypted communication analytics (ECA), a traffic identification and detection technology. ECA can precisely detect malicious traffic by efficiently identifying encrypted and non-encrypted traffic, extracting the characteristics of encrypted traffic, and sending these characteristics to HiSec Insight (a big data-powered security analysis system). Furthering to this, ECA-capable switches can work with the controller iMaster NCE-Campus to automatically isolate threats, thereby ensuring campus network security.
- This series of switches also supports network deception technology. Specifically, switches functioning as sensors can detect threats (such as IP address scanning and port scanning on the network) and lure threat traffic to the honeypot for simulated interaction with attackers. In this way, it is easy to obtain attack behaviors, extract attack tools, and analyze suspicious traffic in depth to create defense policies. Switches then work with iMaster NCE-Campus to automatically isolate threats and block the spread of attack behaviors, ensuring campus network security.

## Open Programmability System(OPS)

- Open Programmability System (OPS) is an open programmable system based on the Python language. IT administrators can program the O&M functions of a switch through Python scripts to quickly innovate functions and implement intelligent O&M.

# Licensing

## Licensing

This series switches supports both the traditional feature-based licensing mode and the latest Huawei IDN One Software (N1 mode for short) licensing mode. The N1 mode is ideal for deploying Huawei CloudCampus Solution in the on-premises scenario, as it greatly enhances the customer experiences in purchasing and upgrading software services with simplicity.

### Software Package Features in N1 Mode

Switch Functions	N1 Basic Software	N1 Foundation Software Package	N1 Advanced Software Package
------------------	-------------------	--------------------------------	------------------------------

Switch Functions	N1 Basic Software	N1 Foundation Software Package	N1 Advanced Software Package
<b>Basic network functions:</b> Layer 2 functions, IPv4, IPv6, MPLS, SVF, and others Note: For details, see the Service Features	√	√	√
<b>Basic network automation based on the iMaster NCE-Campus:</b> <ul style="list-style-type: none"> <li>Basic automation: Plug-and-play, SSID, and AP group management</li> <li>Basic monitoring: Application visualization</li> <li>NE management: Image and topology management and discovery</li> <li>WLAN enhancement: Roaming and optimization for up to 128 APs</li> </ul>	x	√	√
<b>Advanced network automation and intelligent O&amp;M:</b> VXLAN, user access authentication, free mobility, and CampusInsight basic functions	x	x	√

Note: Only V200R019C00 and later versions can support N1 mode

## Product Specifications

Item	CloudEngine S6730-H28Y4C
Fixed ports	28 x 25 Gig SFP28, 4 x 100 Gig QSFP28
Dimensions (H x W x D)	43.6 mm x 442.0 mm x 220.0 mm (1.72 in. x 17.4 in. x 8.66 in.)
Chassis height(U)	1U
Rated voltage range	<ul style="list-style-type: none"> <li>AC input: 100 V AC to 240 V AC, 50/60 Hz</li> <li>High-Voltage DC input: 240 V DC</li> <li>DC input: -48 V DC to -60 V DC</li> </ul>
Maximum voltage range	<ul style="list-style-type: none"> <li>AC input: 90 V AC to 290 V AC, 45 Hz to 65 Hz</li> <li>High-Voltage DC input: 190 V DC to 290 V DC</li> <li>DC input: -38.4 V DC to -72 V DC</li> </ul>
Maximum input current	<ul style="list-style-type: none"> <li>AC 300W: 4A</li> <li>DC 260W: 10A</li> </ul>
Typical power consumption (30% of traffic load, tested according to ATIS standard)	186W
Maximum power consumption (100% throughput, full speed of fans)	253W
Operating temperature	-5°C to +45°C (23°F to 113°F) at an altitude of 0-1800 m (0-5906 ft.) <b>NOTE</b> When the altitude is 1800-5000 m (5906-16404 ft.), the highest operating temperature reduces by 1°C (1.8°F) every time the altitude increases by 220 m (722 ft.).

Item	CloudEngine S6730-H28Y4C
	The switch cannot be started when the ambient temperature is lower than 0°C (32°F).
Storage temperature	-40°C to +70°C (-40°F to +158°F)
Operating altitude	0-5000 m (0-16404 ft.)
Noise (sound pressure at normal temperature)	< 64.5 db(A)
Power supply surge protection	<ul style="list-style-type: none"> <li>Using AC power modules: ±6 kV in differential mode, ±6 kV in common mode</li> <li>Using DC power modules: ±2 kV in differential mode, ±4 kV in common mode</li> </ul>
Power supply type	<ul style="list-style-type: none"> <li>300 W AC Power Module</li> <li>260 W DC Power Module</li> </ul> <p><b>NOTE</b> The S6730-H can use a single power module or double power modules for 1+1 power redundancy. Pluggable AC and DC power modules can be used together in the same switch.</p>
Relative humidity	5% to 95% (non-condensing)
Fans	3, Built-in fan
Heat dissipation	Heat dissipation with fan, intelligent fan speed adjustment

## Service Features

Except for special instructions, the following features are supported by CloudEngine S6730-H with N1 basic software.

Feature	Description
MAC	Up to 384K MAC address entries IEEE 802.1d standards compliance MAC address learning and aging Static, dynamic, and blackhole MAC address entries Packet filtering based on source MAC addresses
VLAN	4K VLANs Guest VLANs and voice VLANs GVRP MUX VLAN VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports VLAN mapping
ARP	Static ARP Dynamic ARP
IP routing	Static routes, RIP v1/2, RIPng, OSPF, OSPFv3, IS-IS, IS-ISv6, BGP, BGP4+, ECMP, routing policy Up to 256K FIBv4 entries Up to 80K FIBv6 entries
Interoperability	VLAN-Based Spanning Tree (VBST), working with PVST, PVST+, and RPVST Link-type Negotiation Protocol (LNP), similar to DTP VLAN Central Management Protocol (VCMP), similar to VTP

Feature	Description
Wireless service	<p>AP access control, AP domain management, and AP configuration template management</p> <p>Radio management, unified static configuration, and dynamic centralized management</p> <p>WLAN basic services, QoS, security, and user management</p> <p>CAPWAP, tag/terminal location, and spectrum analysis</p>
Ethernet loop protection	<p>RRPP ring topology and RRPP multi-instance</p> <p>Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protection switchover</p> <p>SEP</p> <p>ERPS (G.8032)</p> <p>BFD for OSPF, BFD for IS-IS, BFD for VRRP, and BFD for PIM</p> <p>STP (IEEE 802.1d), RSTP (IEEE 802.1w), and MSTP (IEEE 802.1s)</p> <p>BPDU protection, root protection, and loop protection</p>
MPLS	<p>MPLS L3VPN</p> <p>MPLS L2VPN (VPWS/VPLS)</p> <p>MPLS-TE</p> <p>MPLS QoS</p>
IPv6 features	<p>Neighbor Discover (ND)</p> <p>PMTU</p> <p>IPv6 Ping, IPv6 Tracert, IPv6 Telnet</p> <p>ACLs based on source IPv6 addresses, destination IPv6 addresses, Layer 4 ports, or protocol types</p> <p>Multicast Listener Discovery snooping (MLDv1/v2)</p> <p>IPv6 addresses configured for sub-interfaces, VRRP6, DHCPv6, and L3VPN</p>
Multicast	<p>IGMP v1/v2/v3 snooping and IGMP fast leave</p> <p>Multicast forwarding in a VLAN and multicast replication between VLANs</p> <p>Multicast load balancing among member ports of a trunk</p> <p>Controllable multicast</p> <p>Port-based multicast traffic statistics</p> <p>IGMP v1/v2/v3, PIM-SM, PIM-DM, and PIM-SSM</p> <p>MSDP</p> <p>Multicast VPN</p>
QoS/ACL	<p>Rate limiting in the inbound and outbound directions of a port</p> <p>Packet redirection</p> <p>Port-based traffic policing and two-rate three-color CAR</p> <p>Eight queues on each port</p> <p>DRR, SP, and DRR+SP queue scheduling algorithms</p> <p>WRED</p> <p>Re-marking of the 802.1p and DSCP fields of packets</p> <p>Packet filtering at Layer 2 to Layer 4, filtering out invalid frames based on the source MAC address, destination MAC address, source IP address, destination IP address, TCP/UDP source/destination port number, protocol type, and VLAN ID</p> <p>Queue-based rate limiting and shaping on ports</p>
Security	<p>Hierarchical user management and password protection</p> <p>DoS attack defense, ARP attack defense, and ICMP attack defense</p>

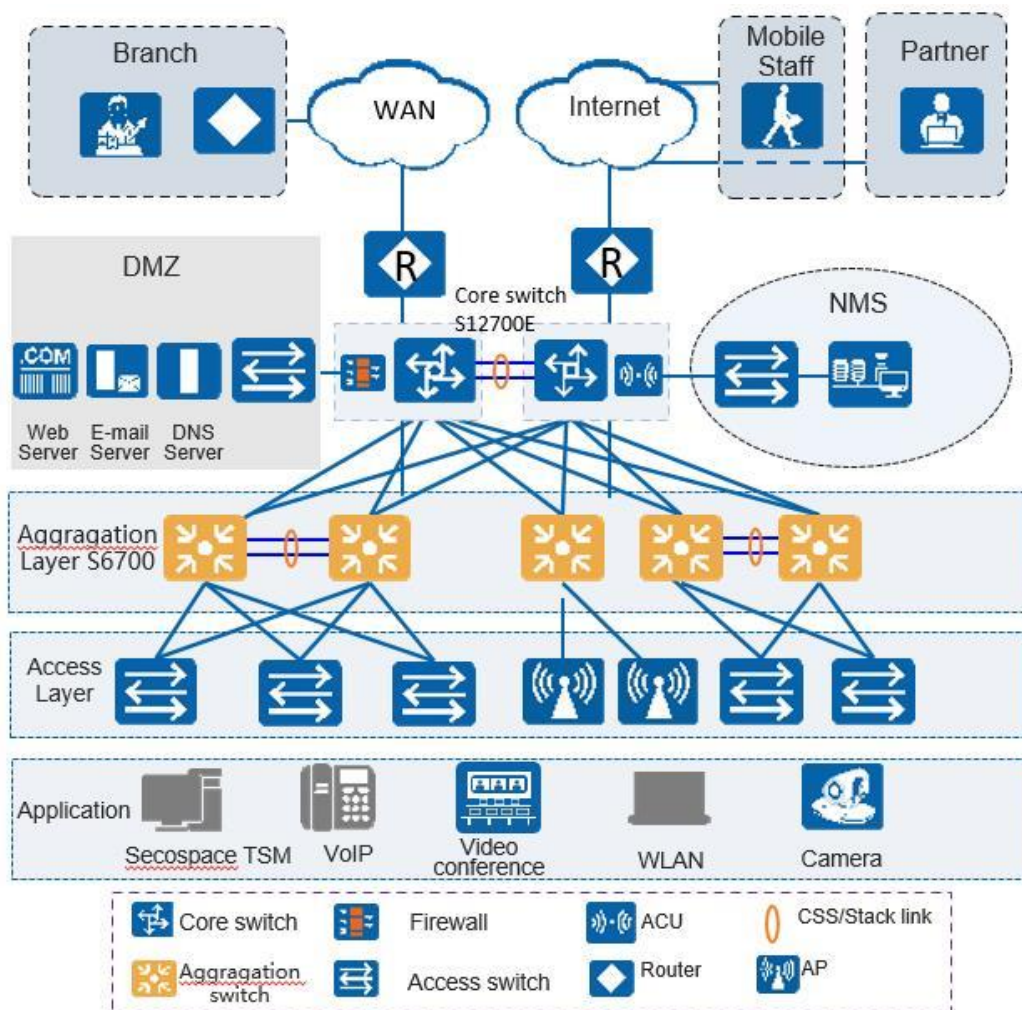
Feature	Description
	Binding of the IP address, MAC address, port number, and VLAN ID Port isolation, port security, and sticky MAC MAC Forced Forwarding (MFF) Blackhole MAC address entries Limit on the number of learned MAC addresses IEEE 802.1X authentication and limit on the number of users on a port AAA authentication, RADIUS authentication, and HWTACACS authentication NAC SSH V2.0 HTTPS CPU protection Blacklist and whitelist Attack source tracing and punishment for IPv6 packets such as ND, DHCPv6, and MLD packets IPsec for management packet encryption ECA Deception MACSec
Reliability	LACP E-Trunk Ethernet OAM (IEEE 802.3ah and IEEE 802.1ag) ITU-Y.1731 DLDP LLDP BFD for BGP, BFD for IS-IS, BFD for OSPF, BFD for static routes
VXLAN	VXLAN L2 and L3 gateways Centralized and distributed gateway BGP-EVPN Configured through the NETCONF protocol
SVF	Acting as the parent node to vertically virtualize downlink switches and APs as one device for management Two-layer client architecture ASs can be independently configured. Services not supported by templates can be configured on the parent node. Third-party devices allowed between SVF parent and clients
iPCA	Marking service packets to obtain the packet loss ratio and number of lost packets in real time Measurement of the number of lost packets and packet loss ratio on networks and devices
Management and maintenance	Cloud-based management Virtual cable test SNMP v1/v2c/v3 RMON Web-based NMS System logs and alarms of different severities GVRP MUX VLAN

Feature	Description
	NetStream Telemetry

## Networking and Applications

### Large-scale Enterprise Campus Network

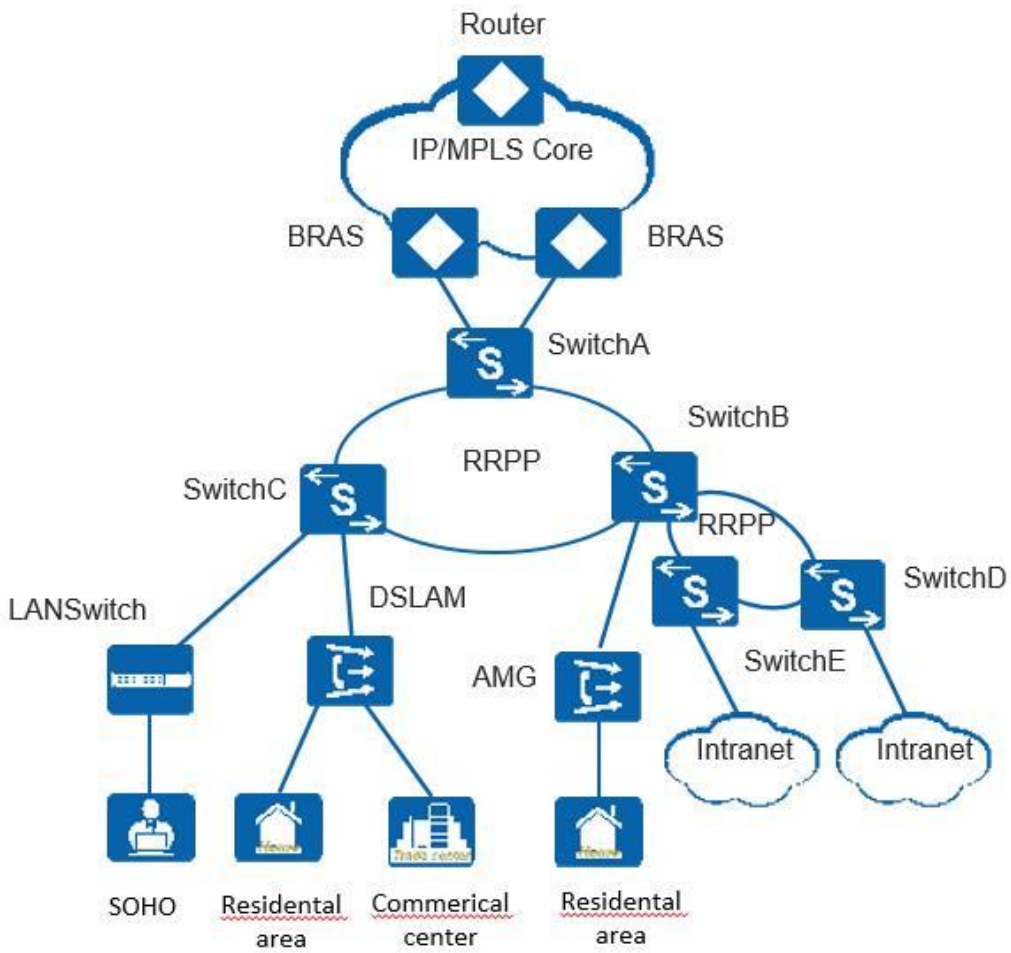
CloudEngine S6730-H series switches can be deployed at the aggregation layer of a large-scale enterprise campus network, creating a highly reliable, scalable, and manageable enterprise campus network.



### Application on a MAN

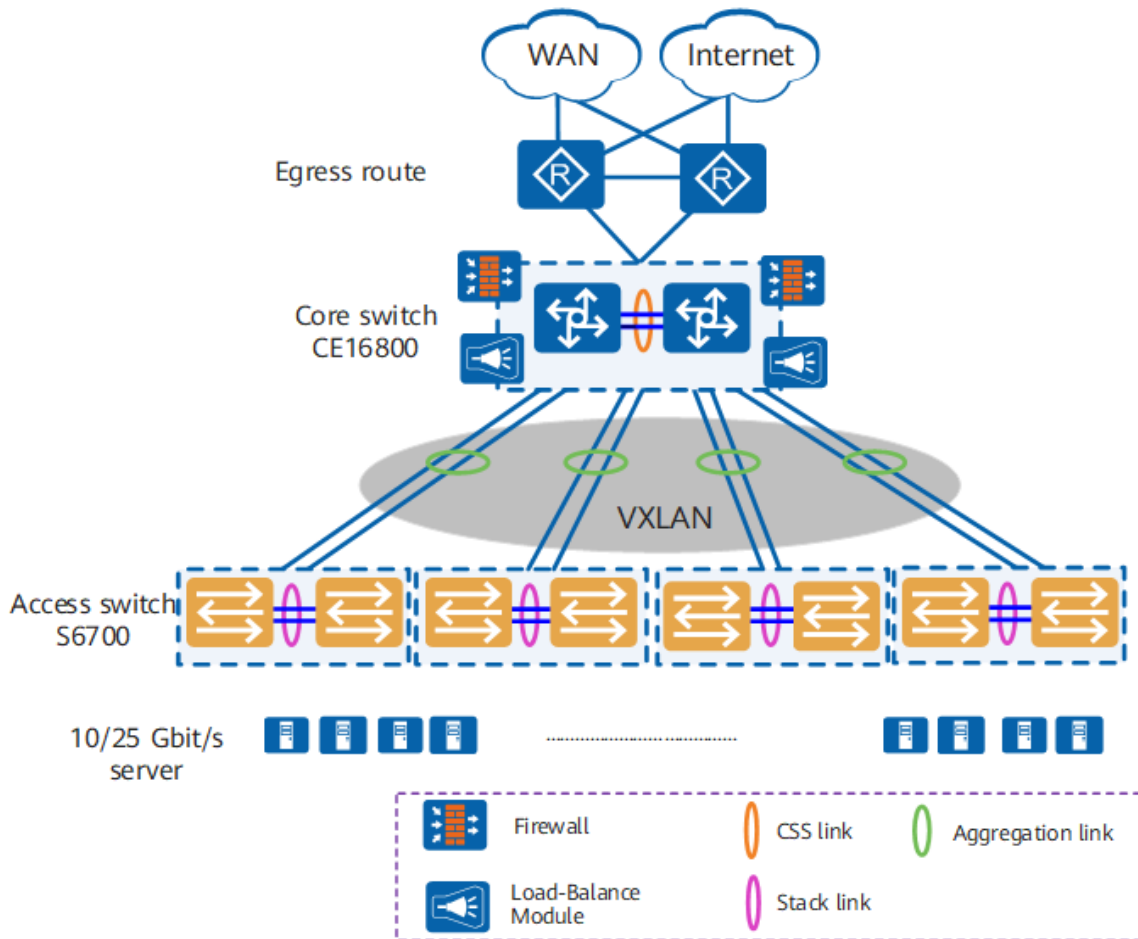
CloudEngine S6730-H series switches can be deployed at the access layer of a MAN (Metropolitan Area Network) to build a high-performance, multi-service, and highly reliable ISP MAN network.





## Data Center

CloudEngine S6730-H switches can be deployed at the access layer build a virtualized, highly reliable, non-blocking, and energy conservative data center network.



## Ordering Information

The following table lists ordering information of the CloudEngine S6730-H series switches.

Model	Product Description
CloudEngine S6730-H28Y4C	S6730-H28Y4C ( 28*25GE SFP28 ports, 4*40GE/100GE QSFP28 ports, without power module )
PAC300S12-CL	300W AC power module
PDC260S12-DL	260W DC power module

License	Product Description
N1-S67H-M-Lic	S67XX-H Series Basic SW,Per Device
N1-S67H-M-SnS1Y	S67XX-H Series Basic SW,SnS,Per Device,1Year
L-VxLAN-S67	S67 Series, VxLAN License, Per Device
L-1AP-S67	S67 Series, Wireless Access Controller AP Resource License-1AP
N1-S67H-F-Lic	N1-CloudCampus,Foundation,S67XX-H Series,Per Device
N1-S67H-F-SnS	N1-CloudCampus,Foundation,S67XX-H Series,SnS,Per Device
N1-S67H-A-Lic	N1-CloudCampus,Advanced,S67XX-H Series,Per Device
N1-S67H-A-SnS	N1-CloudCampus,Advanced,S67XX-H Series,SnS,Per Device

License	Product Description
N1-S67H-FToA-Lic	N1-Upgrade-Foundation to Advanced,S67XX-H,Per Device
N1-S67H-FToA-SnS	N1-Upgrade-Foundation to Advanced,S67XX-H,SnS,Per Device
N1-AM-30-Lic	N1-CloudCampus, Add-On Package, Access Management, Per 30 Endpoints
N1-AM-30-SnS1Y	N1-CloudCampus, Add-On Package, Access Management, Software Subscription and Support, Per 30 Endpoints, 1 Year
N1-EPNP-30-Lic	N1-CloudCampus, Add-On Package, Endpoints Plug and Play, Per 30 Endpoints
N1-EPNP-30-SnS1Y	N1-CloudCampus, Add-On Package, Endpoints Plug and Play, Software Subscription and Support, Per 30 Endpoints, 1 Year
N1-APP-X7FSwitch	N1-CloudCampus, Add-On Package, Intelligent Application Analysis, X7 Series Fixed Switch, Per Device
N1-APP-X7FSwitch-SnS1Y	N1-CloudCampus, Add-On Package, Intelligent Application Analysis, X7 Series Fixed Switch, Software Subscription and Support, Per Device, 1 Year

## More Information


For more information about Huawei Campus Switches, visit <http://e.huawei.com> or contact us in the following ways:

- Global service hotline: <http://e.huawei.com/en/service-hotline>
- Logging in to the Huawei Enterprise technical support website: <http://support.huawei.com/enterprise/>
- Sending an email to the customer service mailbox: [support\\_e@huawei.com](mailto:support_e@huawei.com)

**Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

### Trademarks and Permissions

 HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

### Huawei Technologies Co., Ltd.

Address:Huawei Industrial Base Bantian,  
Longgang Shenzhen 518129 People's  
Republic of China

Website:e.huawei.com