

CloudEngine S6730-S Series Switches


CloudEngine S6730-S series full-featured 10GE switches are Huawei's new generation fixed switches that provide 10GE downlink ports 40GE uplink ports.

Product Overview

CloudEngine S6730-S series full-featured 10 GE switches are Huawei's new generation fixed switches ,to provide 10 GE downlink ports as well as 40 GE uplink ports.

CloudEngine S6730-S can be used to provide high-speed access for 10 Gbit/s access to high-density servers or function as a core/aggregation switch on a campus network to provide 40 Gbit/s rate. In addition, CloudEngine S6730-S provides a wide variety of services, comprehensive security policies, and various QoS features to help customers build scalable, manageable, reliable, and secure campus and data center networks.

Models and Appearance

Appearance	Description
 <p>CloudEngine S6730-S24X6Q</p>	<ul style="list-style-type: none"> 24 x 10 Gig SFP+, 6 x 40 Gig QSFP+ Dual pluggable power modules, equipped power modules by default not available Forwarding performance: 490Mpps Switching capacity: 960Gbps/2.4Tbps <p>NOTE</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

- The CloudEngine S6730-S 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 " structure can be virtualized into a "super switch", greatly simplifying network management.
- The CloudEngine S6730-S 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-S 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-S series 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-S series 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-S series supports Smart Link and Virtual Router Redundancy Protocol (VRRP), which implement backup of uplinks. One CloudEngine S6730-S switch can connect to multiple aggregation switches through multiple links, significantly improving reliability of access devices.

Intelligent Stack (iStack)

- The CloudEngine S6730-S 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 capacity 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

- 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.
- The CloudEngine S6730-S 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.

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.

Big Data Powered Collaborative Security

- Agile switches use NetStream to collect campus network data and then report such data to the Huawei Cybersecurity Intelligence System (CIS). The purposes of doing so are to detect network security threats, display the security posture across the entire network, and enable automated or manual response to security threats. The CIS delivers the security policies to the Agile Controller. The Agile Controller then delivers such policies to agile switches that will handle security events accordingly. All these ensure campus network security.

- The CloudEngine S6730-S series supports Encrypted Communication Analytics (ECA). It uses built-in ECA probes to extract characteristics of encrypted streams based on NetStream sampling and Service Awareness (SA), generates metadata, and reports the metadata to Huawei Cybersecurity Intelligence System (CIS). The CIS uses the AI algorithm to train the traffic model and compare characteristics of extracted encrypted traffic to identify malicious traffic. The CIS displays detection results on the GUI, provides threat handling suggestions, and automatically isolates threats with the Agile Controller to ensure campus network security.
- The CloudEngine S6730-S series supports deception. It functions as a sensor to detect threats such as IP address scanning and port scanning on a network and lures threat traffic to the honeypot for further checks. The honeypot performs in-depth interaction with the initiator of the threat traffic, records various application-layer attack methods of the initiator, and reports security logs to the CIS. The CIS analyzes security logs. If the CIS determines that the suspicious traffic is an attack, it generates an alarm and provides handling suggestions. After the administrator confirms the alarm, the CIS delivers a policy to the Agile Controller. The Agile Controller delivers the policy to the switch for security event processing, ensuring campus network security.

Intelligent O&M

- The CloudEngine S6730-S series provides telemetry technology to collect device data in real time and send the data to Huawei campus network analyzer 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.
- The CloudEngine S6730-S series 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 CloudEngine S6730-S series 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.

Product Specifications

Item	CloudEngine S6730-S24X6Q
Fixed ports	24 x 10 Gig SFP+, 6 x 40 Gig QSFP+
Dimensions (W x D x H)	442 mm x 420 mm x 43.6 mm
Chassis height(U)	1U
Input voltage	AC Power <ul style="list-style-type: none"> • Rated AC voltage: 100V to 240V AC; 50/60 Hz • Max. AC voltage: 90V to 290V AC; 45–65 Hz DC Power <ul style="list-style-type: none"> • Rated DC voltage: –48V~–60V • Max. DC voltage: -38.4V DC~-72V DC
Input current	AC 600W: Max 8A DC 1000W: Max 30A
Maximum power consumption	225W (220V input) 249W (90V input)

Item	CloudEngine S6730-S24X6Q
Minimum power consumption	88W
Operating temperature	<ul style="list-style-type: none"> 0–1800 m altitude: -5°C to 45°C 1800–5000 m altitude: The operating temperature reduces by 1°C every time the altitude increases by 220 m.
Storage temperature	-40-70°C
Operating altitude	5000 m
Noise (sound pressure at normal temperature)	52dB(A)
Surge protection specification	AC power interface: differential mode: $\pm 6\text{kV}$; common mode: $\pm 6\text{kV}$ DC power interface: differential mode: $\pm 2\text{kV}$; common mode: $\pm 4\text{kV}$
Power supply type	600W AC Power 1000W DC Power
Relative humidity	5% to 95% (non-condensing)
Fans	4 , Fan modules are pluggable
Heat dissipation	Heat dissipation with fan, intelligent fan speed adjustment

Service Features

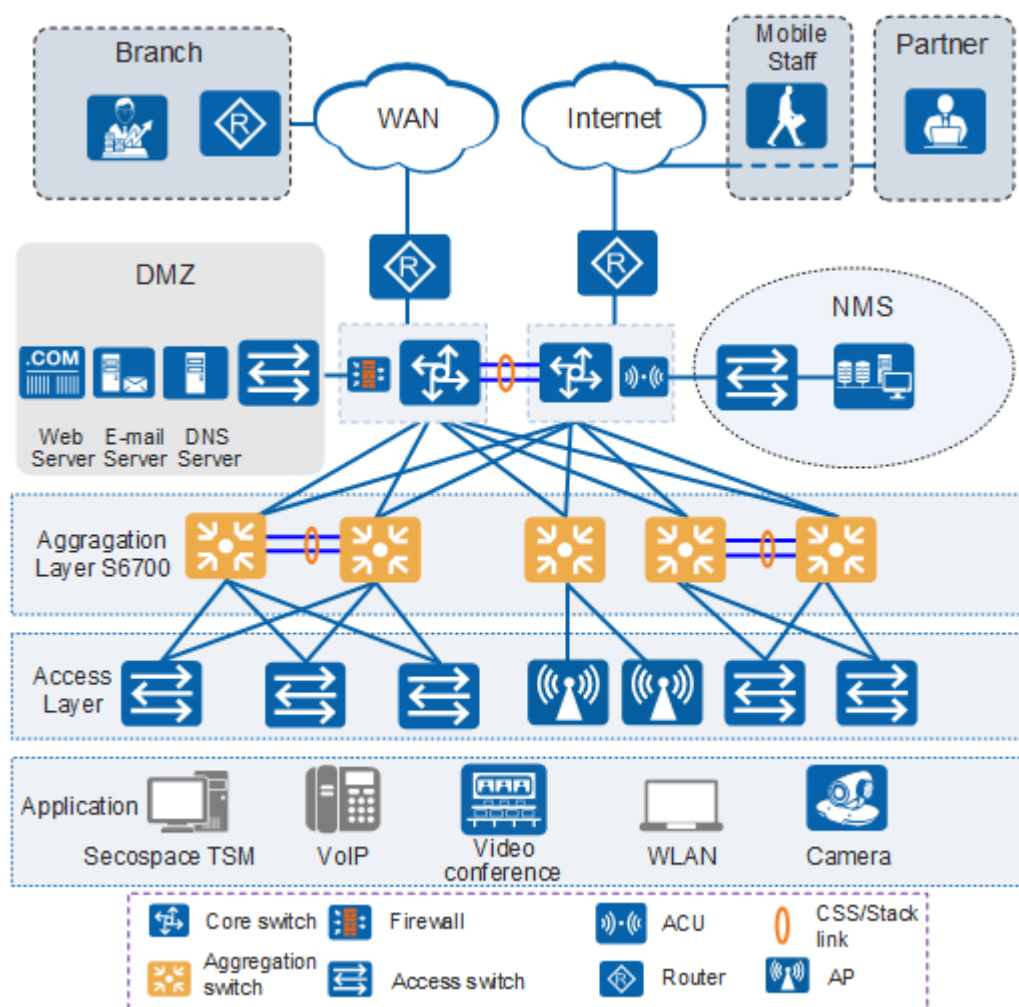
Feature	Description
MAC	Up to 64K MAC address entries IEEE 802.1d standards compliance MAC address learning and aging Static, dynamic, and blackhole MAC address entries Packet filtering based on source MAC addresses
VLAN	4K VLANs Guest VLANs and voice VLANs GVRP MUX VLAN VLAN assignment based on MAC 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 64K FIBv4 entries Up to 32K 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
Ethernet loop protection	RRPP ring topology and RRPP multi-instance

Feature	Description
	<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>BPDUs protection, root protection, and loop protection</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> <p>Binding of the IP address, MAC address, port number, and VLAN ID</p> <p>Port isolation, port security, and sticky MAC</p> <p>MAC Forced Forwarding (MFF)</p> <p>Blackhole MAC address entries</p> <p>Limit on the number of learned MAC addresses</p> <p>IEEE 802.1X authentication and limit on the number of users on a port</p> <p>AAA authentication, RADIUS authentication, and HWTACACS authentication</p> <p>NAC</p> <p>SSH V2.0</p>

Feature	Description
	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
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 functions, VXLAN L2 and L3 gateways, BGP EVPN VXLAN configuration using NETCONF/YANG
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/v2/v3 RMON Web-based NMS System logs and alarms of different severities GVRP MUX VLAN NetStream Telemetry

Networking and Applications

The CloudEngine S6730-S series switches can be used as access or aggregation switches on small- and medium-sized campus networks and provide 10G ports for high-speed access, meeting the requirement for increasing bandwidth. The rich service features and comprehensive security mechanisms make the CloudEngine S6730-S cost effective on campus networks.



Ordering Information

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

Model	Product Description
CloudEngine S6730-S24X6Q	CloudEngine S6730-S24X6Q(24 x 10 Gig SFP+, 6 x 40 Gig QSFP+. equipped power modules by default not available)
N1-S67S-M-Lic	S67 Series Basic SW,Per Device
N1-S67S-M-SnS1Y	S67 Series Basic SW,SnS,Per Device,1Year
PAC600S12-CB	600W AC power module
PDC1000S12-DB	1000W DC power module

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

Copyright © Huawei Technologies Co., Ltd. 2019. 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