S6700 Series 10G Switches

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

S6700 Series 10G Switches

Product Overview

The S6700 series switches (S6700s) are next-generation 10G box switches. The S6700 can function as an access switch in an Internet data center (IDC) or a core switch on a campus network.

The S6700 has industry-leading performance and provides up to 24 or 48 line-speed 10GE ports. It can be used in a data center to provide 10 Gbit/s access to servers or function as a core switch on a campus network to provide 10 Gbit/s traffic aggregation. In addition, the S6700 provides a wide variety of services, comprehensive security policies, and various QoS features to help customers build scalable, manageable, reliable, and secure data centers. The S6700 is available in two models: S6700-48-EI and S6700-24-EI.

Product Appearance

S6700-48-EI

- Forty-eight GE SFP or 10 GE SFP+ ports
- Double swappable AC/DC power supplies
- USB port
- Forwarding performance: 720 Mpps
- Switching capacity: 960 Gbps

S6700-24-EI

- Twenty-four GE SFP or 10 GE SFP+ ports
- Double swappable AC/DC power supplies
- USB port
- Forwarding performance: 360 Mpps
- Switching capacity: 960 Gbps

Product Features

Large-capacity, high-density, 10 Gbit/s access

- To provide sufficient bandwidth for users, many servers, particularly those in data centers, use 10G network adapters. The S6700 can be used in data centers to provide high forwarding performance and 10GE ports. The S6700 has the high density of all 10GE ports and the large switching capacity. Each S6700 provides a maximum of 48 line-speed 10GE ports.
- S6700 ports support 1GE and 10GE access and can identify optical module types, maximizing the return on investment and allowing users to flexibly deploy services.
- The S6700 has a large buffering capacity and uses an advanced buffer scheduling mechanism to ensure non-block transmission when data center traffic volume is high.

Comprehensive security policies

- The S6700 provides multiple security measures to defend against Denial of Service (DoS) attacks, as well as attacks against networks or users. DoS attack types include SYN Flood attacks, Land attacks, Smurf attacks, and ICMP Flood attacks. Attacks to networks refer to STP BPDU/root attacks. Attacks to users include bogus DHCP server attacks, man-in-the-middle attacks, IP/MAC spoofing attacks, and DHCP request flood attacks. DoS attacks that change the CHADDR field in DHCP packets are also attacks against users.
- The S6700 supports DHCP snooping, which discards invalid packets that do not match any binding entries, such as ARP spoofing packets and IP spoofing packets. This prevents hackers from using ARP packets to initiate attacks on campus networks. The interface connected to a DHCP server can be configured as a trusted interface to protect the system against bogus DHCP server attacks.
- The S6700 supports strict ARP learning, which prevents ARP spoofing attacks that exhaust ARP entries. The S6700 also provides an IP source check to prevent DoS attacks caused by MAC address spoofing, IP address spoofing, and MAC/IP spoofing. URPF, provided by the S6700, authenticates packets by checking the packet transmission path in reverse, which can protect the network against source address spoofing attacks.
- The S6700 supports centralized MAC address authentication and 802.1x authentication. The S6700 authenticates users based on statically or dynamically bound user information such as the user name, IP address, MAC address, VLAN ID, access interface, and flag indicating whether antivirus software is installed. VLANs, QoS policies, and ACLs can be dynamically applied to users.
- The S6700 can limit the number of MAC addresses learned on an interface to prevent attackers from exhausting MAC address entries by using bogus source MAC addresses. This function minimizes the packet flooding that occurs when users' MAC addresses cannot be found in the MAC address table.

Higher reliability mechanism

- The S6700 supports redundant power supplies. You can choose a single power supply or use two power supplies to ensure device reliability. With two fans, the S6700 has a longer MTBF time than its counterpart switches.
- The S6700 supports MSTP multi-process that enhances the existing STP, RSTP, and MSTP implementation. This function increases the number of MSTPs supported on a network. It also supports enhanced Ethernet reliability technologies such as Smart Link and RRPP, which implement millisecond-level protection switchover and ensure network reliability. Smart Link and RRPP both support multi-instance to implement load balancing among links, optimizing bandwidth usage.
- The S6700 supports the enhanced trunk (E-Trunk) feature. When a CE is dual-homed to two S6700s (PEs), E-Trunk protects the links between the CE and PEs and implements backup between the PEs. E-trunk enhances link reliability between devices.
- The S6700 supports the Smart Ethernet Protection (SEP) protocol, a ring network protocol applied to the link layer on an Ethernet network. SEP can be used on open ring networks and can be deployed on upper-layer aggregation devices to provide fast switchover (within 50 ms), ensuring the non-stop transmission of

services. SEP features simplicity, high reliability, fast switchover, easy maintenance, and flexible topology, facilitating network planning and management.

- The S6700 supports Ethernet Ring Protection Switching (ERPS), also referred to as G.8032. As the latest ring network protocol, ERPS was developed based on traditional Ethernet MAC and bridging functions and uses mature Ethernet OAM function and a ring automatic protection switching (R-APS) mechanism to implement millisecond-level protection switching. ERPS supports various services and allows flexible networking, helping customers build a network with lower OPEX and CAPEX.
- The S6700 supports VRRP. Two S6700s can form a VRRP group to ensure nonstop reliable communication. Multiple equal-cost routes to upstream devices can be configured on the S6700 to provide route redundancy. When an active route is unreachable, traffic is switched to a backup route.

Enhanced QoS control mechanism

- The S6700 implements complex traffic classification based on packet information, such as the 5-tuple, IP preference, ToS, DSCP, IP protocol type, ICMP type, TCP source port, VLAN ID, Ethernet protocol type, and CoS. ACLs can be applied to inbound or outbound directions on an interface. The S6700 supports a flow-based two-rate three-color CAR. Each port supports eight priority queues, multiple queue scheduling algorithms, such as WRR, DRR, SP, WRR+SP, and DRR+SP, and WRED, a congestion avoidance algorithm. All of these features ensure high-quality voice, video, and data services.

High scalability

- The S6700 supports the iStack function, which allows switches that are far apart to form a stack. A port on the S6700 can be configured as a stack port using a command for flexible stack deployment. The distance between stacked switches is further increased when the switches are connected with optical fibers. A stack is easier to expand, is more reliable, and has a higher performance rate than a single switch. New member switches can be added to a stack without interrupting services when the system capacity needs to be increased or a member switch fails. Compared with the stacking of chassis-shaped switches, the iStack function can increase system capacity and port density without being restricted by hardware. Multiple devices in a stack can function as one logical device, which simplifies network management and configuration.

Convenient management

- The S6700 supports automatic configuration, plug-and-play, deployment using a USB flash drive, and batch remote upgrades. These capabilities simplify device management and maintenance and reduce maintenance costs.
- The S6700 supports SNMP v1/v2c/v3 and provides flexible methods for managing devices. Users can manage the S6700 using the CLI and Web NMS. The NQA function assists users with network planning and upgrades. In addition, the S6700 supports NTP, SSH v2, HWTACACS, RMON, log hosts, and port-based traffic statistics.
- The S6700 supports GARP VLAN Registration Protocol (GVRP), which dynamically distributes, registers, and propagates VLAN attributes to reduce network administrator workloads and ensure correct VLAN configuration. In a complex network topology, GVRP simplifies VLAN configuration and reduces network communication faults caused by incorrect VLAN configuration.

- The S6700 supports Multiplex VLAN (MUX VLAN). MUX VLAN isolates Layer 2 traffic between interfaces in a VLAN. Interfaces in a subordinate separate VLAN can communicate with ports in the principal VLAN, but cannot communicate with each other. MUX VLAN is typically used on an enterprise intranet to isolate user interfaces from each other while still allowing them to communicate with server interfaces. This function prevents communication between network devices connected to certain interfaces or interface groups, but allows these devices to communicate with the default gateway.
- The S6700 supports BFD, which provides millisecond-level fault detection for protocols, such as OSPF, IS-IS, VRRP, and PIM, to improve network reliability. Complying with IEEE 802.3ah and 802.1ag, the S6700 supports point-to-point Ethernet fault management and can detect faults in the last mile of an Ethernet link to users. Ethernet OAM improves Ethernet network management and maintenance capabilities and ensures a stable network.

Various IPv6 features

- The S6700 supports IPv4/IPv6 dual stack and can migrate from an IPv4 network to an IPv6 network. S6700 hardware supports IPv4/IPv6 dual stack, IPv6 over IPv4 tunnels (including manual tunnels, 6to4 tunnels, and ISATAP tunnels), and Layer 3 line-speed forwarding. The S6700 can be deployed on IPv4 networks, IPv6 networks, or networks that run both IPv4 and IPv6. This makes networking flexible and enables a network to migrate from IPv4 to IPv6.
- The S6700 supports various IPv6 routing protocols, including RIPng and OSPFv3. The S6700 uses the IPv6 Neighbor Discovery Protocol (NDP) to manage packets exchanged between neighbors. It also provides a path MTU (PMTU) discovery mechanism to select a proper MTU on the path from the source to the destination, optimizing network resource utilization and obtaining the maximum throughput.

Product Specifications

Item	S6700-24-EI	S6700-48-EI
Port	24* GE SFP/10 GE SFP+ ports	48* GE SFP/10 GE SFP+ ports
MAC address table	128 K MAC address entries MAC address learning and aging Static, dynamic, and blackhole MAC address entries Packet filtering based on source MAC addresses	
VLAN	4 K VLANs Guest VLAN and voice VLAN VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports 1:1 and N:1 VLAN Mapping QinQ and selective QinQ	
IPv4 routing	Static routing, RIPv1, RIPv2, ECMP, and URPF OSPF, IS-IS, and BGP VRRP Policy-based routing Routing policy	

Item	S6700-24-EI	S6700-48-EI
IPv6 routing	Static route RIPng OSPFv3 BGP4+	
IPv6 features	Neighbor Discovery (ND) PMTU IPv6 ping, IPv6 tracert, and IPv6 Telnet 6to4 tunnel, ISATAP tunnel, and manually configured tunnel ACLs based on the source IPv6 address, destination IPv6 address, Layer 4 ports, or protocol type MLD v1/v2 snooping	
multicast	Static Layer 2 multicast MAC address MAC-based multicast forwarding IGMP snooping and IGMP fast leave Multicast VLAN MLD snooping IGMP proxy Controllable multicast Port-based multicast traffic statistics IGMP v1/v2/v3 PIM-SM, PIM-DM, and PIM-SSM MSDP	
QoS/ACL	Rate limiting on packets sent and received by an interface Packet redirection Port-based traffic policing and two-rate three-color CAR Eight queues on each port WRR, DRR, SP, WRR+SP, and DRR+SP queue scheduling algorithms Re-marking of the 802.1p priority and DSCP priority 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, port number, protocol type, and VLAN ID Rate limiting in each queue and traffic shaping on ports	
Reliability	STP(IEEE 802.1d), RSTP(IEEE 802.1w), and MSTP(IEEE 802.1s) BPDU protection, root protection, and loop protection RRPP ring topology and RRPP multi-instance Smart Link tree topology and Smart Link multi-instance, providing the millisecond-level protection switchover SEP ERPS(G.8032) BFD for OSPF, BFD for IS-IS, BFD for VRRP, and BFD for PIM E-Trunk	
MPLS features	MPLS L3VPN MPLS L2VPN (VPWS/VPLS) MPLS-TE MPLS QoS	

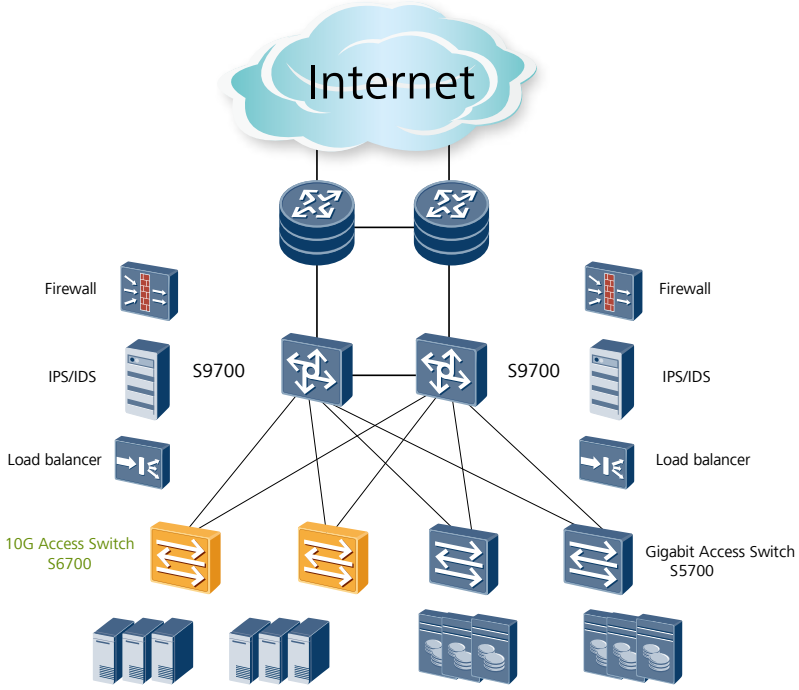
Item	S6700-24-EI	S6700-48-EI
Security	DoS attack defense, ARP attack defense, and ICMP attack defense 802.1x authentication and limit on the number of users on an interface AAA authentication, RADIUS authentication and TACACS authentication SSH v2.0 Hypertext Transfer Protocol Secure (HTTPS) CPU defense Blacklist and whitelist	
Management and maintenance	iStack (using service ports as stack ports) MAC Forced Forwarding (MFF) Virtual cable test Ethernet OAM (IEEE 802.3ah and 802.1ag) SNMP v1/v2c/v3 RMON Web NMS System logs and alarms of different levels GVRP MUX VLAN sFlow	
Interoperability	Supports VBST (Compatible with PVST/PVST+/RPVST)	
	Supports LNP (Similar to DTP)	
	Supports VCMP (Similar to VTP)	
Operating environment	Operating temperature: 0°C–45°C Relative humidity: 5%–95% (non-condensing)	
Input voltage	AC: Rated voltage range: 100 V to 240 V AC, 50/60 Hz Maximum voltage range: 90 V to 264 V AC, 50/60 Hz DC: Rated voltage range: –48 V to –60 V, DC Maximum voltage range: –36 V to –72 V, DC	
Dimensions (W x D x H)	442 mm x 420 mm x 43.6 mm	
Power consumption	153W	240W

Applications

Data Centers

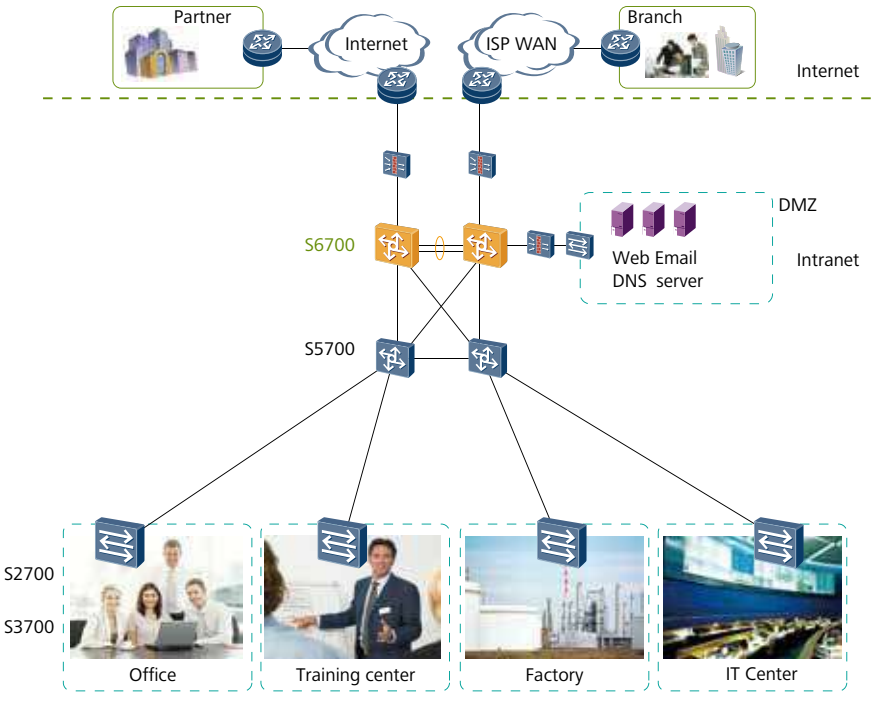
The S6700 can be used in Huawei's sustainable data center solution, which offers four major advantages: evolution, availability, pooling, and visualization.

As shown in the following figure, the S9700 Terabit routing switches function as core switches in a data center and use firewall and load balancer boards to ensure security and load balancing. The S6700 functions as an access switch and provides high-density 10GE ports to connect to 10G servers.



Campus Networks

The S6700 can function as a core switch on a campus network and provide high-density line-speed 10GE ports, rich service features, and comprehensive security mechanisms. This makes the S6700 a cost-effective option.



For more information, visit http://enterprise.huawei.com or contact the Huawei local sales office.

HUAWEI TECHNOLOGIES CO.,LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129,P.R.China
Tel: +86 755 28780808

www.huawei.com