

S6300 Switches





Product Overview

S6300 switches (S6300 for short) are next-generation box-shaped 10-gigabit switches developed by Huawei for accessing 10-gigabit servers in a data center and converging devices on a Metropolitan Area Network (MAN) or campus network.

The S6300, one of the best-performance switches in the industry, provides a maximum of 24/48 full-line-speed 10-gigabit interfaces, which gives possibility to high-density access of 10-gigabit servers in a data center and high-density convergence of 10-gigabit devices on a campus network. In addition, the S6300 provides diversified features, perfect security control measures, and multiple QoS control modes to meet the requirements of data centers for expansibility, reliability, manageability, and security.

Product Appearance

At present, the S6300 offers two models.

S6348-EI



- S6348-EI: provides 48 GE SFP or 10GE SFP+ ports, two power supply slots, and one USB interface; supports AC power supplies.

S6324-EI



- S6324-EI: provides 24 GE SFP or 10GE SFP+ ports, two power supply slots, and one USB interface; supports AC power supplies.



Product Features

Large-Capacity High-Density 10-Gigabit Access

- The increasing bandwidth on the users' side and wide application of 10-gigabit network adapters on servers require the switches in the data centers to provide better forwarding capability and 10-gigabit port expandability. The S6300 provides the most 10-gigabit ports and the largest switching capacity among similar switches in the industry. A single S6300 can provide a maximum of forty-eight 10-gigabit ports for line-speed forwarding.
- The S6300 supports GE access and 10GE access, can automatically identify the type of the installed optical module. This protects the investment of customers and ensures flexible usage to the greatest degree.
- To meet the requirement for non-blocking data transmission under heavy traffic in data centers, the S6300 provides powerful caching capability and supports the advanced caching scheduling mechanism to ensure the optimized use of the caching capability.

Perfect Security Control

- The S6300 provides various security protection measures. It can defend against Denial of Service (DoS) attacks, attacks to networks, and attacks to users. DoS attacks 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, DHCP request flood attacks, and DoS attacks by changing the CHADDR field of packets.
- The S6300 listens to the MAC/IP address, address lease, VLAN ID, and port number about a DHCP user by establishing and maintaining a DHCP snooping binding table. In this way, IP addresses and access ports of DHCP users can be tracked. The S6300 directly discards invalid packets that do not match binding entries, such as ARP spoofing packets and packets with bogus IP addresses, to prevent hackers or attackers from initiating man-in-the-middle attacks to campus networks by using ARP packets. The trusted port feature of DHCP snooping is used to ensure the validity of the DHCP server.
- The S6300 supports strict ARP learning to prevent ARP spoofing attackers from exhausting ARP entries so that authorized users can connect to the Internet. It also supports IP source check to prevent DoS attacks caused by MAC address spoofing, IP address spoofing, and MAC/IP address spoofing. The URPF function provided by the S6300 can check packet transmission paths to authenticate the packets received, which can protect the network against the spread of source address spoofing attacks.
- The S6300 supports centralized MAC address authentication and 802.1x authentication. User information such as the user account, IP address, MAC address, VLAN ID, access port number, and flag indicating whether antivirus software is installed on the client can be bound statically or dynamically, and user policies (VLAN, QoS, and ACL) can be delivered dynamically.
- The S6300 can limit the number of source MAC addresses learned on a port to prevent attackers from exhausting MAC address entries by using bogus source MAC addresses. In this way, MAC addresses of authorized users can be learned and flooding is prevented.

High Reliability

- The S6300 supports dual power supplies for backup. Users can select a single power supply or dual power supplies to improve device reliability. The switch provides two fans to improve operating stability and has a long MTBF.
- Enhancing STP, RSTP, and MSTP, the S6300 supports MSTP multi-process which greatly increases the number of subrings. It supports enhanced Ethernet technologies such as Smart Link and RRPP to implement millisecond-level protective link switchover, improving network reliability. In addition, the S6300 supports multi-instance for Smart Link and RRPP to implement load balancing among links, further improving bandwidth usage.
- The S6300 supports Enhanced Trunk (E-Trunk). When a CE is dual homed to a VPLS, VLL, or PWE3 network, E-Trunk can be configured to protect the links between the CE and PEs and implement protective switchover between PEs. The E-Trunk technology can implement link aggregation across devices to upgrade the link reliability to device level.
- The S6300 supports the Smart Ethernet Protection (SEP) protocol, a ring network protocol applied to the link layer of an Ethernet network. SEP is applicable to open ring networks and can be deployed independently from the upper-layer aggregation devices to provide millisecond-level switchover without interrupting services. Huawei devices have implemented Ethernet link management by using SEP. SEP features simplicity, high reliability, high switchover performance, convenient maintenance, and flexible topology, enabling customers to manage and deploy networks conveniently.
- The S6300 supports VRRP to keep the communication continuity and reliability, ensuring a stable network. Multiple equal-cost routes can be configured on the S6300 to implement route redundancy. When the active uplink route is faulty, traffic is automatically switched to a backup route. This feature implements multi-level backup for uplink routes.

Diversified QoS Control

- The S6300 supports multiple QoS control modes. It can implement complex traffic classification based on information such as the five-tuple, IP priority, ToS, DSCP, IP protocol type, ICMP type, TCP source port number, VLAN ID, Ethernet frame protocol type, and CoS. The S6300 supports inbound and outbound ACLs. The S6300 supports flow-based two-rate three-color CAR. Each port supports eight priority queues, WRED congestion prevention mechanism, and multiple queue scheduling algorithms such as WRR, DRR, SP, WRR+SP, and DRR+SP. This ensures the quality of voice, video and data services.

Good Expansibility

- The S6300 supports long-distance Intelligent Stacking (iStack). A common port can be configured as a stacking port by using command lines to meet different requirements. Compared with traditional stacking, stacking by using optical fiber can greatly increase the stacking distance. Compared with a single device, iStack features powerful expansibility, reliability, and performance. When customers need to expand the device or replace a single faulty device, they can add new devices without stopping services. Compared with chassis switches, the performance and port density of iStack are not restricted by the hardware structure. Multiple stacked devices can be logically considered as a single device, which simplifies the network management and configuration.

Easy Deployment and Maintenance

- The S6300 supports automatic configuration, plug-and-play, deployment from USB devices, and batch remote upgrade. Deployment, upgrade, and service provisioning of the S6300 can be completed at a time, which simplifies subsequent management and maintenance. Therefore, maintenance costs are greatly reduced.
- The S6300 supports diversified management and maintenance modes such as SNMP v1/v2/v3, CLI, Web network management, Telnet, and HGMP, which make device management more flexible. In addition, the S6300 supports NTP, SSH v2, HWTACACS, RMON, multiple log hosts, port-based traffic statistics, and NQA, which help to better deploy and reconstruct networks.
- The S6300 supports the GARP Registration Protocol (GVRP). The GVRP technology implements dynamic configuration of VLANs. In a complex networking environment, GVRP can simplify VLAN configuration and reduce network communication faults caused by incorrect configuration of VLANs. This reduces the manual configurations of network administrators and ensures correct VLAN configurations.
- The S6300 supports MUX VLAN. MUX VLAN is used to isolate Layer-2 traffic between ports on a VLAN. All subordinate VLANs can communicate with the principal VLAN but cannot communicate with each other. MUX VLAN is usually used on enterprise intranets. With this function, a user port can communicate with a server port but cannot communicate with other user ports. MUX VLAN prevents communication between network devices connected to some interfaces or interface groups but allows these devices to communicate with the default gateway. This function ensures resource sharing and secure communication in an enterprise.
- The S6300 supports BFD and provides millisecond-level detection for protocols such as OSPF, IS-IS, VRRP, and PIM to improve network reliability. Complying with IEEE 802.3ah and 802.1ag, the S6300 supports point-to-point Ethernet fault management to detect faults on user links. Ethernet OAM improves the network management and maintenance capabilities on the Ethernet and ensures a stable network.

Various IPv6 Features

- The S6300 supports the IPv4/IPv6 protocol stack and can be upgraded smoothly. The S6300 hardware supports both IPv4 and IPv6, IPv6 over IPv4 tunnels (including manual tunnels, 6-to-4 tunnels, and ISATAP tunnels), and Layer-3 line-speed forwarding. Therefore, the S6300 can be deployed on IPv4 networks, IPv6 networks, and networks that run IPv4 and IPv6 simultaneously. This makes the networking flexible and meets the requirements for the network transition from IPv4 to IPv6.
- The S6300 supports various IPv6 routing protocols including RIPng and OSPFv3. It uses the IPv6 Neighbor Discovery Protocol (NDP) to manage packets exchanged between neighboring nodes. The S6300 supports the Path MTU Discovery (PMTU) mechanism. That is, it selects a proper MTU on the path from the source to the destination to optimize network resource usage and obtain the maximum throughput.



Product Specifications

Item	S6324-EI	S6348-EI
Port	S6324-EI: 24 GE SFP ports or 10GE SFP+ ports	S6348-EI: 48 GE SFP ports or 10GE SFP+ ports
Forwarding performance	358 Mpps	715 Mpps
switching capacity	480 Gbit/s	960 Gbit/s
MAC address table	Supports 128 K MAC address entries. Supports automatic learning and aging of MAC addresses. Supports static, dynamic, and blackhole MAC address entries. Supports packet filtering based on source MAC addresses.	
VLAN features	Supports up to 4,096 VLANs. Supports guest VLANs and voice VLANs. Supports VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports. Supports 1:1 and N:1 VLAN switching. Supports basic QinQ and selective QinQ.	
IPv4 routing	Supports static routing, RIP v1, RIP v2, ECMP, and URPF. Supports OSPF, IS-IS, and BGP. Supports VRRP. Supports policy-based routing. Supports routing policies.	
IPv6 routing	Supports static routing. Supports RIPng. Supports manual tunnels. Supports 6-to-4 tunnels. Supports ISTAP tunnels. Supports OSPFv3.	
IPv6 features	Supports Neighbor Discovery (ND). Supports PMTU. Supports IPv6 Ping, IPv6 Tracert, and IPv6 Telnet. Supports 6-to-4 tunnels, ISATAP tunnels, and manually configured tunnels. Supports ACLs based on the source IPv6 address, destination IPv6 address, Layer-4 port, or protocol type. Supports MLD v1/v2 snooping.	
Multicast	Supports static Layer-2 multicast MAC addresses. Supports MAC-based multicast forwarding. Supports IGMP snooping and fast leave. Supports multicast VLAN. Supports MLD snooping. Supports IGMP proxy. Supports controllable multicast. Supports port-based multicast traffic statistics. Supports IGMP v1/v2/v3. Supports PIM-SM, PIM-DM, and PIM-SSM. Supports MSDP.	

Item	S6324-EI	S6348-EI
QoS/ACL	<p>Supports rate limit on packets sent and received by a port.</p> <p>Supports packet redirection.</p> <p>Supports port-based traffic policing and two-rate three-color CAR.</p> <p>Supports eight queues on each port.</p> <p>Supports multiple queue scheduling algorithms including WRR, DRR, SP, WRR+SP, and DRR+SP.</p> <p>Supports WRED.</p> <p>Supports re-marking of the 802.1p priority and DSCP priority.</p> <p>Supports packet filtering based on Layer 2 to Layer 4 information, filtering out invalid frames based on the source MAC address, destination MAC address, source IP address, destination IP address, port number, protocol, and VLAN ID.</p> <p>Supports queue-based rate limit and traffic shaping on ports.</p>	
Reliability	<p>Supports STP, RSTP, and MSTP.</p> <p>Supports BPDU protection, root protection, and loopback protection.</p> <p>Supports the RRPP ring topology and RRPP multi-instance.</p> <p>Supports the Smart Link tree topology and Smart Link multi-instance to implement millisecond-level protective switchover between active and standby links.</p> <p>Supports SEP.</p> <p>Supports BFD for OSPF, BFD for IS-IS, BFD for VRRP, and BFD for PIM.</p> <p>Supports E-Trunk.</p>	
Security	<p>Supports hierarchical user management and password protection.</p> <p>Supports DoS attack defense, ARP attack defense, and ICMP attack defense.</p> <p>Supports binding of the IP address, MAC address, port number, and VLAN ID.</p> <p>Supports port isolation, port security, and sticky MAC.</p> <p>Supports blackhole MAC addresses.</p> <p>Supports limit on the number of MAC addresses to be learned.</p> <p>Supports IEEE 802.1x authentication and the limit on the maximum number of users on a port.</p> <p>Supports multiple authentication methods including AAA, RADIUS, HWTACACS, and NAC.</p> <p>Supports SSH v2.</p> <p>Supports HTTPS.</p> <p>Supports CPU protection.</p> <p>Supports blacklisting and whitelisting.</p>	
Management and maintenance	<p>Supports intelligent stacking (implemented by service ports).</p> <p>Supports MAC Forced Forwarding (MFF).</p> <p>Supports Virtual Cable Test (VCT).</p> <p>Supports Ethernet OAM (IEEE 802.3ah and 802.1ag).</p> <p>Supports local port mirroring, Remote Switched Port Analyzer (RSPAN), and packet forwarding on an observing port.</p> <p>Supports remote configuration and maintenance by using Telnet.</p> <p>Supports SNMP v1/v2/v3.</p> <p>Supports RMON.</p> <p>Supports the Network Management System (NMS) and Web management.</p> <p>Supports HGMP.</p> <p>Supports system logs and multi-level alarms.</p> <p>Supports GVRP.</p> <p>Supports MUX VLAN.</p> <p>Supports 802.3az (Energy Efficient Ethernet).</p>	
Operating environment	<p>Operating temperature: 0 ° C to 45 ° C (long term); -5 ° C to 50 ° C (short term);</p> <p>relative humidity: 10% to 90% (non-condensing)</p>	

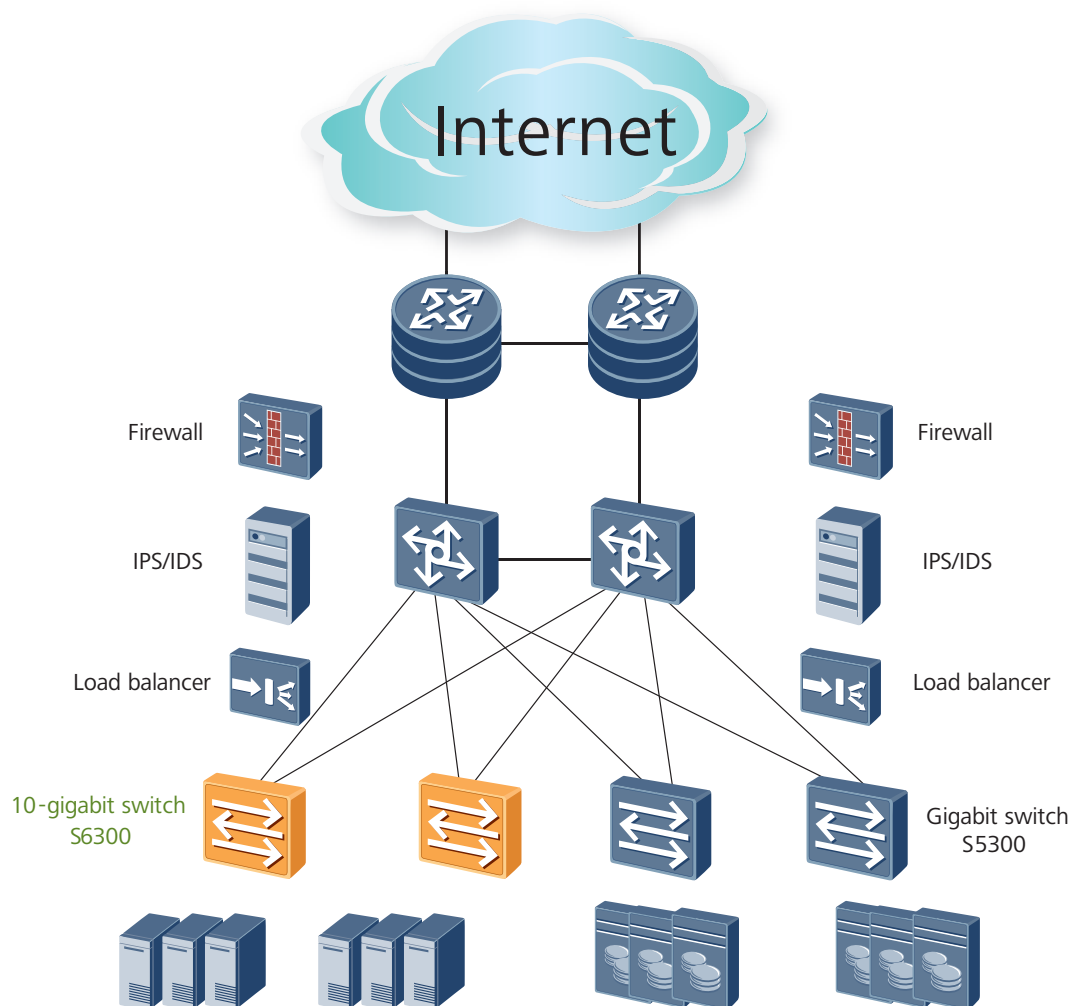
Item	S6324-EI	S6348-EI
Input voltage	AC: Rated voltage: 100 V to 240 V, 50/60 Hz Maximum voltage: 90 V to 264 V, 50/60 Hz	
Dimensions: width x depth x height	442 mm x 420 mm x 43.6 mm	
Power consumption	165 W	237 W

Applications

Application in Data Centers

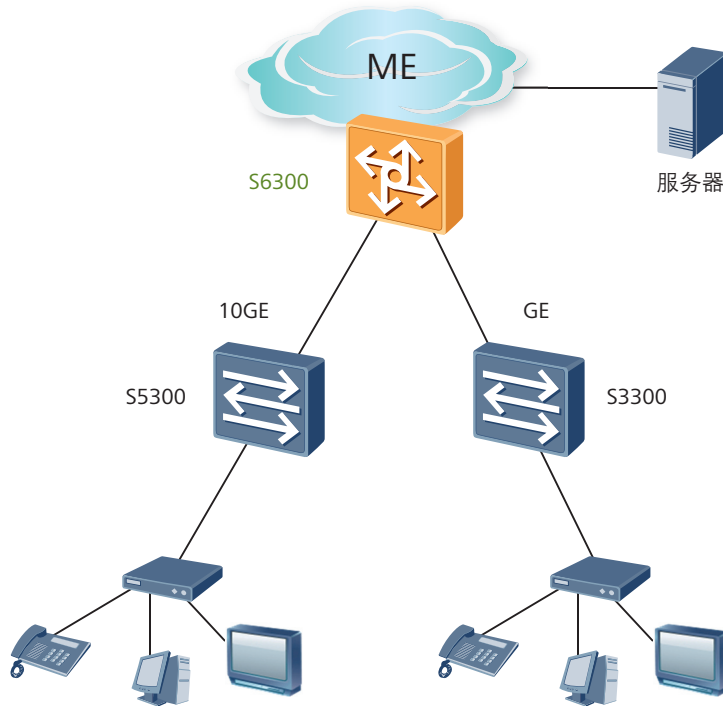
Huawei proposes a data center network solution complying with Huawei's core concept of sustainable development to tackle the severe challenge for networks in the data center era.

As shown in the following figure, the T-bit router S9300 serves as the core of the data center, and its integrated firewall and load sharing cards are used to ensure security and balance load. The S6300 supports high-density access of 10-gigabit servers.



Application in MAN

The S6300 is applicable to MAN convergence. It provides industry-leading high-density 10-gigabit ports to meet the increasing bandwidth demand. Abundant features and perfect security control mechanisms enable the S6300 to be the most cost-effective choice for MAN convergence.



Order Information

Product Description
S6324-EI
S6348-EI
AC power supply
10GE-SFP+ Optical Module
Optical module, SFP+, 10GE, multimode modules (850 nm, 0.3 km, LC)
Optical module, SFP+, 10 Gbit/s, single-mode modules (1310 nm, 10 km, LC)
Optical module, SFP+, 10 Gbit/s, single-mode modules (1310 nm, 40 km, LC)
GE-SFP Optical Module
Optical module, ESFP, GE, multimode modules (850 nm, 0.5 km, LC)
Optical module, SFP, GE, single-mode modules (1310 nm, 10 km, LC)
Optical module, eSFP, GE, single-mode modules (1310 nm, 40 km, LC)
Optical module, eSFP, GE, single-mode modules (1550 nm, 40 km, LC)
Optical module, eSFP, GE, single-mode modules (1550 nm, 80 km, LC)
Optical module, ESFP, GE, single-mode modules (1550 nm, 100 km, LC)

For more information, visit www.huawei.com or contact the local sales office of Huawei.




Copyright © Huawei Technologies Co., Ltd. 2011. 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.

Trademark Notice



HUAWEI, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned are the property of their respective owners.

NO WARRANTY

THE CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO CASE SHALL HUAWEI TECHNOLOGIES CO., LTD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, BUSINESS, REVENUE, DATA, GOODWILL OR ANTICIPATED SAVINGS ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS MANUAL.

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808

www.huawei.com