

# S5700S-LI Series Gigabit Enterprise Switches





# S5700S-LI Series Gigabit Enterprise Switches

## Product Overview

The S5700S-LI series gigabit enterprise switches (S5700S-LI for short) are next-generation energy-saving switches developed by Huawei to meet the demand for high-bandwidth access and Ethernet multi-service aggregation. Based on the cutting-edge hardware and Huawei Versatile Routing Platform (VRP) software, the S5700S-LI provides a large switching capacity and high-density GE ports. The S5700S-LI is for use in various enterprise network scenarios. For example, it can function as an access or aggregation switch on a campus network, a gigabit access switch in an Internet data center (IDC), or a desktop switch to provide 1000 Mbit/s access for terminals. The S5700S-LI is easy to install and maintain, reducing workloads for network planning, construction, and maintenance. The S5700S-LI uses advanced reliability, security, and energy conservation technologies, helping enterprise customers build a next generation IT network.

## Product Appearance



- Twenty-four 10/100/1000 Base-T ports and four 1000Base-X ports
- AC power supply, supporting RPS
- Forwarding performance: 42Mpps



- Forty-eight 10/100/1000 Base-T ports and four 1000Base-X ports
- AC power supply, supporting RPS
- Forwarding performance: 78Mpps

## Product Features and highlights

### Comprehensive reliability mechanisms

- Besides STP, RSTP, and MSTP, the S5700S-LI supports enhanced Ethernet reliability technologies such as Smart Link and RRPP (Rapid Ring Protection Protocol), which implement millisecond-level protection switchover and ensure network reliability. It also provides Smart Link multi-instance and RRPP multi-instance to implement load balancing among links, optimizing bandwidth usage.
- The S5700S-LI 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 non-stop transmission of services. SEP features simplicity, high reliability, fast switchover, easy maintenance, and flexible topology, facilitating network planning and management.
- Complying with IEEE 802.3ah and 802.1ag, the S5700S-LI supports point-to-point Ethernet fault management and can detect faults in the last mile of an Ethernet link to users.

## Well-designed QoS policies and security mechanisms

- The S5700S-LI 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 direction on an interface. The S5700S-LI supports a flow-based two-rate three-color CAR. Each port supports eight priority queues and multiple queue scheduling algorithms such as WRR, DRR, PQ, WRR+PQ, and DRR+PQ. All of these ensure the quality of voice, video, and data services.
- The S5700S-LI provides multiple security measures to defend against Denial of Service (DoS) attacks, and 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, DHCP request flood attacks. DoS attacks that change the CHADDR field in DHCP packets are also attacks against users.
- The S5700S-LI supports DHCP snooping, which generates user binding entries based on MAC addresses, IP addresses, IP address leases, VLAN IDs, and access interfaces of users. DHCP snooping discards invalid packets that do not match any binding entries, such as ARP spoofing packets and IP spoofing packets. This prevents man-in-the-middle attacks to campus networks that hackers initiate by using ARP packets. The interface connected to a DHCP server can be configured as a trusted interface to protect the system against bogus DHCP server attacks.
- The S5700S-LI supports strict ARP learning, which prevents ARP spoofing attacks that will exhaust ARP entries. It also provides IP source check to prevent DoS attacks caused by MAC address spoofing, IP address spoofing, and MAC/IP spoofing.
- The S5700S-LI supports centralized MAC address authentication, 802.1x authentication, and NAC. It 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 applied to users dynamically.
- The S5700S-LI 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 packet flooding that occurs when MAC addresses of users cannot be found in the MAC address table.

## Easy deployment and maintenance free

- The S5700S-LI supports automatic configuration, plug-and-play, and batch remote upgrade. These capabilities simplify device management and maintenance and reduce maintenance costs. The S5700S-LI supports SNMP v1/v2/v3 and provides flexible methods for managing devices. Users can manage the S5700S-LI using the CLI, Web NMS, Telnet, and HGMP. The NQA function helps users with network planning and upgrades. In addition, the S5700SLI supports NTP, SSH v2, HWTACACS+, RMON, log hosts, and port-based traffic statistics.

- The S5700S-LI supports GVRP (GARP VLAN Registration Protocol), which dynamically distributes, registers, and propagates VLAN attributes to reduce manual configuration workloads of network administrators and to ensure correct VLAN configuration. In a complex network topology, GVRP simplifies VLAN configuration and reduces network communication faults caused by incorrect VLAN configuration.
- The S5700S-LI supports 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 usually used on an enterprise intranet to isolate user interfaces from each other but allow them to communicate with server interfaces. This function prevents communication between network devices connected to certain interfaces or interface groups but allows the devices to communicate with the default gateway.

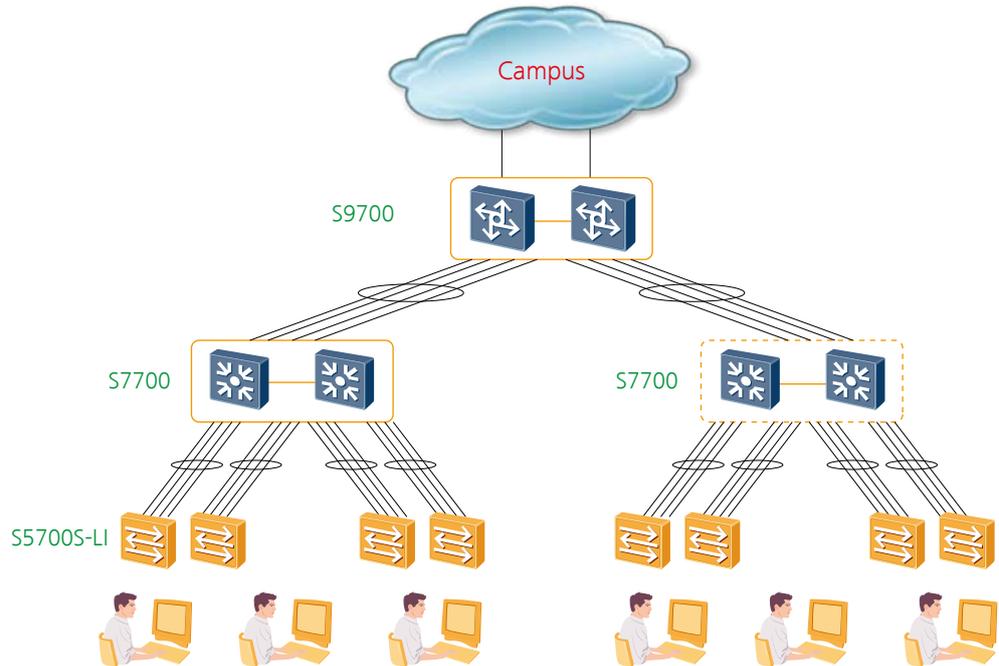
## Product Specifications

Item	S5700S-LI	
	S5700S-28P-LI-AC	S5700S-52P-LI-AC
1000M port	24*10/100/1000Base-T, 4*1000 Base-X	48*10/100/1000Base-T, 4*1000 Base-X
MAC address table	IEEE 802.1d compliance 8 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 QinQ, Selective QinQ 1:1 and N:1 VLAN Mapping GVRP	
Reliability	RRPP ring topology and RRPP multi-instance Smart Link tree topology and Smart Link multi-instance, providing the millisecond-level protection switchover Smart Ethernet Protection (SEP) STP(IEEE 802.1d), RSTP(IEEE 802.1w), and MSTP(IEEE 802.1s) BPDU protection, root protection, and loop protection	
IP routing	Static routing	
IPv6 features	IPv6 host Static IPv6 routes Path MTU (PMTU) IPv6 ping, IPv6 tracert, and IPv6 Telnet ACLs based on the source IPv6 address, destination IPv6 address, Layer 4 ports, or protocol type	
multicast	IGMP v1/v2/v3 snooping and IGMP fast leave MLD v1/v2 snooping Multicast VLAN Multicast load balancing among member ports of a trunk Controllable multicast Port-based multicast traffic statistics	

Item	S5700S-LI	
	S5700S-28P-LI-AC	S5700S-52P-LI-AC
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, PQ, WRR+PQ, and DRR+PQ 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	
Security	User privilege management and password protection DoS attack defense, ARP attack defense, and ICMP attack defense Binding of the IP address, MAC address, interface, and VLAN Port isolation, port security, and sticky MAC Limit on the number of learned MAC addresses 802.1x authentication and limit on the number of users on an interface AAA authentication, RADIUS authentication, HWTACACS authentication, and NAC SSH v2.0 Hypertext Transfer Protocol Secure (HTTPS) CPU defense Blacklist and whitelist	
Surge protection	6 KV surge protection capability on service ports	
Management and maintenance	MAC Forced Forwarding (MFF) Virtual cable test Ethernet OAM (IEEE 802.3ah and 802.1ag) Port mirroring and RSPAN (remote port mirroring) Remote configuration and maintenance by using Telnet SNMP v1/v2/v3 RMON Web NMS HGMP NTP System logs and alarms of different levels DLDP MUX VLAN IEEE 802.3az(Energy Efficient Ethernet)	
Operating environment	Operating temperature: 0°C–50°C (long term); -5°C–55°C (short term) Relative humidity: 10%–90% (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	
Dimensions (W x D x H)	442 mm x 220 mm x 43.6 mm	442 mm x 310 mm x 43.6 mm
Power consumption	< 25W	< 52W

## Applications

### 1000 Mbit/s Access Rate for Terminals



## Product List

### Product Description

S5700S-28P-LI-AC Mainframe(24 GE RJ45,4 GE SFP,AC 110/220V)

S5700S-52P-LI-AC Mainframe(48 GE RJ45,4 GE SFP, AC 110/220V)

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

**Copyright © Huawei Technologies Co., Ltd. 2012. 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.

**General Disclaimer**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

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

[www.huawei.com](http://www.huawei.com)