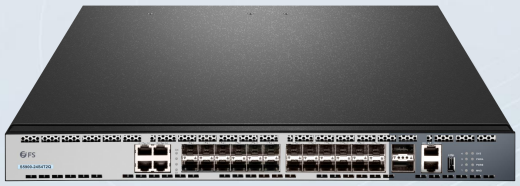
FS S5860-20SQ and S5900-24S4T2Q Switch Competitive Comparison

S5860-20SQ



S5900-24S4T2Q

Product Comparison Models

- S5860-20SQ
- S5900-24S4T2Q

Contents

Product Software Function

Compared with S5900-24S4T2Q switch, S5860-20SQ has a great improvement in function. The Layer 3 equipment network will be more flexible, which can do more strategies, software control and software linkage, etc. S5860-20SQ supports high throughput and low latency to meet the needs of users with high-density access and high-performance aggregation.

S5860-20SQ Switches Features

- Support diversified security features to ensure network stable and meet more choices for users.
- Aggregation layer of large networks, core of small and medium-sized networks, full 10G layer 3 access for large enterprises or office buildings.
- The wide variety of management mechanisms provides network security protection, high-security access control and effective network access control.
- The comprehensive management policies help to manage bandwidth and guarantee the key services such as voice call, multicast audio and video services, and video on demand.
- Green and energy-saving, it supports EEE (Efficient Energy-Efficient Ethernet) protocol, which can help customers reduce expenses while extending the service life of equipment.

Models	S5860-20SQ	S5900-24S4T2Q
Security	• Port security, IP Source Guard, Dynamic Arp Inspection; • Support IP+MAC data binding using DHCP SNOOPING[1]; • Support the use of 1X IP+MAC data binding; • Support IP+MAC data binding using IP SOURCE GUARD; • Hardware CPP, ICMP anti-attack, anti-IP anti-scanning attack, DHCP V6 anti-attack; • Support trusted ARP and VRRP dual-core environment deployment; • Web Portal V2.0; • Support IPV6 certification;	• Identification and Filtration of L2/L3/L4 Based ACL. • Defend Against DDoS attack, SYN Flood of TCP, UDP Flood Attack. • Suppression of Broadcast, Multicast and Unknown Unicast Packet. • Port Security, IP+MAC+Port Binding • DHCP Snooping and DHCP Option 82 • Command Line Authority Control Based on User Levels
Operation and Maintenance Method	SNMP[2], RMON, HTTPS, Telnet, SSH, Openflow, Syslog/Debug	SNMP, RMON, HTTP, Telnet, SSH
Layer 3 Feature	Support IPv4/IPv6 RIP/OSPF[3]/BGP/ISIS	RIP, OSPF, BGP
Stackability	2 Units	4 Units

Product Performance

S5860-20SQ provides flexible 10 Gigabit optical, multi-rate (10G/1G) access capability, and supports high-performance 10G/25G/40G uplinks to meet the needs of users with high-density access and high-performance aggregation. It also provides perfect end-to-end QoS, flexible and rich security settings for large-scale network aggregation, small and medium-sized network cores to meet the needs of the high-speed, safe and intelligent enterprise network.

Models	S5860-20SQ	S5900-24S4T2Q
1G RJ45 Port	/	4
10G SFP+ Port	20	24
25G SFP28 Port	4	/
40G QSFP+ Port	2	2
Layer Type	Layer 3	Layer 3
Switch Chip	BCM56170	BCM56842
Switching Capacity	760 Gbps	640 Gbps
Forwarding Rate	565 Mpps	480 Mpps
Packet Buffer	4MB	9MB
SDRAM	1GB	2GB
Routing Table	16K	16K
MAC Address	32K	128K

Product Reliability

S5860-20SQ Switch Features

- Support VRRP[4] to effectively ensure network stability. Suitable for scenarios such as finance, retail, call center, etc.
- Support RLDP[5], which can quickly detect the on-off of the link and the unidirectionality of the optical fiber link. Support the loop detection function under the port to prevent network failures caused by loops formed by privately connecting Hub and other devices under the port. Suitable for scenarios such as retail, hospital, enterprise, etc.
- In the case of not enabling STP, REUP[6] can be used to provide a fast on-chain protection function. REUP enables users to provide basic link redundancy even when STP is turned off, while providing millisecond-level failure recovery faster than STP. Suitable for scenarios that require quick failure recovery.
- Support stacking millisecond fault recovery: Stacking devices and peripheral devices are connected through aggregated links. If one of the devices or a member link fails, it only takes 50 to 200 milliseconds to switch to another member link.
- Support rich Authentication methods, QoS, CPU Protection, ARP spoofing prevention

Models	S5860-20SQ	S5900-24S4T2Q
VRRP	Yes	Yes
RLDP	Yes	No
REUP	Yes	No
CPU Protection Policy (CPP[7])	Yes	No

Product Hardware

S5860-20SQ Switch Features

- Use modular power supply to improve equipment stability and reliability. When the power supply fails, it can be directly replaced by the continuous network.
- Larger flash memory allows customers to save more configurations and systems, etc., to facilitate maintenance.
- The port lightning protection index reaches 6KV, and the lightning protection ≥8KV.
- Key components such as fans and power supplies that are prone to accumulate dust are coated with three anti-corrosion to prevent corrosion by dust.
- It provides a variety of port types including 25G/40G uplinks to meet the future network expansion, enabling network deployment more flexible.
- S5860-20SQ supports hardware dual-start technique and implements hardware-level redundancy to prevent chip damage. Utilize the existing resources of memory chip of main program to reduce cost.
- Support anti-grid fluctuation with trunk monitoring designed. When the voltage is abnormal, the power of motherboard will be down. After the voltage returns to normal, the motherboard will be powered up sequentially and all services are automatically restored.

Models	S5860-20SQ	S5900-24S4T2Q
Flash Memory	1GB	32MB
Lightning Protection	6KV-8KV	2KV
Material	Conformal Coating	ENIG
Power Supply	1+1 Hot-swappable Power Supplies	1+1 Hot-swappable Power Supplies

Features Explanation

DHCP SNOOPING[1]: DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

SNMP[2]: Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

OSPF[3]: Open Shortest Path First (OSPF) ensures an optimal access path. Suitable for scenarios such as finance, traffic, large office network, etc.

VRRP[4]: The Virtual Router Redundancy Protocol is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP). Suitable for scenarios such as finance, retail, call center, etc.

RLDP[5]: The Rapid Link Detection Protocol is a link protocol used to quickly detect Ethernet link failures. Suitable for scenarios such as retail, hospital, enterprise, etc.

REUP[6]: Rapid Ethernet Uplink Protection provides a fast on-chain protection function. It is a solution that provides a reliable and efficient backup and switching mechanism for dual uplinks. It can provide faster convergence performance and is often used in dual-uplink networking. Suitable for scenarios that require quick failure recovery.

CPP[7]: CPU Protection Policy (CPP) distinguishes the data flows sent to the CPU, which are processed according to their priorities, and implements bandwidth limitations as needed. In this manner, users can prevent the CPU from being occupied by illegal traffic and protect against malicious attacks to guarantee security of the CPU and switch.

Online Resources

S5860-20SQ Switch Datasheet: https://img-en.fs.com/file/datasheet/s5860-series-switches-datasheet.pdf

S5900-24S4T2Q Switch Datasheet: https://img-en.fs.com/file/datasheet/s5900-24s4t2q-switch-datasheet.pdf

https://www.fs.com