Hillstone W-Series
Web Application Firewall

Hillstone W-Series Web Application Firewall (WAF) provides enterprise-class, comprehensive security for web servers, applications and APIs. It defends against attacks at both the network and application layers, providing protections against DDoS, the OWASP Top 10 threats, and bot attacks, for example. In addition, the WAF validates APIs against the schema defined in OpenAPI, and automatically generates positive security model policies to detect and defend against attacks and misuse.

Hillstone WAF combines traditional rules-based detection with innovative semantics analysis. This dual-engine approach significantly increases accuracy while minimizing false positives. Hillstone WAF also leverages machine learning technology to fine tune security policies and block unknown threats and attacks. Further, logs can be automatically aggregated across multiple dimensions to allow admins to easily identify suspicious anomalies or locate false positives, and then further refine policies as needed.

Product Highlights

Comprehensive Web Application Security

Hillstone Web Application Firewall (WAF) provides complete security of web-based applications and APIs for enterprises and other organizations. It detects and defends against attacks at both the network layer (such as DDoS attacks, flood attacks, scan and spoof, etc.), and at the application layer (such as the OWASP Top 10 risks including injection attacks, cross site scripting (XSS) attacks, injection, etc). Hillstone WAF automatically discovers web servers and related assets and puts them under protection. With this capability, Hillstone WAF covers the entire web estate even when it scales, which helps improve operational efficiencies and deliver faster time-to-value.

Advanced API Protection

As the digital transformation continues to evolve, APIs play a more and more important role in application development and integration. The popularity of APIs potentially exposes additional attack surfaces, such as excessive data exposure, lack of resources and rate limiting, injection and XSS attacks among API calls, etc. Based on the schema defined in the OpenAPI files, Hillstone WAF helps validate and generate positive security model policies to detect those threats in APIs.

Improved Detection Accuracy and Efficiency with Dual Engines

Hillstone WAF integrates the industry's most innovative semantics analysis with traditional WAF detection engines. Combined with traditional rules-based detection, the seman-

© 2021 Hillstone Networks All Rights Reserved.

Product Highlights (Continued)

tics analysis engine helps further detect threats like SQL injection and cross site scripting, and minimizes false positives. Hillstone WAF's recursive decoding capability also detects attacks that are obscured by multiple encoding. This dual-engine approach significantly improves the accuracy of detection and efficiency in operation.

Machine-Learning-Driven Security Rule Optimization and Unknown Attack Defense

In addition to general protection based on rules and scripts for known attacks, Hillstone WAF's auto-learning capability helps mitigate never-before-seen exploits to protect specific applications from zero-day attacks. Its ML-based model learns from the data of normal traffic such as parameter length, cookie, HTTP methods, etc., tunes itself based on the test results as well as input from administrators, and continues updating the learning models and optimizing WAF rules as applications evolve. It significantly reduces operational overhead by eliminating the troubleshooting of false positives and manual policy tuning.

Rich Logs for Intelligent Analysis and Reporting

Hillstone WAF provides administrators and operators high visibility and comprehensive report with threat analysis, traffic analysis, attack breakdown and threat control. Its log aggregation capability allows logs to be aggregated from multiple dimensions, which helps operators easily identify suspicious anomalies or find false positives from logs, and then tune the policies accordingly.

Features

Web Application Protection

- Defend against HTTP anomalies
- SSL transparent proxy
- HTTP fast flood and slow flood attacks defense
- Injection attacks defense, including SQL injection, LDAP injection, SSI injection, Xpath injection, Command injection, Remote File Include (RFI) injection, etc.
- Defend against cross-site attacks, including XSS and CSRF attacks
- Semantic analysis based detection of SQL injection and XSS attacks
- Prevention of data leakage, including leakage of server error, database error, Web directory content, code, keyword, etc.
- Prevent leakage of sensitive personal data. Support detection the leakage of personal identification, number of bank card, credit card, and email account. Support desensitization of sensitive information (replace with specified characters)
- Cookie security. Support prevention of cookie tampering and hijacking; support cookie signature and encryption
- Web access control ability, which can defend the behavior of scanning, crawling, and directory traversal
- Support fine-grained control of HTTP access based on client IP, by matching HTTP method, HTTP header, HTTP content type, HTTP protocol version, URI path, etc.
- Support defense against vulnerability attacks to web servers, web framework and web application
- Defense against illegal resource access, including illegal uploads, illegal downloads and hotlinking attacks; support illegal download control based on file size and MIME file type
- Defense against malware, including WebShell and Trojan attacks, etc.
- Defense against brute force attacks
- Support detecting and blocking client by its source IP (via X-forward-for) when deployed behind a load balancer or a proxy
- Support customized rules
- Pre-defined protection policy templates; support customized protection policies
- Real time update of signature databases
- Support API security detection and protection; Support validation based on OpenAPI specification documents
- Support configuring site status as website maintaining

Anti-defacement

- Support two operating modes: learning mode and protection mode
- Similarity comparison of protected contents
- Support customized protected static web page types; support exception URL list for tamper resistance; Support duration and time setting for protection
- Support synchronization with servers and establish baseline by the built-in sync engine.
- Support monitoring of tampering and normal modification
- Support forensic of tampering

Network Security Protection

- Defense against DoS attacks, including: Ping of Death attacks, Teardrop attack, IP fragmentation attack, Smurf and Fraggle attack, Land attack, ICMP large packet attack, etc.
- Defense against DNS query flooding attacks, support configuring alert level according to the source and destination address
- Protection against TCP abnormalities
- Protection against IP scanning/spoofing and port scanning
- Protection against flooding, including: ICMP flood, UDP flood, SYN flood, etc.
- Support IP reputation and blocking malicious IP
- Support policy control based on HTTP header, including: Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Cookie, etc.
- Support HTTP2 in reverse proxy mode
- Support HTTPS decryption and IPv6 traffic detection in TAP mode

IPv6

- Optimization of access control policy
- Support IPv4, IPv6 dual stack deployment. IPv4 and IPv6 addresses can be added as protected sites simultaneously

Policy auto-learning

- Support detection and protection of IPv6 traffic
- Intelligent learning of the traffic to the protected site, and tune the policies based on the learning results
- Learned contents including: dynamic URL address, URL parameter, HTTP access method, cookie and other information
- Support learning mode and protection mode; support auto switching to protection mode after learning

Defense Response

- Support learning from the specific URL
- Support alarming only if a trigger behavior is executed
- Support blocking the behavior that break the security rules and responding with an alert page
- Support alert page customization
- Support redirecting the alert page to another URL
- Support adding whitelist (exception rule) via

© 2021 Hillstone Networks All Rights Reserved.

Features (Continued)

security logs, and support exception rules based on URL and source IP
- Support adding attacker to blacklist to block subsequent access
- Support IP and URL whitelist
- Support interaction with firewall to issue blacklist
- Support access control based on geoIP

Deployment
- Support multiple deployment modes, including Transparent proxy mode, TAP mode, reverse proxy mode, one-arm reverse proxy mode and traction
- Web assets auto-discovery
- Support default site
- Support configuring non-interface IP to the site and ARP response in one-arm reverse proxy mode and reverse proxy mode
- Support graphical deployment wizard

Virtualized Offering
- Supported Hypervisors: VMware, KVM, Openstack and Xen
- Support built-in Agent, such as VMware Tools and Cloud-init
- Support AWS, Azure, AliCloud
- Support HA deployment in public cloud environment (AliCloud, AWS)
- Support license management through LMS system
- Support Restful API
- Support hot-swappable NIC, SR-IOV and elastic scaling

High Availability
- Active/ passive mode
- Active/ Active Peer Mode
- Support software Bypass (in transparent proxy mode)

Application Acceleration and Server Load Balancing
- Support web Cache, page compression and TCP Multiplexing, SSL unloading, SSL proxy
- Support server load balancing (in reverse proxy mode), including weighted round-robin, least connection and IP Hash algorithm
- Server load balancing support IPv6
- Support server health check. Support customizing the URL object used by the health check
- Support using X-header as load balancing IP

Network and Interface Configuration
- Support static routing
- Support interface aggregation
- Support VLAN sub-interface
- Support multiple vSwitches, virtual-wires

Authentication
- Multi-level authorization, predefined roles including system administrators, operators, auditors, etc.
- Support local authentication, Radius and TACAS-C+

Device Management
- Multiple management methods including: HTTP, HTTPS, SSH, Console, etc. Support configuration of trusted management host
- Support device status monitoring, including: summary and detail information of hard disk, storage, CPU utilization and temperature
- Support centralized management and firmware upgrade through Hillstone Security Management System (HSM)
- Support operation and maintenance tools such as ping/tcpdump/curl

Log, Report and Alarm
- Rich log information, including device management logs, network security logs, web security logs, tamper-proof logs, access control logs, auto-learning strategy logs, web access logs, etc.
- Support logging all HTTP headers in attack events, including URL, UserAgent, POST content, cookie, etc.
- Support logging server responses
- Supports alarming via e-mail, SNMP, SYSLOG, SMS, etc.
- Support reporting (report templates supported) from multi-dimensions such as security risk overview, site risk details, attack type details, site tampering analysis, site visits, summary of network layer attack, system operation status, etc.
- Support log aggregation according to policy or client IP
- Support intelligent log analysis, including threat analysis and false positive analysis, and optimization of security policy based on analysis results
- Support playback of attack, which can help administrators quickly analyze and locate the threats and attacks in network
- Support deleting web security log
- Support log transfer via FTP
- Support user-defined report
- Support report exported in PDF, DOC format
- Support periodic export of report
- Mail server supports STARTTLS and SSL encrypted transmission
- Support user session tracking to add user name, session identifier and session identity value in logs

Specifications

	SG-6000-WV02	SG-6000-WV04	SG-6000-WV08	SG-6000-WV12
Maximum Throughput (1518 bytes) (vNIC/ SR-IOV) (1)	5G	10G	20G	40G
Maximum Concurrent Sessions (1)	400,000	1,200,000	2,500,000	4,000,000
HTTP Throughput (HTTP GET 512KB file) (2)	1200M	2500M	5500M	8000M
HTTP Concurrent Sessions (HTTP GET 64B file) (2)	100,000	300,000	1,500,000	2,500,000
HTTP New Sessions (HTTP GET 1B file) (2)	2,800	5,800	14,000	20,000
HTTP Maximum Transactions Per Second (TPS) (2)	3,000	6,500	16,000	22,000
HTTP Throughput Reference for Model Selection (2)	250M	650M	1500M	2000M
HTTPS Throughput (3)	200M	400M	900M	1500M
HTTPS New Sessions (3)	400	900	2,200	3,300
HTTPS Maximum Transactions Per Second (TPS) (3)	3,000	6,000	15,000	24,000
HTTPS Throughput Reference for Model Selection (3)	50M	80M	200M	300M
vCPU Support	2 Core	4 Core	8 Core	12 Core
Storage (Min/Max)	100GB/1TB	100GB/1TB	100GB/1TB	100GB/1TB
RAM	4G	8G	16G	24G
Network Interface Support (Minimum / Maximum)	10	10	10	10
Protected Sites	16	32	128	256
Protected IP/PORT Pairs	32	64	1024	1024

NOTES:

(1) Network performance is obtained under WAF disabled, and no protection site configured;

(2) HTTP protection performances are obtained under protection site configured and "Medium Protection Strategy" used;

(3) HTTPS protection performances are obtained under "Medium protection strategy", TLSv1.2 cipher suite ECDHE-RSA-AES128-GCM-SHA256, key length 2K RSA.

© 2021 Hillstone Networks All Rights Reserved.
Version: EX-08.01-W-Series-V2.7.4-0921-EN

RG-S6120-20XS4VS2QXS

10G Switch Datasheet

Scan QR Code
For More Enquiry

Product Highlights

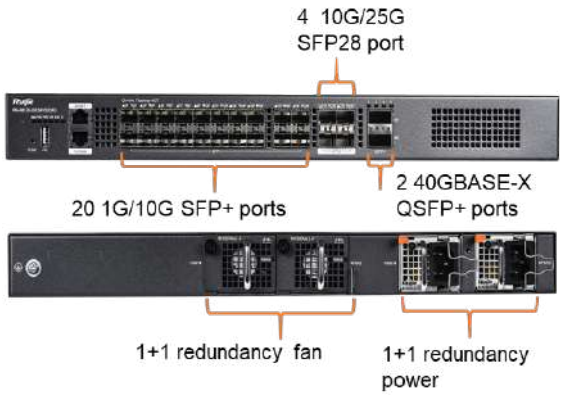
- **Up to 32 x 10G Base-X Access Ports and 4 25G & 2 40G uplink**
- **Built-in Advanced Layer 3 Routing Support**
- **Power and Fan Redundancy Support (hot-swappable)**
- **Robust High Reliability Hardware Design (Guarantee for 30 Years MTBF)**

Product Overview

RG-S6120 series switches are next-generation 10G Ethernet switches with high performance and high security newly launched by Ruijie. Adopting advanced hardware architecture design and Ruijie's new RGOS gen 12th modular operating system, the switches provide faster hardware processing performance and more convenient operating experience.

RG-S6120 series provides maximum 32 10G fiber access and supports high-performance 10/25/40G port uplink, which fully meets the user requirements of high-density access and high-performance aggregation.

RG-S6120 series switches provide high-performance and comprehensive end-to-end QoS, as well as flexible and feature-rich security settings for large-scale network aggregation as well as small and medium-sized network cores, meeting the needs of high-speed, high-security and smart enterprise networks.



RG-S6120-20XS4VS2QXS Front (above) and Rear (bottom) product view

Product Features

IPv4/IPv6 Dual-Stack Multilayer Switching

RG-S6120 series provides hardware support for IPv4/IPv6 dual-stack multilayer switching at line rates, supports distinction and processing of IPv4 and IPv6 packets by hardware, and provides flexible IPv6 network communication solutions according to the requirements of the IPv6 network for network planning or maintaining the current network status.

The switches also support a wide range of IPv4 routing protocols, including static routing, RIP, OSPFv2, IS-ISv4, BGP4, etc., enabling users to select appropriate protocols for network building in different environments. The series also supports an abundant list of IPv6 routing protocols, such as static routing, RIPng, OSPFv3, IS-ISv6, BGP4+, etc., enabling users to select appropriate protocols for upgrading an existing network to IPv6 or building a new IPv6 network.

Virtual Switch Unit (VSU)

The Virtual Switch Unit technology, or VSU in short, enables interconnection of several physical devices via link aggregation by virtualizing them into one logical device. The logical device uses one single IP address, Telnet process, command-line interface (CLI), and enables auto version inspection and configuration for management. From the user perspective, they are only managing one device, but realizing the work efficiency and user experience brought by several devices operating at the same.

Link aggregation can be either 10G ports or dedicated stack cards for user's investment protection.

• **Easy management:** Administrators can centrally manage all the devices at the same time. It is no longer necessary to configure and manage the switches one by one.

• **Simplified typology:** The VSU is regarded as one switch in the network. By connection of aggregation link and peripheral network devices, MSTP protocol is unnecessary as there is no Layer 2 loop network. All protocols operate as one switch.

• **Millisecond failover:** The VSU and peripheral devices are connected via the aggregation link. Upon failure of any device or link, failover to another member link requires only 50 to 200ms.

• **Exceptional scalability:** The network is hot swappable. Any devices leaving or joining the virtualized network cause zero impact on other devices.

Comprehensive Security Policies

The RG-S6120 series effectively prevents and controls virus spread and hacker attacks with various inherent mechanisms such as anti-DoS attacks, hacker IP scanning, illegal ARP packets checking and multiple hardware-based ACL policies.

Hardware-based IPv6 ACL: Control IPv6 users' access to edge devices even when IPv6 users exist within an IPv4 network. It allows coexistence of IPv4 and IPv6 users on the network and controls the resources access by IPv6 users, such as restricting access to sensitive network resources.

Hardware-based CPU protection mechanism: The 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.

IP/MAC binding: Allow flexible binding of a port or the switch to the IP address and MAC address of users, strictly limiting user access on a port or in the entire switch.

DHCP snooping: Allow DHCP responses from trusted ports only to prevent spoofing by unauthorized DHCP servers. Based on DHCP snooping, the switches dynamically monitor ARP packets, check user IP addresses, and directly discard illegal packets inconsistent with the binding entries to effectively defends against ARP spoofing and source IP address spoofing.

IP-based Telnet access control: Prevent unauthorized users or hackers from attacking or controlling the devices and thereby strengthens security of the device network management.

SSH and SNMPv3: Implement Secure Shell (SSH) and Simple Network Management Protocol v3 (SNMPv3) to encrypt management information in Telnet and SNMP processes, thereby ensuring security of the management device information and preventing hacker from attacking or controlling the devices.

Access Control: Prevents unauthorized users from network access through multiple features including multi-element binding, port security, time-based ACL, and flow-based rate limiting. The RG-S6120 Series highly strengthens the access control of visitors and restricts the access of unauthorized users to meet the needs of enterprise networks and campus networks.

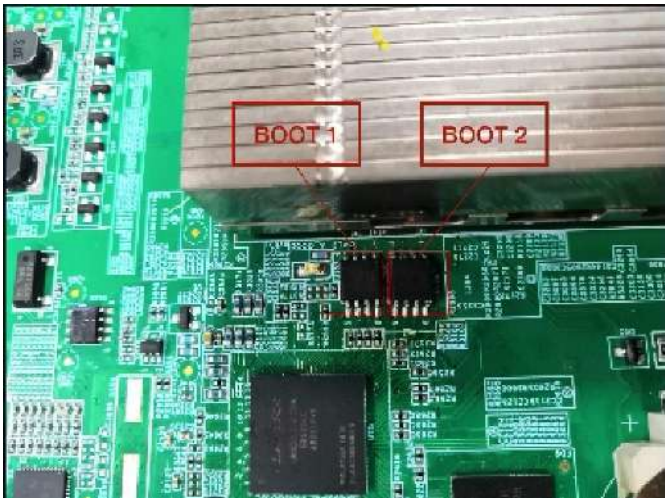
NFPP: The NFPP (Network Foundation Protection Policy) enhances switch security. It protects the switch processor and channel bandwidth by isolating the attacking sources. Normal packet forwarding and protocol status are hence guaranteed.

High Reliability Design

RG-S6120 series adopt multiple-tier hardware fault isolation and protection mechanism, guarantee for 30 Years MTBF. RG-S6120 series switches offer built-in power modules and fan modules redundancy. Both the power modules and the fan modules can be hot swapped without affecting the normal operation of the device. In addition, the switches also support fault detection and alarm for power modules and fan modules and automatically adjust the fan speed according to temperature changes to better adapt to the environment. The devices support front/rear ventilation to improve heat dissipation efficiency and provide multiple reliability protections at the equipment level and link level. Overcurrent protection, overvoltage protection and overheat protection technology are also adopted.

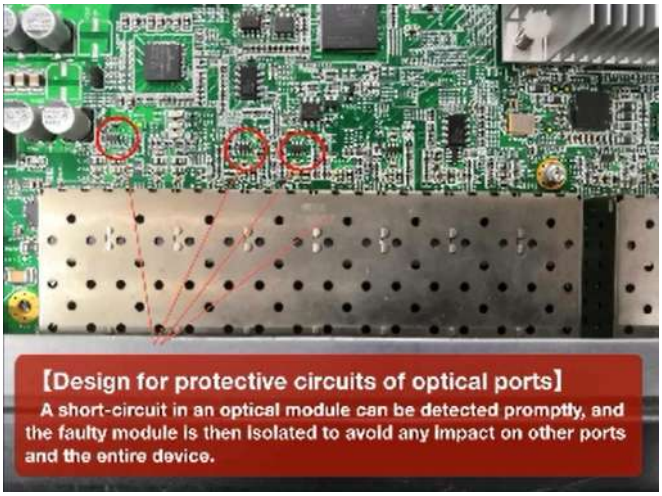
Hardware-level Dual Flash Chip

Flash-related faults account for approximately 5% of total faults throughout the year. RG6120 series switches use dual flash chips to store boot software to implement hardware-level redundancy backup and prevent startup failures.



Fault Isolation Technology

A short-circuit in an optical module may cause an optical port failure or even a switch breakdown or burnout. Ruijie S6120 series switch design for protective circuits of optical ports, a short-circuit in an optical module can be detected promptly, and the faulty module is then isolated to avoid any impact on other ports and the entire device.



Other than robust hardware design, powered by Ruijie gen 12th RGOS, all Ruijie enterprise switches built-in with variety of high availability networking features for different scenario and applications:

Spotlight High Availability Features:

Spanning tree protocols: The series supports spanning tree protocols of 802.1D, 802.1w, and 802.1s to ensure rapid convergence, improve fault tolerance capabilities, ensure the stable operation of the network, load balancing of links and reasonable use of network channels, and increase the redundant link utilization.

Virtual Router Redundant Protocol (VRRP): The series supports Virtual Router Redundancy Protocol (VRRP) which effectively ensures network stability.

Rapid Link Detection Protocol (RLDP): The series supports Rapid Link Detection Protocol (RLDP), which can perform quick link connectivity detection and unidirectional link detection of the optical fiber links, and support port-based loop detection to prevent network failures caused by loops generated by the improper connection of devices such as hubs to the ports.

Rapid Ethernet Uplink Protection Protocol (REUP): When Spanning Tree Protocol (STP) is disabled, the Rapid Ethernet Uplink Protection Protocol (REUP) can provide basic link redundancy through the rapid uplink protection and provide millisecond fault recovery faster than STP.

Bidirectional Forwarding Detection (BFD): Provide a method for upper-layer protocols such as routing protocols to quickly detect the connectivity of forwarding paths between 2 routing devices, greatly reducing the convergence time of upper-layer protocols in the case of changes in link status.

Exceptional business support performance: Support IPv4 and IPv6 multicast with abundant multicast protocols, e.g. IGMP Snooping, IGMP, MLD, PIM, PIM for IPv6, MSDP, etc. The switches offer multicast service for IPv4 network, IPv6 network, and IPv4/IPv6 co-existing network. IGMP source port and source IP check are also supported to effectively eliminate unauthorized multicast sources and improve network security.

Abundant QoS Policies

The RG-S6120 series offers multilayer traffic classification and flow control for MAC traffic, IP traffic, application traffic, etc. and realizes various traffic policies such as refined bandwidth control and forwarding priority. The series also supports customized QoS features for various applications.

The DiffServ-based QoS system supports a complete set of QoS policies covering 802.1P, IP TOS, Layer 2 to 7 filtering, SP, WRR, etc., and realizes the multi-service QoS logic of the entire network system.

Energy Saving

The RG-S6120 series switches adopt the next-generation hardware architecture, advanced energy-saving circuit design and components to save energy for users and reduce noise pollution. The series adopts the variable-speed axial fans so that the devices can intelligently control the fan speed according to the current temperature to ensure stable operation of the device while reducing power consumption and noise.

Easy Network Maintenance

RG-S6120 series supports abundant features such as SNMP, RMON, Syslog, logs and configuration backup using USB for routine network diagnosis and maintenance. Administrators can use a wide variety of management and maintenance methods for easier device management and such include command line interface (CLI), web management, Telnet, etc.

Technical Specifications

Model	RG-S6120-20XS4VS2QXS
Basic specifications	
Fixed ports	20 1G/10GBASE-X SFP+ ports, 4 10G/25GBASE-X SFP28 ports, 2 40GBASE-X QSFP+ ports, Support up to 32 10G ports, 2 modular power slots, 2 modular fan slots
Management ports	1 MGMT port 1 console port 1 USB port
Switching capacity	2.56T/23.04T
Packet forwarding rate	570Mpps/1260Mpps

Model	RG-S6120-20XS4VS2QXS
Port Buffer	4MB
ARP Table	Up to 16K
MAC Address	Up to 32K
Routing Table Size (IPv4/IPv6)	4K/4K
ACL Entries	Up to 2500
Product Features	
VLAN	4K 802.1Q VLAN Port-based VLAN Private VLAN GVRP Super VLAN
QinQ	Basic QinQ
Link aggregation	LACP (802.3ad)
Port mirroring	Flow-based mirroring Many-to-one mirroring, One-to-many mirroring RSPAN Link aggregation mirroring
Multiple Spanning Tree (MST) Instances	64
Spanning tree protocols	STP, RSTP, MSTP
Maximum Aggregation Port (AP)	128
DHCP	DHCP Server DHCP Client DHCP Snooping DHCP Relay IPv6 DHCP Snooping IPv6 DHCP Client IPv6 DHCP Relay
IPv6 protocols	IPv6 addressing, ICMPv6, Path MTU Discovery
IP routing	Static routing RIP, RIPng OSPFv2, OSPFv3, IS-ISv4, IS-ISv6 BGP4, BGP4+ ECMP
Multicast	IGMP v1/v2/v3, IGMP proxy IGMP v1/v2/v3 snooping IGMP filtering, IGMP fast leave PIM-DM, PIM-SM, PIM-SSM MLD Snooping, MLD MSDP

Model		RG-S6120-20XS4VS2QXS
ACL & QoS	ACL	Various hardware-based ACLs: Standard IP ACL (Based on IP address) Extended IP ACL (Based on IP address and TCP/UDP port number) Extended MAC ACL (Based on source and destination MAC addresses and Ethernet type) Time-based ACL Expert ACL (Based on the flexible combination of VLAN ID, Ethernet type, MAC address, IP address, TCP/UDP port, protocol type and time) ACL80 IPv6 ACL
	QoS	Port-based traffic recognition Port-based speed limit 802.1p/DSCP/TOS traffic classification 8 priority queues per port Queue scheduling algorithms: SP, WRR, DRR, SP+WRR, SP+DRR, RED/WRED
Security		Filter unauthorized MAC addresses Broadcast storm suppression Hierarchical management by administrators and password protection RADIUS and TACACS+ SSH BPDU Guard CPP, NFPP
Management		SNMP, CLI (Telnet/Console), RMON (1,2,4,9), Syslog, NTP, SNMP over IPv6, IPv6 MIB support for SNMP, Telnet v6, FTP/TFTP v6, DNS v6, NTP for v6, Traceroute v6 Support sFlow to sample the packets of the switch traffic using the random sampling technology of data stream
Reliability		VSU (virtualization technology for virtualizing multiple devices into 1); GR for RIP/OSPF/BGP; BFD; G.8032 (ERPS), REUP; RLDP; 1+1 power redundancy; Hot-swappable power module and fan module
VSU (Virtual Switch Unit)		Up to 2 stack members
Physical Specifications		
Power supply		Supported power module: RG-PA150I-F AC input: Rated voltage range: 100 to 240VAC; 50/60Hz Maximum voltage range: 90 to 264VAC; 47/63Hz Rated input current: 3A HVDC input: Rated voltage range: 240VDC Maximum voltage range: 192 to 288 VDC Rated current per input: 3A
Power Consumption		<85W
Power Surge Protection		4KV (MGMT Port) Power Supply Module (RG-PA150I-F): common mode 6KV/difference mode 6KV
Fan		Support 2 pluggable modular fans with front and rear air ducts Support fan speed adjustment and malfunction alert
Temperature alarm		Support temperature alarm function
Temperature		Operating temperature: 0°C to 50°C Storage temperature: -40°C to 70°C

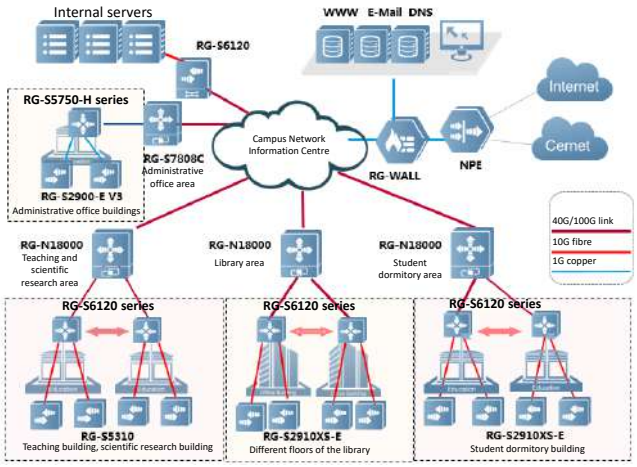
Model	RG-S6120-20XS4VS2QXS
Humidity	Operating humidity: 10% to 90%RH Storage humidity: 5% to 90%RH
Operating Altitude	0 to 5,000m
Dimensions (W x D x H) (mm)	440 * 330 * 43.6
Rack Height	1RU
MTBF	30 Years
Safety Standards	GB4943-2011 EN 62368-1:2014+A11:2017
Emission Standards	GB9254-2008 CLASSA EN 55032:2015+AC:2016 EN 61000-3-2:2014 EN 61000-3-3:2013+A1:2019 EN 55035:2017 ETSI EN 300 386 V2.1.1 (2016-07)

Typical Applications

- 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.

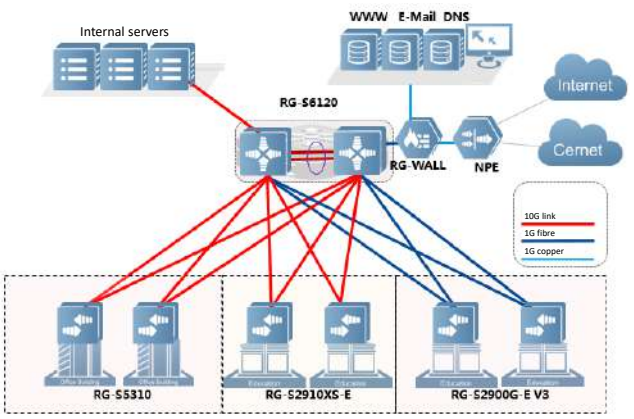
Scenario 1

As the aggregation layer switches of large campus networks, RG-S6120 series switches provide 10G bandwidth for access equipment, and 40G aggregation-to-core high-bandwidth link, which meets the users' growing needs.

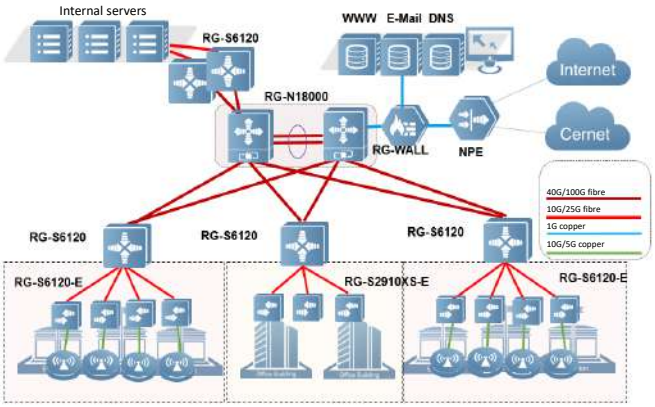


Scenario 2

The RG-S6120 series switches can also be deployed as 10-Gigabit core switches in small and medium-sized enterprises, which can greatly improve the reliability and efficiency of the network system while simplifying the network architecture through VSU technology.



Scenario 3



RG-S6120 can be deployed for the access or aggregation of small and medium campus networks. The 10G access ports can be used for high-speed AP access, forming 10G/25G access-to-aggregation and 40G aggregation-to-core high-bandwidth link to meet the users' growing needs.

Ordering Information

Please order according to the below sections including switch models, expansion modules and power modules selection. The expansion modules and power modules may be updated at any time. Please consult the related personnel before ordering.

Model	Description
RG-S6120-20XS4VS2QXS	20 1G/10GBASE-X SFP+ ports, 4 10G/25GBASE-X SFP28 Ports, 2 40GBASE-X QSFP+ ports, support up to 32 10G ports, 2 modular power supply slots (at least one RG-PA150I-F power module), 2 modular fan slots (2 fan modules are equipped by default)
RG-PA150I-F	150W AC power module for RG-S6120-20XS4VS2QXS
Mini-GBIC-GT	1000BASE-GT mini GBIC transceiver
XG-SFP-SR-MM850	10G LC interface module for SFP+ ports (62.5/125μm: 33m; 50/125μm: 66m; 300m when the modal bandwidth is 2000MHz•km)
XG-SFP-LR-SM1310	10G LC interface module for SFP+ ports (1310nm, 10km)
XG-SFP-ER-SM1550	10G LC interface module for SFP+ ports (1550nm, 40km)
VG-SFP-SR-MM850	25G fiber module VG-SFP-SR-MM850
VG-SFP-LR-SM1310	25G fiber module VG-SFP-LR-SM1310
XG-SFP-AOC1M	10G SFP+ optical cable, 1 meter, including one cable + both side transceivers
XG-SFP-AOC3M	10G SFP+ optical cable, 3 meters, including one cable + both side transceivers
XG-SFP-AOC5M	10G SFP+ optical cable, 5 meters, including one cable + both side transceivers
VG-SFP-AOC5M	25G SFP+ optical cable (including both side transceivers), 5 meters
40G-QSFP-SR-MM850	40G SR fiber module for QSFP+ ports (OM3/OM4 MPO, 8-core, 850nm, 100m with OM3 fiber, 150m with OM4 fiber)
40G-QSFP-LR4 SM1310	40G LR single-mode fiber module for QSFP+ ports, transmission distance up to 10km (LC, 2-core, 1310nm)
40G-AOC-5M	40G QSFP+ optical cable, 5 meters, including one cable + both side transceivers
40G-AOC-10M	40G QSFP+ optical cable, 10 meters, including one cable + both side transceivers

INNOVATION
Beyond Networks

Ruijie Networks Co., Ltd.

For further information, please visit our website https://www.ruijienetworks.com

All rights are reserved by Ruijie Networks Co., Ltd. Ruijie reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

BOE

Interactive WHITEBOARD

INTERACTIVE WHITEBOARD DISPLAYS

Interactive whiteboard display available in **55, 65, 75, 86 or 98 inch display** format is the largest in its kind. The **multi-touch touchscreen** feels like touching a tablet screen and is very easy to use. The **intuitive display** is perfect for presentations of any sort, such as business presentations or classroom lessons.

The **slim design** and direct bonding process gives users an excellent visual experience. The display is slim and elegant and the base is adjustable in height.

Another great feature is the **built-in intelligent conference system** to easily achieve a paperless office.

50000 hrs

MAIN CHARACTERISTICS

- ARRAY-TYPED MICROPHONES (make voice natural and clear)
- HIGH ACCURACY TOUCHPAD (makes smooth writing)
- HIDDEN ANTENNA (with simple and elegant designing)
- DOUBLE-PORTS USB
- BOE ORIGINAL DISPLAY

FEATURES AND FUNCTIONS

- Built-in writing software (Android) with all-channel annotating
  Make notes on the screen under multiple sources, save it by email or scanning. Easy to erase or add/delete pages.
- Android 8.0&Window dual systems
  With standard Android OS, and Window as option. OPS micro PC enables easier installation, use and maintenance.
- Smart sidebar
  Easy operation with the sidebars to achieve multiple functions.
- Dual-band Wifi
  Support 2.4GHz/5GHz dual-band Wifi, the signal is strong, stable, and with higher transmission speed.
- Full channel HDMI Loop out function (optional)
  Synchronous output is available through HDMI loop out interface.

APPLICATIONS

- Conference room, exhibition hall, classroom, office room, etc

TECHNICAL SPECIFICATIONS

Panel

	55”	65”	75”	86”	98”
Backlight	D-LED				
Resolution	3840 × 2160				
Display (H x V)	1209.60 × 680.40 mm	1428.48 × 803.52 mm	1649.66 × 927.94 mm	1895.04 × 1065.96 mm	2158.848 × 1214.352 mm
Pixel distance (H x V)	0.420 x 0.315 mm	0.496 x 0.372 mm	0.4296 x 0.4296 mm	0.4935 x 0.4935 mm	0.5622 x 0.5622 mm
Brightness	350 nit	450 nit		400 nit	460 nit
Contrast ratio	1300:1	1200:1			
Viewing angle	178°				
Colors	1.07B				
Color Gamut (x% NTSC)	68%	65%			
Aspect ratio	16:9				
Refresh rate	60Hz				
Lift Time	>50000 hrs				
Speaker Position	8 Ω 20 Hz , 18kHz 30W				

Interfaces

	55”	65”	75”	86”	98”
HDMI input	n° 3				
DP input	n° 1				
LAN port	n° 2				
AV/TV/VGA input	n° 1				
PC-AUDIO input	n° 1				
Y Pb Pr input	n° 1				
OPS port	n° 1				
Touch-UBS	n° 2 USB 2.0 (USB-B)				
PC-USB/Android USB	n° 2				
RS232	n° 1 (DB9)				
AV/S/PDIF/HDMI output	n° 1				
Audio output	n° 1				

Basic Configurations

	55”	65”	75”	86”	98”
Scalar	MSD8386	MSD6A848			MSD8386
CPU	ARM A73+A53				
CPU frequency	1.5GHz.				
Cores	Quad-core				
GPU	Mali-G51				
RAM	2/3GB DDR4	2GB DDR4	3GB DDR4		3/4GB DDR4
ROM	16/32GB	16GB		32GB	
OS	Android 8.0				

Touch Screen

	55”	65”	75”	86”	98”
Touch frame	Infrared touch frame				
Tempered glass	4 mm thickness				
Response time	< 10 ms	6 ms	8 ms		< 10 ms
Output	HID-compliant				
Total hits	Unlimited				
Touch diameter	≥ 2 mm.				

Weight and dimensions

	55”	65”	75”	86”	98”
Net weight (± 1.5 Kg)	25 Kg	42 Kg	58 Kg	85 Kg	113 Kg
Gross weight (± 1.5 Kg)	36 Kg	57 Kg	75 Kg	98 Kg	125 Kg
Dimensions (W x D x H)	1298.4 x 93.6 x 789.1 mm	1506.3 x 96.1 x 901.3 mm	1735.98 x 103.75 x 1034.52 mm	1989.18 x 119.7 x 1180.22 mm	2244.9 x 108.2 x 1340.4 mm
Packing (W x D x H)	1420 x 245 x 910 mm	1660 x 245 x 1045 mm	1880 x 280 x 1160 mm	2140 x 280 x 1340 mm	2525 x 435 x 1750 mm

Power consumption

	55”	65”	75”	86”	98”
Power supply	100~240 V/AC 50/60 Hz				
Working power	≤ 170 Watt	≤ 220 Watt	≤ 400 Watt	≤ 400 Watt	≤ 500 Watt
Standby power	< 0.5 Watt				