Miercom

Lab Testing Summary Report

March 2012

Report SR120120

Product Category:

Enterprise Switch

Vendor Tested:

HUAWEI

Product Tested:

S1700-28GFR-4P Switch

Miercom PERFORMANCE VERIFIED ™

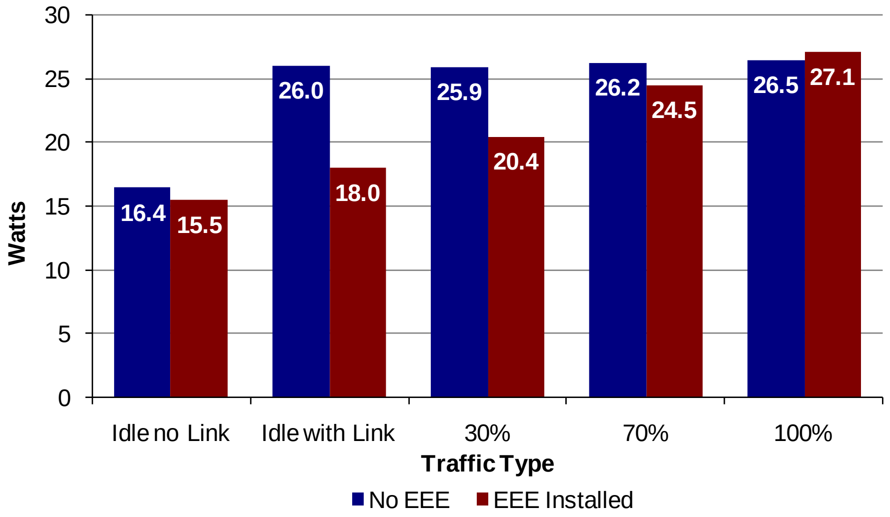
Key findings and conclusions:

- **Huawei S1700-28GFR-4P-AC switch provides one-button operation for system recovery, upgrade and information collection to streamline administration**
- **Interoperability proven through tests with Cisco switches**
- **Advanced features supported include DoS attack prevention, anti-worm function, IP and MAC source guard, and VCT**
- **Energy Efficient Ethernet (EEE) is supported, resulting in up to 30% power savings**

Huawei Technologies engaged Miercom to evaluate the S1700 series of enterprise switches for feature support and energy efficiency. The S1700 series consists of maintenance-free, Web-managed, and SNMP-based switches. SNMP-based switches include S1700-28FR-2T2P, S1700-52FR-2T2P, S1700-28GFR-4P, and S1700-52GFR-4P. The S1700-28GFR-4P switch was tested but the discussion of features pertains to the entire series of switches.

Testing focused on the rich feature set and energy efficiency of the switch. Up to 30% power savings is realized by EEE support of the S1700-28GFR-4P-AC switch. Energy Efficient Ethernet operates by shutting down port transmitters when traffic is not sent to save power. The figure below illustrates the power savings of the S1700-28GFR-4P when EEE was enabled.

Figure 1: Huawei S1700-28GFR-4P-AC Power Consumption with Power-Saving EEE Disabled and Enabled



Source: Miercom, March 2012

Power consumption of Huawei S1700-28GFR-4P-AC switch was measured with Energy Efficient Ethernet enabled and disabled. With EEE enabled, the switch consumed from 5 to 30% less energy except under full load. When fully loaded, the switch cannot go into sleep mode for EEE use.

Switch Features

Simple Management The S1700 series of switches has a variety of simple management features. These include Web system network management (HTTPS), one-button restoration, system log, Virtual Cable Test (VCT), Remote Network Management (RMON), ping/traceroute, and DHCP client.

HTTPS The S1700 series contains a Web-based GUI which can be used to monitor the switch, set security parameters, configure features, and perform troubleshooting.

One Button Features The S1700 contains several features that can be enabled or performed using a one-button operation. These features can be accessed through the Web management GUI. See *Figure 2* for a screen shot of the management information screen. This screen illustrates the interfaces of the switch and displays which interfaces are active, inactive, or disabled. This screen also displays the current CPU usage and running temperature of the switch. Information about the firmware version, MAC address, and other administrative readouts can also be seen in the summary screen.

With one-button system recovery, the S1700 switch provides a reset-to-factory-settings option. The management GUI provides "Reset to Factory," with or without the previous IP address settings.

Additionally, the switch includes a one-button upgrade option. From the GUI, you can upgrade the system by uploading a file via HTTP or FTP. For FTP transferring, address information is required and user authentication may be necessary.

Selecting the *Tools* option from the Device Management Panel allows you to download the configuration settings, log file, and error messages into a .txt file. This is accomplished using one-button information collecting.

System Log The S1700 series keeps system logs that can be accessed from the Web GUI. These logs can be viewed or downloaded to a local machine. The log files contain verbose system information for use by a network administrator.

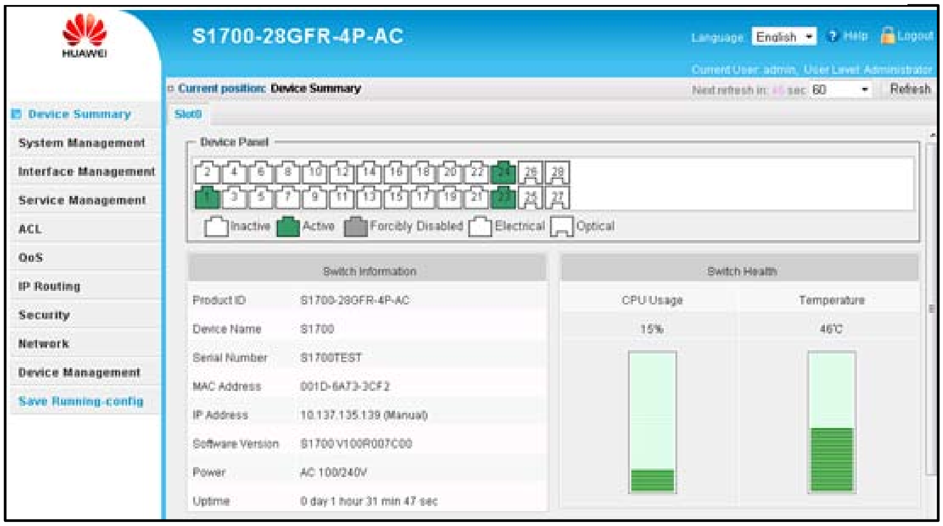
Virtual Cable Test (VCT) This feature displays the connection present on the switch, as well as the estimated copper length. This feature can also display short circuit information, as to where it can be found by port number and type of cable.

Remote Network Management (RMON) S1700 series supports RMON for network management. RMON monitors devices, network traffic, and system status to report errors.

RADIUS Authentication The S1700 switch supports 802.1x RADIUS authentication. This is used to grant access to devices before they can operate on the network. Using the RADIUS authentication feature of the switch also allows the administrator to monitor and modify access as needed. All of this can be accomplished through the management GUI of the switch. RADIUS authentication works well with Huawei's

The Device Summary screen from the management GUI of the S1700 displays CPU usage, temperature of the unit, port status, and general switch information.

Figure 2: Huawei S1700 Device Summary Screen



Switch Information	
Product ID	S1700-28GFR-4P-AC
Device Name	S1700
Serial Number	S1700TEST
MAC Address	001D-6A73-3CF2
IP Address	10.137.135.139 (Manual)
Software Version	S1700 V100R007C00
Power	AC 100/240V
Uptime	0 day 1 hour 31 min 47 sec

Switch Health	
CPU Usage	Temperature
15%	46℃

Source: Miercom, March 2012

Table 1: Chart of Features of the S1700 Series of Switches

Model	S1700-28FR-2T2P	S1700-52FR-2T2P	S1700-28GFR-4P ✱	S1700-52GFR-4P
Features				
Ports	24*10/100M Base-TX 2 GE Base-TX 2 GE Base-X SFP	48*10/100M Base-TX 2 GE Base-TX 2 GE Base-X SFP	24*10/100/ 1000 Base-TX 4 GE Base-X SFP	48*10/100/ 1000 Base-TX 4 GE Base-X SFP
Forwarding Rate	9.6 Mpps	13.2 Mpps	42.0 Mpps	78.0 Mpps
Switching Capacity	12.8 Gbps	17.6 Gbps	56.0 Gbps	104.0 Gbps
Web GUI	✓	✓	✓	✓
SNMP	✓	✓	✓	✓
One-Button Restoration	✓	✓	✓	✓
Ping/ Traceroute	✓	✓	✓	✓
VCT	✓	✓	✓	✓
LLDP	✓	✓	✓	✓

Source: Miercom, March 2012

✱ - *Tested model*

own RADIUS server, as well as third party servers. To verify that the S1700 switch can operate with a third party RADIUS server, a Cisco RADIUS authentication server was deployed in the network. The switch and the server both exhibited no issues during the testing process and authentication was accomplished successfully.

DoS The S1700-28GFR-4P-AC switch includes a variety of DoS attack prevention features that can be enabled or disabled from the management GUI. Tested with the Spirent TestCenter, these features kept CPU utilization within the same range as normal operation. The DoS attack did not affect the network or device.

For the test, the TCP UDP Port Zero option was selected and a DoS attack was implemented. When attack prevention was enabled, the CPU usage remained at 9%, which is within the normal operating range of a switch. When DoS prevention was disabled and the attack was re-run, the CPU spiked to 35% utilization, effectively proving that the prevention features saves CPU usage.

Anti-worm The S1700 switch contains an anti-worm function that can be enabled from the management GUI. The GUI allows the administrator to select which worm they would like to block against and to enable the specific anti-worm function using a check box. The screen also displays a counter for attack statistics to keep a tally of how many times this worm was detected on the network and blocked. See *Figure 3* on *page 4* for a screenshot of this interface. For this portion of testing, we selected the Blaster virus prevention function and saw that the attack package was dropped. This test consisted of sending a blaster virus package across the switch. As soon as the switch detected the package and verified it was a blaster virus, the switch discarded the traffic. Switch performance was not affected.

ARP Limit Rate limiting is supported by the S1700 switch. To challenge this feature, we set the rate limit on one of the interfaces to 100 frames per second (FPS). When we sent traffic from a load generator at a rate of less than 100 FPS, the switch operated normally. As soon as traffic passed the 100 FPS rate, the port stopped forwarding traffic and port shutdown was almost immediate. This test verified the success of the limiting feature. The settings can be modified and changed to allow for different limits on various ports on the switch.

MAC Limit Similar to the ARP limit, the S1700 can be configured to limit the number of MAC addresses it learns per interface, or switch-wide. The S1700 series is capable of supporting up to 8K of MAC addresses in its table. Once a particular interface reaches the pre-set MAC limit, the switch allows traffic forwarding for any packets signed with a MAC address learned under the limit. If a MAC address is connected to the switch that was learned after the limit was reached, traffic will be discarded from this address.

DHCP Limit The DHCP Pretender Attack function can be used on the switch to prevent traffic from being transmitted once a pre-set limit is reached. This can be configured on a port-by-port basis or set for the entire switch. Setting the limit to 20 frames, and using a load generator and running RFC 2544 tests, we sent 500 FPS from the test equipment to the switch. The first 20 frames were received without issue, but then the alarm trap function triggered indicating that the 20 frame limit had been reached. All subsequent frames were not received.

IP and MAC Source Guard This option allows the selection or restriction of traffic being transmitted based on IP address, MAC address, or VLAN. A combination of these three criteria can also be set to control traffic.

LACP The S1700 switch supports load balancing of a static LACP link aggregation group. This feature allows the switch to balance a load across all ports so that no one port gets congested. We verified this feature by sending traffic from a load generator to the switch using eight active ports. Once traffic was started, we could view the balanced load in the CLI. Next, a cable was unplugged from the switch to the traffic generator to simulate a down link. Traffic was immediately redistributed to another connection and re-balanced.

MAC Capacity. According to the system interface, the S1700 can support up to 8K MAC addresses. To confirm this value, we tested and verified that the switch can support 8K MAC addresses without issues.

VLAN Capacity. The S1700 can support up to 4,094 VLANs. The capacity of VLANs was tested using the onsite test center. We confirmed that no packet loss was recorded while routing through all 4,094 VLANs.

Interoperability

S1700 series of switches supports interoperability with third party switches. The features that are compatible with other vendors include LACP, STP, and MSTP functionality.

LACP S1700 series of switches supports Link Aggregation Control Protocol. This feature is interoperable with other vendor switches, allowing it to be used in a mixed network.

STP/MSTP Both STP and MSTP are supported protocols on the S1700 switch series. These protocols work in mixed vendor networks, as well as Huawei-only networks.

Energy Efficiency

The S1700 switch utilizes the EEE feature to save energy consumption. Energy Efficient Ethernet is a feature set designed to allow less power to be consumed during periods of low data activity by putting the transmit path into sleep mode. This feature is outlined in IEEE standard 802.3az.

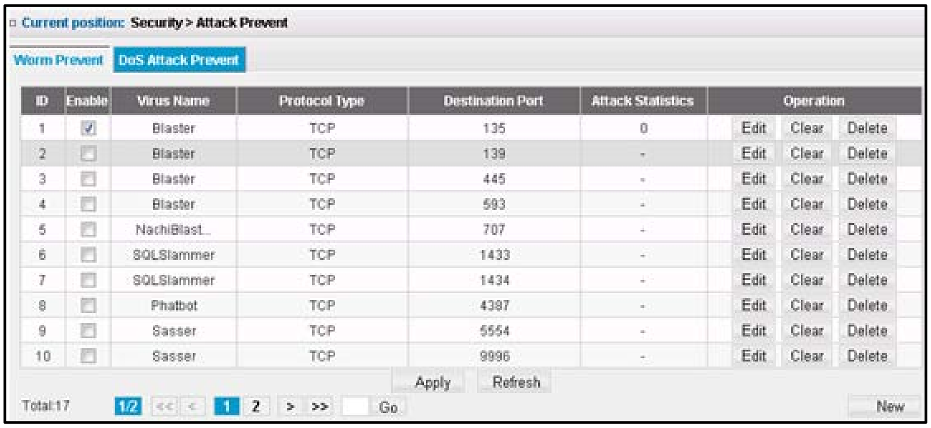
To evaluate the energy saved in the S1700 switch, power measurements were taken at five different points. These points included: idle with no link, idle with link, 30% load, 70% load, and 100% load. Each data point was taken twice, once with the EEE feature disabled and once with it enabled. See *Figure 1 on page 1.*

Bottom Line

The Huawei S1700 series of switches is very resilient and feature-rich. They are capable of being deployed in both enterprise network settings and small business environments with equal utilization. Web interfaces for the switch make configuration and access to settings far easier than the interfaces of other switches in its class. The switch is complete with all the security and access features required by a network administrator to deploy the device.

The S1700 Switch Series includes EEE features to conserve power by placing the ports in sleep mode when traffic is not being passed through the device. In our tests, we found the EEE feature can save up to 30% of total power consumption for normal use cases.

Figure 3: Huawei S1700-28GFR-4P-AC Switch Worm Prevention Screen



□ Current position: Security > Attack Prevent

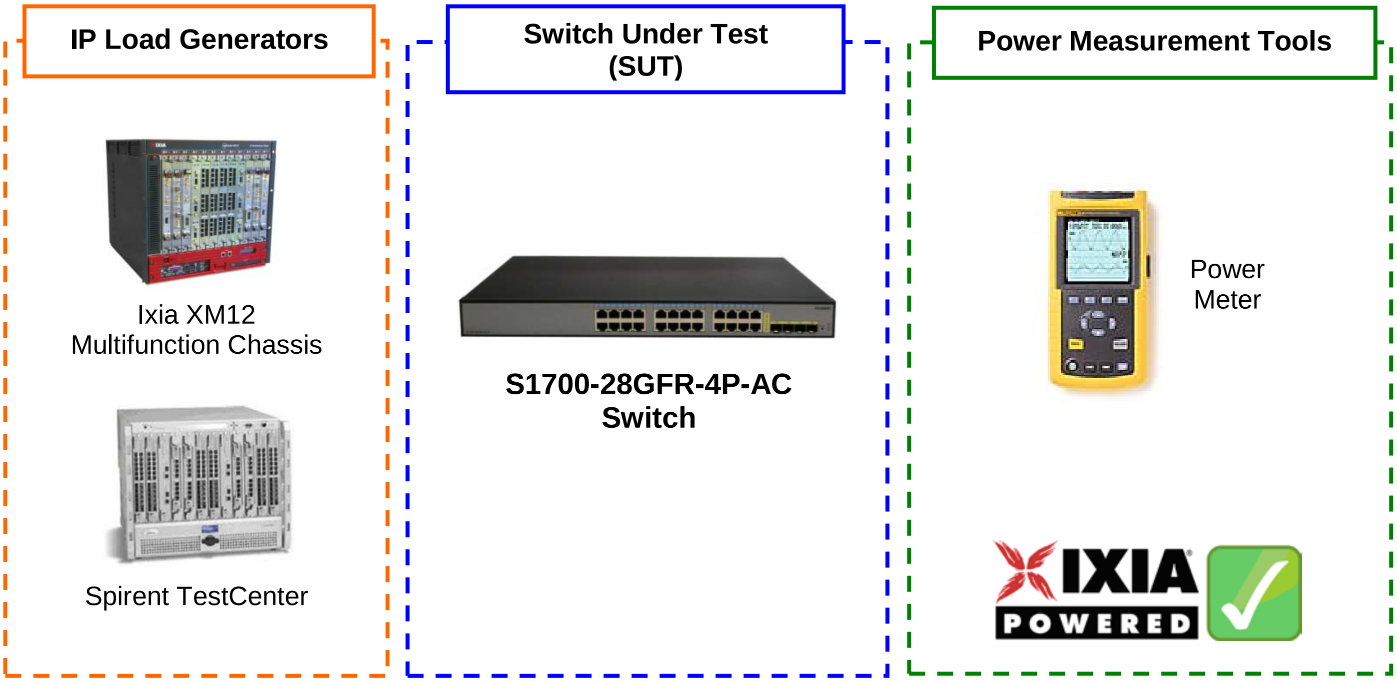
ID	Enable	Virus Name	Protocol Type	Destination Port	Attack Statistics	Operation		
1	☑	Blaster	TCP	135	0	Edit	Clear	Delete
2	□	Blaster	TCP	139	-	Edit	Clear	Delete
3	□	Blaster	TCP	445	-	Edit	Clear	Delete
4	□	Blaster	TCP	593	-	Edit	Clear	Delete
5	□	NachiBlast...	TCP	707	-	Edit	Clear	Delete
6	□	SQLSlammer	TCP	1433	-	Edit	Clear	Delete
7	□	SQLSlammer	TCP	1434	-	Edit	Clear	Delete
8	□	Phatbot	TCP	4387	-	Edit	Clear	Delete
9	□	Sasser	TCP	5554	-	Edit	Clear	Delete
10	□	Sasser	TCP	9996	-	Edit	Clear	Delete

Total:17

Source: Miercom, March 2012

Worm prevention screen allows the administrator to select various worms to defend against, the destination port for the prevention, and options to edit the rules or delete them.

Test Bed Diagram



Source: Miercom, March 2012

How We Did It

The Huawei S1700 series of switches was evaluated for energy efficiency and feature functions. Testing was conducted to verify that each of the features outlined in this report operated as advertised. Energy efficiency was evaluated by measuring energy consumption without any energy saving features enabled and then repeating the testing with these features turned on in order to compare savings.

The Huawei S1700 switch being evaluated was running firmware version 5.7 OS, the latest firmware version available for this device. Sections of this testing required the use of a traffic generator to evaluate the features of the product. Two different traffic generators were used during the course of the tests, Ixia XM12 running IxNetwork version 5.50.121.48 and Spirent TestCenter running version 3.76.0076.

Measuring Power Consumption: The power consumption of the S1700 switch was measured using varying network and link loads that the switch would typically encounter in a real world type of deployment. Power consumption was measured using a power meter connected directly to the S1700 switch. The switch was then loaded with Layer 2 traffic using the Ixia XM12.

Miercom recognizes Ixia (www.ixiacom.com) as an industry leader in energy efficiency testing of networking equipment. Ixia's unique approach utilizes coordination of energy measurements with network traffic load – allowing energy consumption to be graphed against network traffic volume. Real-world traffic is generated by Ixia's test platform and test applications, principally IxNetwork for Layer 2-3 routing and switching traffic and IxLoad for Layer 4-7 application traffic.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results may contact reviews@miercom.com for details on the configurations applied to the Switch Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.

Miercom Performance Verified

The performance of Huawei S1700-28GFR-4P-AC enterprise-class switch was verified by Miercom. In hands-on testing, Huawei demonstrated advanced performance features such as:

- One-button capabilities for system recovery, system upgrade and information collection
- Energy saving features, using EEE, result in 5 to 30% lower power consumption
- Interoperability with switches from other manufacturers
- DoS attack prevention, anti-worm function, IP and MAC source guard, and Virtual Cable Test

S1700-28GFR-4P-AC
Switch

Huawei Technologies Co., Ltd.
http://www.huawei.com/enterprise

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review, Tech Web - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.

Report SR120120 reviews@miercom.com www.miercom.com

Before printing, please consider electronic distribution

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report. Consult with professional services such as Miercom Consulting for specific customer needs analysis.