HUAWEI S12700 Agile Switch

Enable Networks to Be More Agile for Services

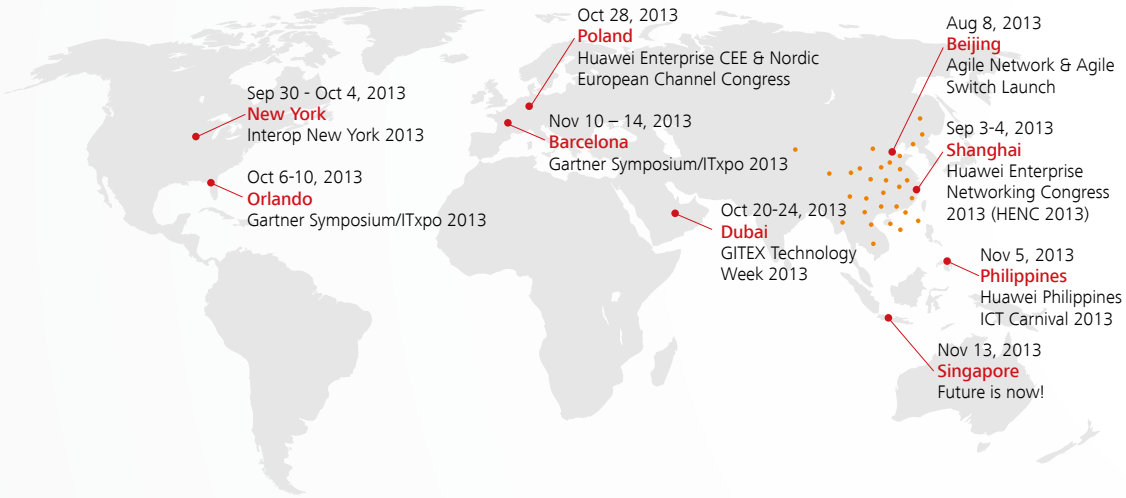
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Contents

1

Footprints of Huawei S12700 Agile Switches' Global Tour



Since Huawei rolled out its S12700 series agile switches on August 8, 2013 in Beijing, China and showcased the S12700 on Huawei Enterprise Networking Congress (HENC) in September 2013 in Shanghai, China, the S12700 has been continuously showcased on international large-scale exhibitions, opening the "Global Tour" of Huawei agile switches. The "Global Tour" activities are ongoing.

In addition, Huawei Enterprise Business Group (EBG) also showcased its agile network solution, fully demonstrating Huawei EBG's overall strong competitiveness and strategies for next-generation networks.

Glimpses of Agile Switches' Global Footprints

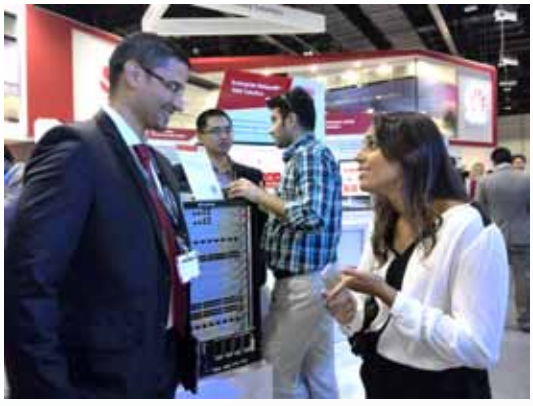
Interop and Gartner Symposium ITxpo in North America

From September 30 to October 4, 2013, Interop New York 2013 was held in New York, US. As one of the global partners of Interop, Huawei has showcased its products and solutions on Interop Las Vegas 2013 and Interop Tokyo 2013 in succession. Interop New York 2013 poses a significant influence in North America and even across the globe, has attracted a wide variety of device vendors from around the world. All the vendors gathered at the exhibition to show their new products. Huawei focused on showcasing its agile network solution and S12700 series agile switches. Huawei's agile network solution features agile services, agile management, and agile evolution, which are the key cornerstones for quickly and flexibly responding to fast-changing network services. Huawei's agile switches support automation of network deployment and management, full-scale network security

collaboration, flexible adaptation to various and fast-changing services, and full programmability, satisfying the future network's requirements

From October 6 to October 10, 2013, Gartner Symposium ITxpo was held in Orlando in North America. Gartner Symposium ITxpo is a grand IT event held by Gartner Inc., the world's leading information technology research and advisory company, and has over 200 conferences in total across the globe on a yearly basis. Huawei showcased its newly launched agile switches and Software-Defined Networking (SDN) and Bring Your Own Device (BYOD) solutions at Gartner Symposium ITxpo. The unique values of Huawei Enterprise Networking SDN Solution are full programmability (including chip programmability), service-friendly architecture (real-time service quality detection through Huawei's unique iPCA technology), and future-oriented smooth evolution. At Gartner Symposium ITxpo 2013 Orlando, Huawei's leaders and technical experts in the field made in-depth discussions about hot topics such as SND and BYOD with Gartner's analysts and users, allowing analysts in the industry and users to have a new and profound understanding of Huawei EBG's development and vision.

GITEX in Dubai



Dubai, UAE, October 20, 2013 – Huawei, a leading global information and communications technology (ICT) solutions provider, showcased the industry's first service and user experience centered agile network architecture and S12700 series agile switches at GITEX. Huawei S12700 series agile switches accommodate the SDN requirements and can help users build networks easily and enable the network to be more agile for services. During the exhibition, Mr. Swift Liu, President of Huawei Enterprise Networking Product Line, Paul Black, Director of Telecoms MEA at IDC, and experts in the industry together with user representatives have made keynote speeches.

GOVETECH ICT summit in Cape Town, South Africa

From October 21 to 23, 2013, the 2nd GOVETECH ICT summit was held in Cape Town, South Africa. The organizer, State Information Technology Agency (SITA), is an official agency that is responsible for ICT device procurement for the South African government and invited many ICT device vendors in the industry. Huawei unveiled its S12700 series agile switches at the exhibition, attracting significant attention and leading to strong reactions around the world.

Changing the Future with Agile Network

— Huawei Launches the Industry's First Service and User Experience Centered Agile Network and S12700 Agile Switch

Beijing, China, August 8, 2013, – Huawei, a leading global information and communications technology (ICT) solutions provider, today launched the industry's first agile network architecture technology and agile switch, the S12700. With a design that has been developed from a service and user experience perspective, the Huawei S12700 switch supports higher reliability and larger Ethernet frames. This innovative new technology features the key attributes required to support new industry trends including; cloud computing, bring your own device (BYOD), software-defined network (SDN), internet of things (IoT), and big data related analytics for business use.

By launching the first service and user experience centered agile network architecture, Huawei has introduced SDN architecture into campus networks for the first time. This has enabled networks to provide more efficient and agile services and evolve from single-node service processing into full-scale management and control. Huawei S12700 switch forms part of the industry's most advanced series of agile switches, and is expected to lead a new revolution in Ethernet switching technology and network construction. Featuring automatic network deployment and management, the S12700 supports end-to-end (E2E) security collaboration with the flexibility for fast-changing services and full programmability.

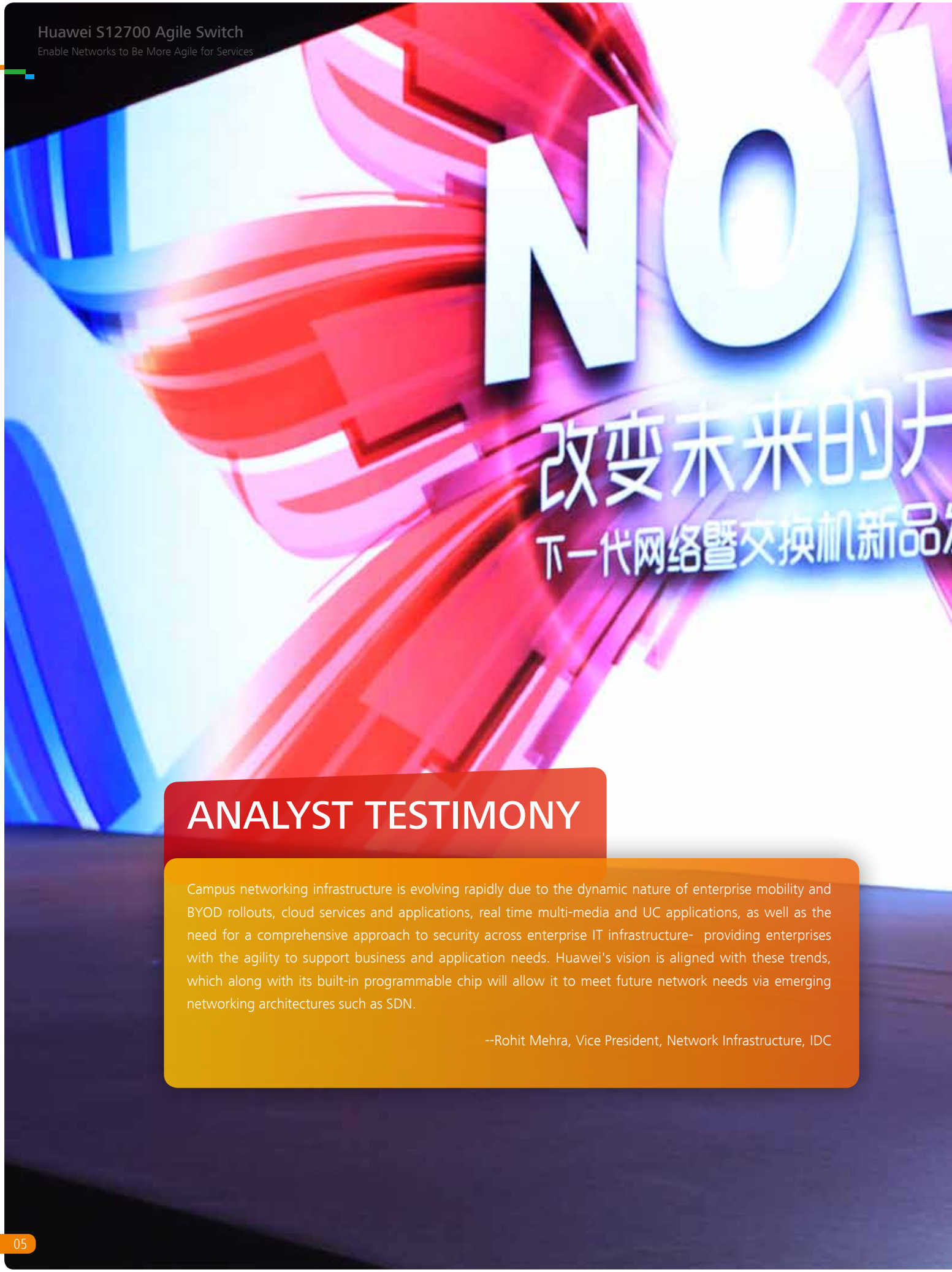
"The inevitable trends of broadband services, multimedia, mobility and social networking are shifting the focus of networks from technologies and devices to services, users and experiences," said Mr. William Xu, Chief Executive Officer, Huawei Enterprise Business Group. "Huawei is committed to customer-centric innovation and open collaboration with the industry, and leveraging our 10 years' experience in enhancing IP network capabilities to best meet the needs of our customers. With the launch of industry's first agile network and agile switch that focus on service efficiency and user experience, I am confident that we will change the future of next-generation enterprise networks."

Photo Caption 1: Mr. William Xu, Chief Executive Officer, Huawei Enterprise Business Group, emphasized Huawei's confidence in changing the future of next-generation enterprise networks at the conference.

In a fast-changing era with emerging technologies and trends such as cloud computing, big data, mobility, and Social Networking Service (SNS), the management of networks now faces three great challenges: insufficient service processing capability, fault location difficulties, and slow service responses. Leadership teams look forward to the availability of networks that can provide more agile services and flexibility to respond to changes in service requirements on demand.

"Campus network infrastructure is experiencing rapid evolution due to the dynamic nature of enterprise mobility and BYOD rollouts, cloud services and applications, real time multi-media and unified communication applications, as well as the need for a comprehensive approach to security across enterprise IT infrastructure. These innovation trends urge enterprises to enhance their abilities to support business and application needs. Huawei's next generation network architecture is aligned with these trends, which along with its built-in programmable chip will enable enterprises to meet future network requirements through emerging networking architectures such as SDN," said Rohit Mehra, Vice President, Network Infrastructure, IDC.

As a leading global device vendor in the IP field, Huawei is committed to meeting the needs of the Ethernet market by launching its groundbreaking new agile network architecture and agile switches. This latest innovation from Huawei marks a significant step in Huawei's efforts to bring more value to its customers and facilitate business transformation, changing the future of the industry.



ANALYST TESTIMONY

Campus networking infrastructure is evolving rapidly due to the dynamic nature of enterprise mobility and BYOD rollouts, cloud services and applications, real time multi-media and UC applications, as well as the need for a comprehensive approach to security across enterprise IT infrastructure- providing enterprises with the agility to support business and application needs. Huawei's vision is aligned with these trends, which along with its built-in programmable chip will allow it to meet future network needs via emerging networking architectures such as SDN.

--Rohit Mehra, Vice President, Network Infrastructure, IDC


HUAWEI

2

Certification & Report

HUAWEI
S12700 Switch
Miercom Report

HUAWEI
S12700 Switch
Tolly Report

Miercom

Lab Testing Summary Report

August 2013

Report SR130801

Product Category:

Enterprise Switch

Vendor Tested:

HUAWEI

Product Tested:

S12700 Series Agile Switches

Miercom PERFORMANCE VERIFIED

Key findings and conclusions:

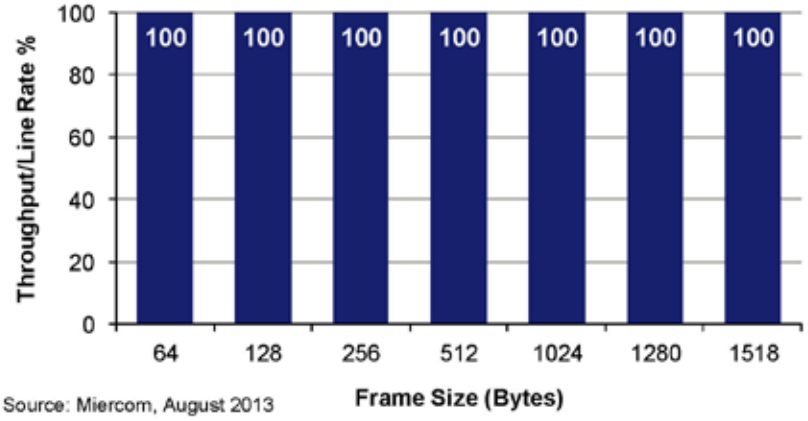
- **Huawei S12708 agile switch demonstrates 100% line rate throughput with 384 10GE ports in full line rate throughput tests**
- **As a next-generation core switch for campus networks, the S12708 switch has full programmability, is SDN ready, and supports Protocol Oblivious Forwarding (POF)**
- **Resilient operation continues with fully loaded 384 10GE ports even after removing one of four switching fabric modules**
- **Ethernet Ring Protection Switching (ERPS) and Smart Ethernet Protection (SEP) demonstrated fault recovery in less than 50 milliseconds on an Open Ring Network**
- **Support for hardware-based Bidirectional Forwarding Detection (BFD) with fast fault detection and switch back without packet loss**

Huawei Technologies engaged Miercom to evaluate the S12700 series agile switches. Testing focused on Software-Defined Networking (SDN) / Programmability capability, performance, throughput, scalability and failover capability.

The S12700 series are LAN switches for campus core applications. There are two models in the series: S12708 and S12712. The S12712 has 12 slots for line card modules. The model tested, the S12708, offers eight slots for line card modules.

Performance testing verified 100% line rate throughput for all packet sizes with zero frame loss, low latency and low jitter. The switching fabric N + 1 redundancy was verified at the conclusion of the throughput test by removing one of the four switching fabric modules while the switch was fully loaded with full-mesh traffic.

Figure 1: Huawei S12708 Agile Switch RFC 2544 Layer 2 Throughput



Source: Miercom, August 2013

The Huawei S12708 agile switch forwarded full line rate traffic with zero loss for all frame sizes tested. The switch was configured with 384 x 10GE ports in full mesh configuration and conducted in accordance with RFC 2544.

The programmability tests involved a Huawei Campus Controller to "program" or direct one or more S12708 switches. The advanced programmability test was one of the first practical examples of SDN that Miercom has observed in hands-on testing.

Feature testing included CPU protection, fast fault detection based on support for Bidirectional Forwarding Detection (BFD) and protection and recovery switching based on support for Ethernet Ring Protection Switching (ERPS).

Throughput Tests

Tests were conducted in accordance with RFC 2544 to determine Layer 2 throughput, latency, jitter and frame loss on the S12708 agile switch.

Layer 2 frames were forwarded at 100% of line rate for all frame sizes with zero frame loss. The frame sizes tested ranged from 64 to 1518 bytes. See *Figure 1* on *page 1*.

The average latency observed across all 384 of the 10GE ports ranged from 3.9µsec for 64-byte packets to 29.7µsec for 1518-byte packets.

The average jitter observed across all ports ranged from 1.8µsec for 64-byte packets to 5.0µsec for 1518-byte packets. See *Figure 2* for both latency and jitter measurements.

Large frames, 1518 bytes, were used to validate aggregate throughput. Small frames of 64 bytes were used to validate packet handling capability.

N + 1 Redundancy

The S12700 series agile switches have four switching fabric modules. Following the RFC 2544 throughput test, for which the S12700 series agile switch was fully loaded with full-mesh traffic, one of the fabric modules was removed, stressing the backplane.

The switch had sufficient capacity in the remaining three switching fabric modules to quickly recover, stabilize and resume operating at full line rate.

Programmability

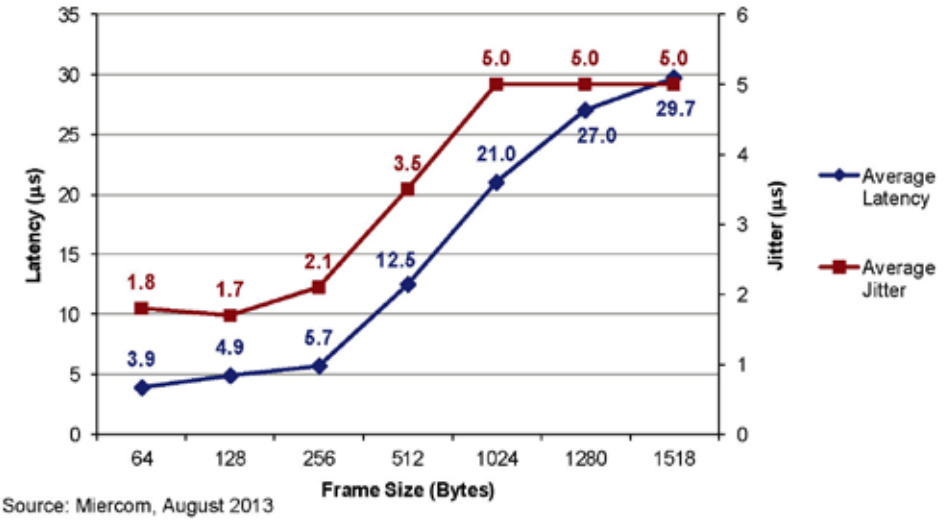
Programmability of the S12700 series agile switches is provided by the Huawei SDN forwarding plane technology, Protocol Oblivious Forwarding (POF). Miercom believes POF to be more capable than the original specification on which it is based, OpenFlow 1.3 from the Open Networking Foundation.

POF offers full backward compatibility with OpenFlow 1.3 and applies to all routing protocols, while OpenFlow applies to only IP routing.

POF provides benefits to user organizations in the present and can future-proof the switching infrastructure for the long haul.

POF enables users to make changes to the switching infrastructure that typically requires a patch from the vendor. Examples include trying a new protocol, testing a new RFC handle or adding a specific security requirement for handling traffic.

Figure 2: Huawei S12708 Agile Switch
Average Latency and Average Jitter

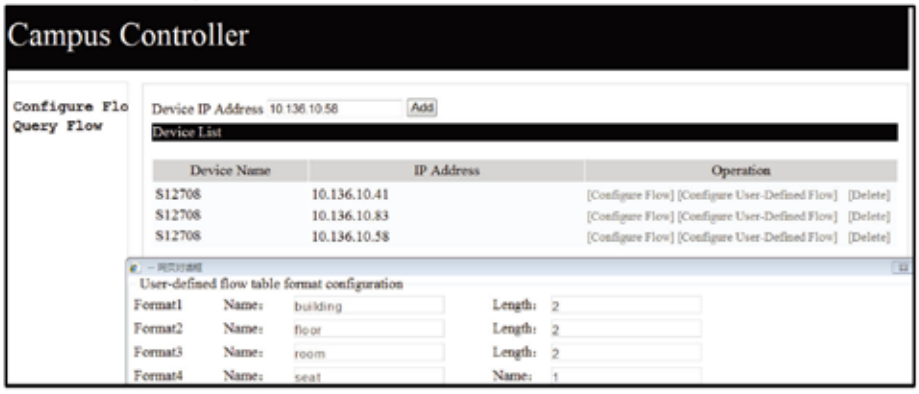


Source: Miercom, August 2013

The Huawei S12708 agile switch demonstrated excellent low latency with consistent (low jitter) performance during testing with full line rate traffic to 384 x 10GE traffic load in accordance with RFC 2544.

The Huawei S12700 series agile switches provide an easy-to-use interface for adding custom header information to Ethernet frames for special purpose use of Software Defined Networking (SDN). In this example, the custom header was specified to indicate specific location details: building, floor, room and seat numbers. Command instructions to the switch could then make traffic forwarding decisions based on these simple locations identified in these fields.

Figure 3: Huawei S12700 Agile Switch Campus Controller Interface



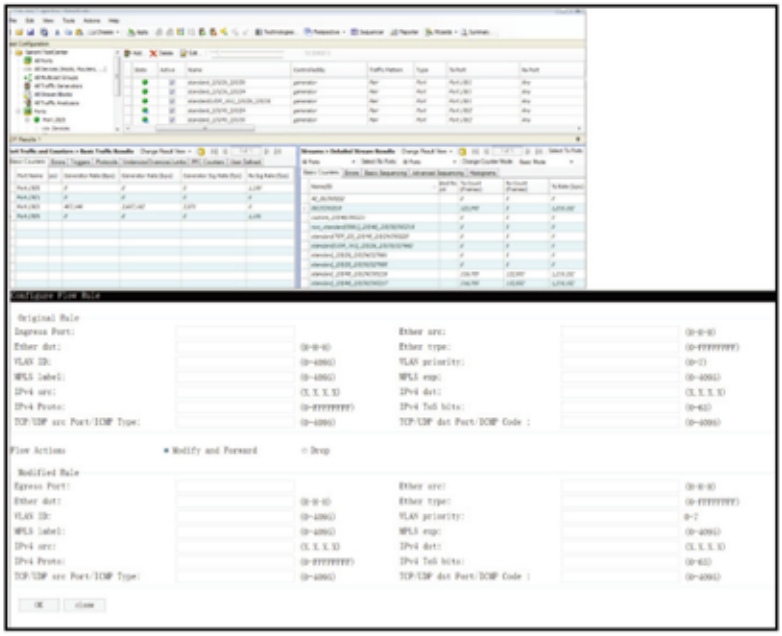
Source: Miercom, August 2013

Because POF applies to all protocols, in the future it will be able to control traffic types that have yet to be introduced.

Basic Programmability A Huawei Campus Controller successfully programmed a S12700 agile switch to forward a non-standard Ethernet packet type, 0x0889, created from the Spirent TestCenter traffic generator.

Usually, a switch will drop non-standard traffic types that are not defined as valid Ethernet frame types. In this test, however, we programmed a S12700 agile switch to forward traffic (non-standard 0x0889 type) generated from the Spirent TestCenter through the switch under test. The Spirent test system accurately reported the non-standard Ethernet frames being forwarded through the switch when it was programmed to do so. We also verified that the switch would drop these non-standard frames when we removed the command to forward the non-standard traffic, as expected.

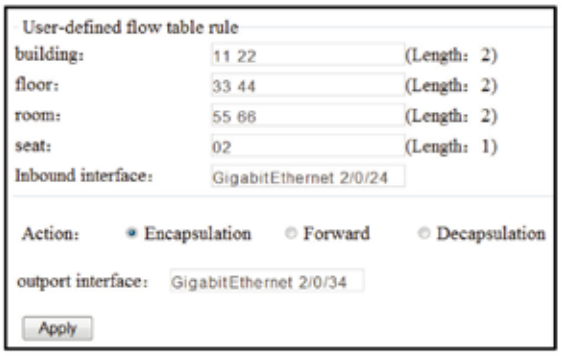
Figure 4: Huawei S12700 Agile Switch SDN Programmable Interface and Spirent TestCenter Generating Custom Ethernet Frames



Source: Miercom, August 2013

The Huawei Campus Controller interface is shown here and used to program the SDN functionality of the S12700 agile switch. The interface of the Spirent TestCenter, shown here, was used to generate traffic and monitor the custom Ethernet frames used in the testing to prove the non-standard Ethernet frame-handling ability of the Huawei S12700 agile switch.

Figure 5: User-defined Flow Table Rule Sets



Source: Miercom, August 2013

A user-defined rule example for the Campus Controller shown here is used to apply, forward or remove the custom header for traffic through the Huawei S12700 agile switch.

Advanced Programmability In this test, three Huawei S12700 agile switches were used to simulate a small campus network. In *Diagram 1* on *page 7*, DUT-2 is the core switch. DUT-1 and DUT-3 are access switches that connect directly to users.

Testing verified that the core switch can be programmed by the Campus Controller to encapsulate packets with a non-standard, additional header containing administrator-defined information.

The Campus Controller also could provide the commands to remove the added header as well as define the destinations to which traffic can be forwarded.

As shown in *Diagram 1*, the non-standard, additional header was user-defined information, including the building, room, floor and seat.

The success of this test was one of the first practical examples of SDN that Miercom has observed in hands-on testing.

Rate Limiting & Blocking Protection

Three tests carried out with the Spirent Test Center validated the ability of the Huawei S12700 series agile switches to protect the CPU from overburdening of resources due to excessive traffic.

Rate Limiting The S12700 agile switch overcame a simulated DoS flood attack of double the designated traffic rate. The Spirent Test Center generated 64 Kbps of traffic. The amount of traffic allowed to pass through the switch by its rate limiting functionality was 32 kbps. CPU utilization stayed below three percent for the duration of the test.

Rate Limiting and Blocking The switch was subjected to DoS flood attack of 150 packets per second, which exceeded the defined threshold.

The switch blocked the IP addresses of offending sources for five minutes. CPU utilization remained less than three percent for the duration of the test.

Whitelist A whitelist of IP addresses that were to be excluded from blocking during the DoS attack in the test were entered into the ACL of a S12700 agile switch.

The switch successfully allowed traffic from the whitelist of IP addresses to pass through uninhibited even when traffic exceeded the threshold for rate limiting and blocking.

The CPU was protected as utilization remained below five percent for the duration of the test.

Note: The Huawei S12700 series agile switches can be configured to send an SNMP alert when the traffic limit is reached.

Bidirectional Forwarding Detection

Linkage Huawei S12700 series agile switches support Bidirectional Forwarding Detection (BFD) linkage between switches.

BFD is a detection protocol that verifies connectivity between network nodes and provides rapid failure detection, while maintaining low overhead. It is a single, standardized method of detecting link, device and protocol failure for any encapsulation topology at any protocol layer and over any media.

One of the problem scenarios that BFD solves is the lack of fast fault detection where no routing protocols exist, such as the lower layers of Ethernet. Without BFD, an Ethernet node cannot rely on an "interface down" event to trigger network reconvergence. It must wait for higher layer protocol timers to time out before determining that a neighboring node is not reachable.

In this test, two Huawei S12700 series agile switches (DUT-1 and DUT-2) and a Huawei S5700 series switch (S57) were linked in a VLAN. A BFD session was initiated between DUT-1 and DUT-2. Linkage was verified as shutting down Port 1 on DUT-1 caused Port 2 on DUT-2 to shut down. See *Diagram 2* on *page 8*.

Linkage under OSPF This test validated the ability of the S12700 series agile switches with BFD enabled and running under Open Shortest Path First (OSPF) to quickly detect a failure, recover in the desired timeframe and reroute traffic.

OSPF is a Layer 3 interior routing protocol for IP networks. Because BFD is protocol-neutral and can be used at any layer, it can provide failure detection under OSPF.

In *Diagram 3* on *page 8*, the two Huawei S12700 series agile switches (DUT-1 and DUT-2) with BFD enabled and running under OSPF were linked with two other Huawei switches (Switch 3 and Switch 4).

The test generation platform delivered routable, 128-byte traffic at 10,000 frames per second (fps) to Port 1 of DUT-1 and Port 1 of DUT-2. The direct route between DUT-1 and DUT-2 was set as higher cost path, forcing traffic to flow via Switch 3 and Switch 4.

A failure was created by disconnecting the link between Switch 3 and Switch 4. The switch over of traffic to the direct (higher cost) path between DUT-1 and DUT-2 and reconvergence occurred in 65 milliseconds (ms), one-third less time than the expected 100ms.

It was very impressive to note that cutover back to the original state occurred without any packet loss under a heavy traffic load condition.

Ethernet Ring Protection Switching

Tests were conducted to validate the support of the Huawei S12700 series agile switches for Ethernet Ring Protection Switching (ERPS), which provides protection and recovery switching in less than 50 ms for Ethernet traffic in a ring topology. It also insures that no loops are formed.

In the event of a failure, a single ring in the ring topology that usually is blocked is unblocked to allow traffic to flow and reconvergence to occur.

ERPS on Open Ring Network This test utilized an ERPS "semi ring" neighboring a Spanning Tree Protocol topology.

The ERPS semi ring in *Diagram 4* on *page 8* consisted of two Huawei S12700 series agile switches (DUT-1 and DUT-2). The tester generated 10,000 fps of routable IP traffic via Path A.

The spanning tree protocol caused the switch to block the connection between the C3750 (Cisco switch) and DUT-2 to avoid a looping condition. Also, the ERPS semi-ring connection blocked Port 6 of S57_1.

A link failure of Port 1 on DUT 1 was introduced. STP switched the state of the connection between the C3750 and DUT-2 to forwarding from blocking, allowing traffic to flow and reconvergence to occur.

Recovery of the spanning tree topology occurred in 139 ms. Recovery to the original topology took 12 ms.

For the ERPS rerouting test, the Port 5 connection from S57_1 to DUT-2 was interrupted, causing the ERPS semi ring to reconverge with traffic flowing through Path C.

Multiple Instances of ERPS Support for ERPS and the ability to properly route traffic through a test network of two ERPS rings was validated in this test. See *Diagram 5* on *page 9*.

The same load of routable IP traffic was used as in the previous test, 10,000 fps.

The Huawei S12700 series agile switches are DUT-1 and DUT-2. Huawei S5700 series switches are S57_1 and S57_2.

Loop avoidance in ERPS is achieved by guaranteeing that at any time, traffic may flow on all but one of the ring links. That link, the Ring Protection Leader (RPL), is blocked under normal conditions. In case of a failure, one end of the RPL is unblocked to allow it to handle traffic.

For this test, Port 3 on DUT-1 was configured as the RPL for one instance of ERPS. Port 2 on S57_1 was configured as the RPL for the second instance of ERPS. The ports initially would be blocked to avoid a looping condition.

Upon interrupting traffic by disconnecting Port 1 on DUT-2, the ring topology reconverged to Path B. The interruption and reconvergence took 16 ms.

The switches in the ERPS rings were set to allow one minute to elapse before reconverging the network, which took 7.25 ms. One minute was a good length of time to help avoid route flapping by ensuring a stable, reconnected state.

Smart Ethernet Protocol

This test proved the S12700 series agile switches can successfully reroute traffic through a hybrid environment with fast reconvergence, minimum cutover times and no route flapping. A hybrid ring consisting of a SEP "semi ring" neighboring a Multiple Spanning Tree Protocol (MSTP) network was utilized. See *Diagram 6* on *page 9*.

Smart Ethernet Protection (SEP) protocol delivers fault convergence in under 50ms for ring networks. Multiple Spanning Tree Protocol (MSTP) configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

In the test bed, the DUT is a S12700 agile switch. C3750, a Cisco switch, is the root switch for the MSTP network. S57_1, S57_2 and S57_3 are Huawei S5700 series switches.

In normal state, the MSTP topology blocks Port 3 of the DUTs to prevent a looping condition. Also, the SEP semi-ring topology blocks Port 6 of switch S57_3.

Upon interrupting Port 2 on the DUT, the MSTP reconverged to allow traffic to flow in 19.7 ms.

When the port connection was restored, cutover back to the original topology took 22.4 ms after the configured wait time of one minute to avoid route flapping.

A second interruption, Port 5 of the DUT, forced a reconvergence of the SEP semi ring. Traffic was then rerouted to Path C. The time needed to reconverge was 45.7 ms.

When the port connection was restored, cutover back to original topology took 8.4 ms after the configured wait time of one minute to avoid route flapping.

Easy Operation Solution

Two tests verified the functionality of the Easy Operation Solution in the Huawei S12700 series agile switches. The functionality is rare and ingeniously simple.

The first test utilized a S12700 agile switch as a "commander" to aid in the initial configuration of new devices on the network. In the second test, the commander aided in updating software of the same devices.

In *Diagram 7* on *page 9*, the S12700 agile switch is the DUT. When new, un-configured devices were added to the network (Huawei S5700 switches, S57_1 client and S57_2 client), they obtained the configuration file from the SFTP server in the following way. They contacted the gateway (DHCP server) to obtain the IP address of the commander, which redirected to the SFTP server.

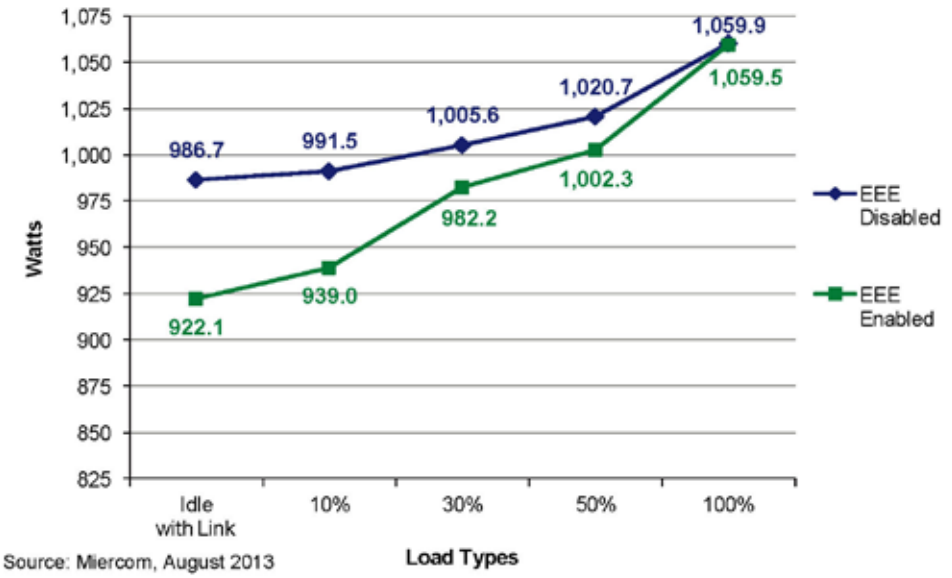
In the second test, Client1 and Client2 followed the same path to the SFTP server to update software. Examples of software that can be updated include the configuration file and firmware. Patches also can be received in this way, a time-saving alternative to contacting the vendor.

As a commander, the Huawei S12700 series agile switches can command 255 devices.

Energy-Efficient Ethernet

This portion of testing validated support of the Huawei S12700 series agile switches for IEEE

Figure 6: Huawei S12700 Agile Switch Power Savings Due to Energy Efficient Ethernet (IEEE 802.3az)



Source: Miercom, August 2013

The Huawei S12700 agile switch exhibits very low power consumption during fully loaded 384 x 1GE port tests. Additional energy savings was achieved when 802.3az Energy Efficient Ethernet setting was enabled on the switch. The switch exhibits lower power consumption than most switches in this class, even before the EEE savings feature was enabled.

802.3az, the Energy Efficient Ethernet standard, which allows energy to be saved on a per-port basis by capitalizing on the periods of inactivity between packet transmission and powering down the physical interface for brief periods of time during periods of low link utilization.

The S12700 agile switch was tested for power consumption with EEE disabled. Results then were compared to results with EEE enabled.

With all 384 links up, no traffic and EEE disabled, the measured power consumption for the S12700 agile switch was 986.7 watts. It is a testament to the switch's energy-efficient switching fabric that consumption only increased by less than 74 watts, to 1,059.9 watts while handling a 100% load of Layer 2, IMIX traffic.

With EEE enabled, the S12700 agile switch consumed 922 watts with all 384 links up and no traffic applied. It then was tested while handling various levels of IMIX traffic: 10% (939 watts), 30% (982), 50% (1,002) and 100% (1,060). See *Figure 6* on *page 6* for more details.

MAC Address Table Capacity

Testing verified a capacity of 1,048,576 addresses for the MAC table of the Huawei S12700 series agile switches. This number is slightly higher than the vendor specification of one million.

FIB Routing Table Capacity

Testing verified a capacity of 3 million IPv4 routes and one million IPv6 routes.

Bottom Line

The Huawei S12700 series agile switches can play a significant role in campus networks now and for years to come, thanks to its future-proof design and capability to accommodate evolving user needs.

Key components of the future-proof design include large capacity of MAC, FIB and ARP tables as well as its SDN-ready/programmable architecture.

Overall, we found the Huawei S12700 series agile switches to be full-featured, high-performance Layer 2 and Layer 3 Ethernet LAN switches for core campus network applications.

The switches provide a strong combination of high performance, a rich feature set, high resiliency and excellent programmability for multiple protocols.

Diagram 1: Programmability

Enhanced Function of Programmability

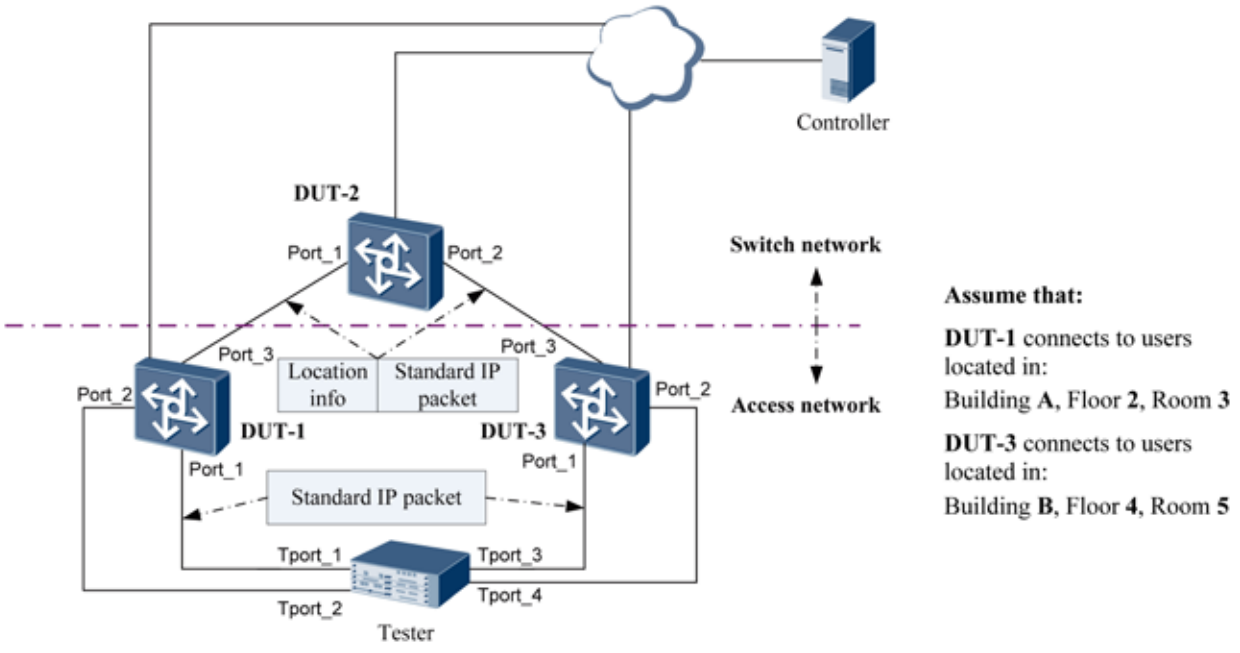


Diagram 2: Bidirectional Forwarding Detection
Linkage between BFD and Interface

Diagram 3: Bidirectional Forwarding Detection
Linkage under OSPF

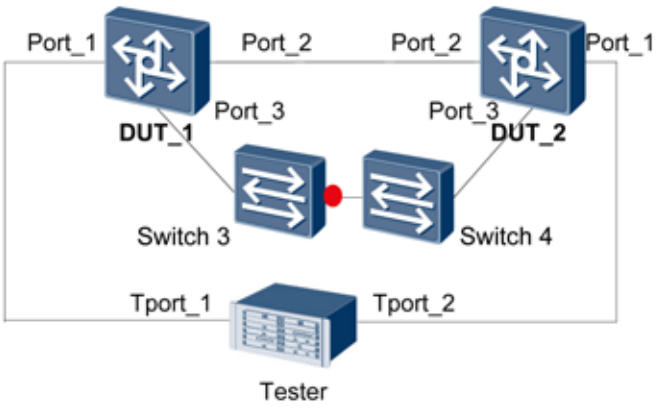


Diagram 4: Ethernet
ERPS (G.8032) on an Open Ring Network

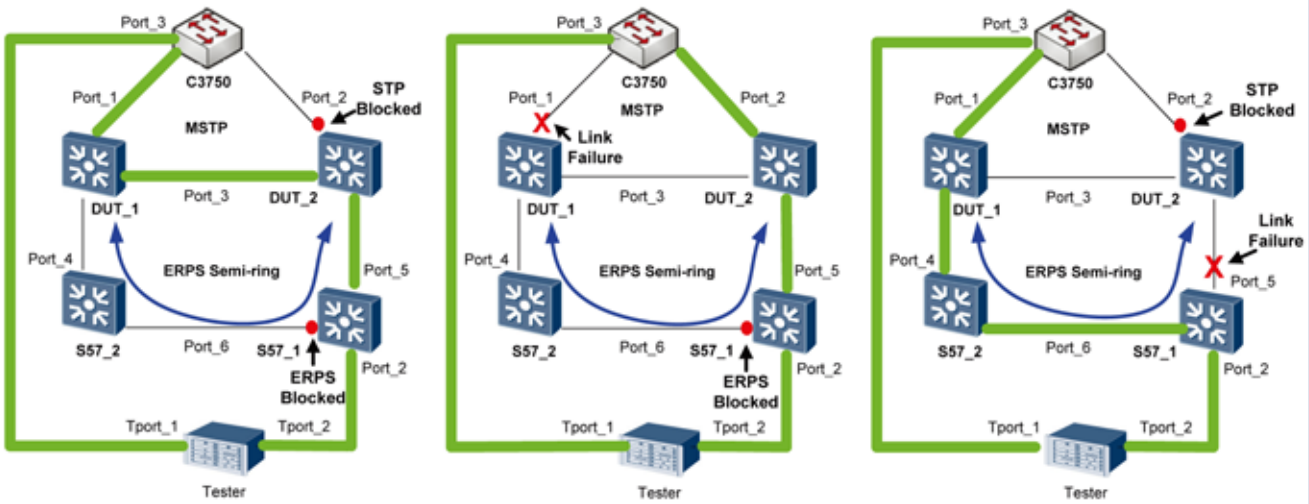


Diagram 5: Ethernet - ERPS Multi-Instance

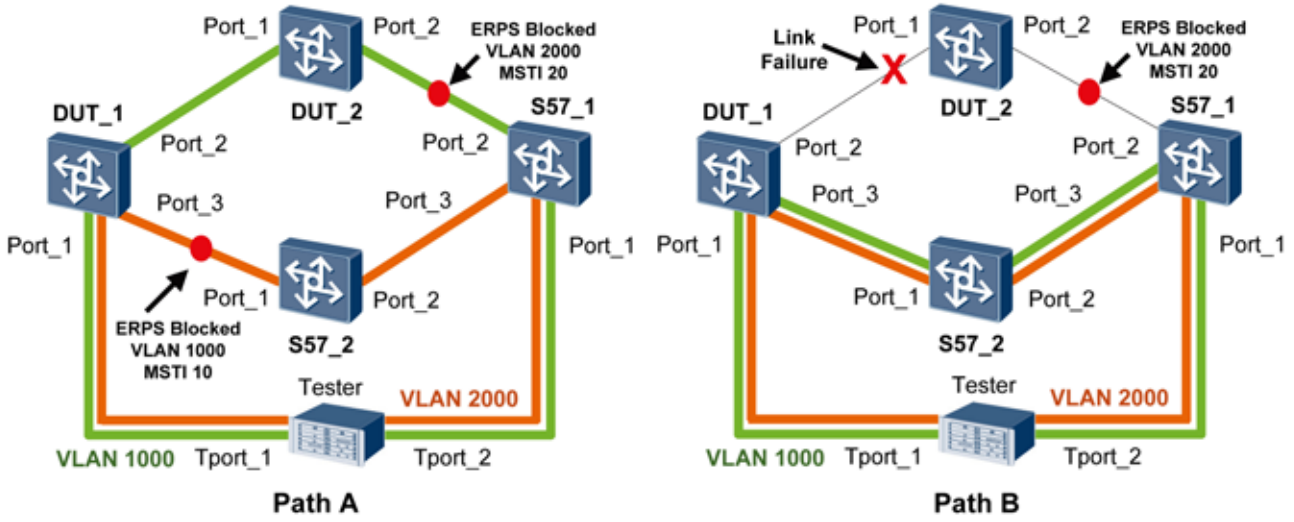


Diagram 6: SEP on an Open Ring Network

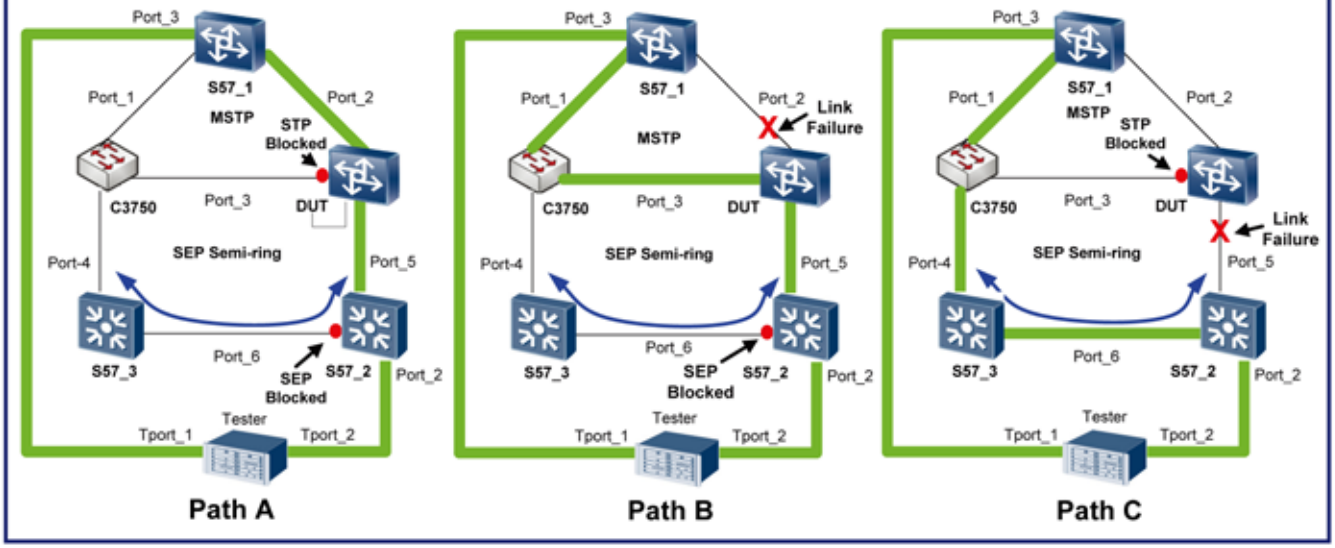
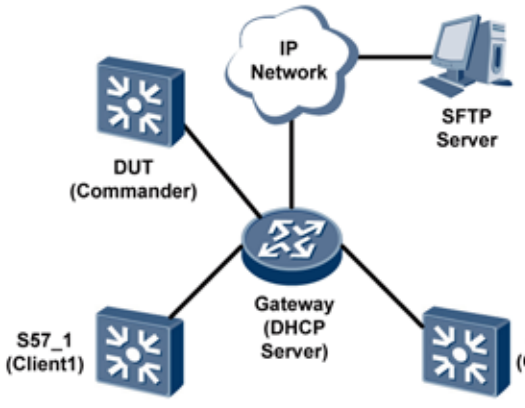
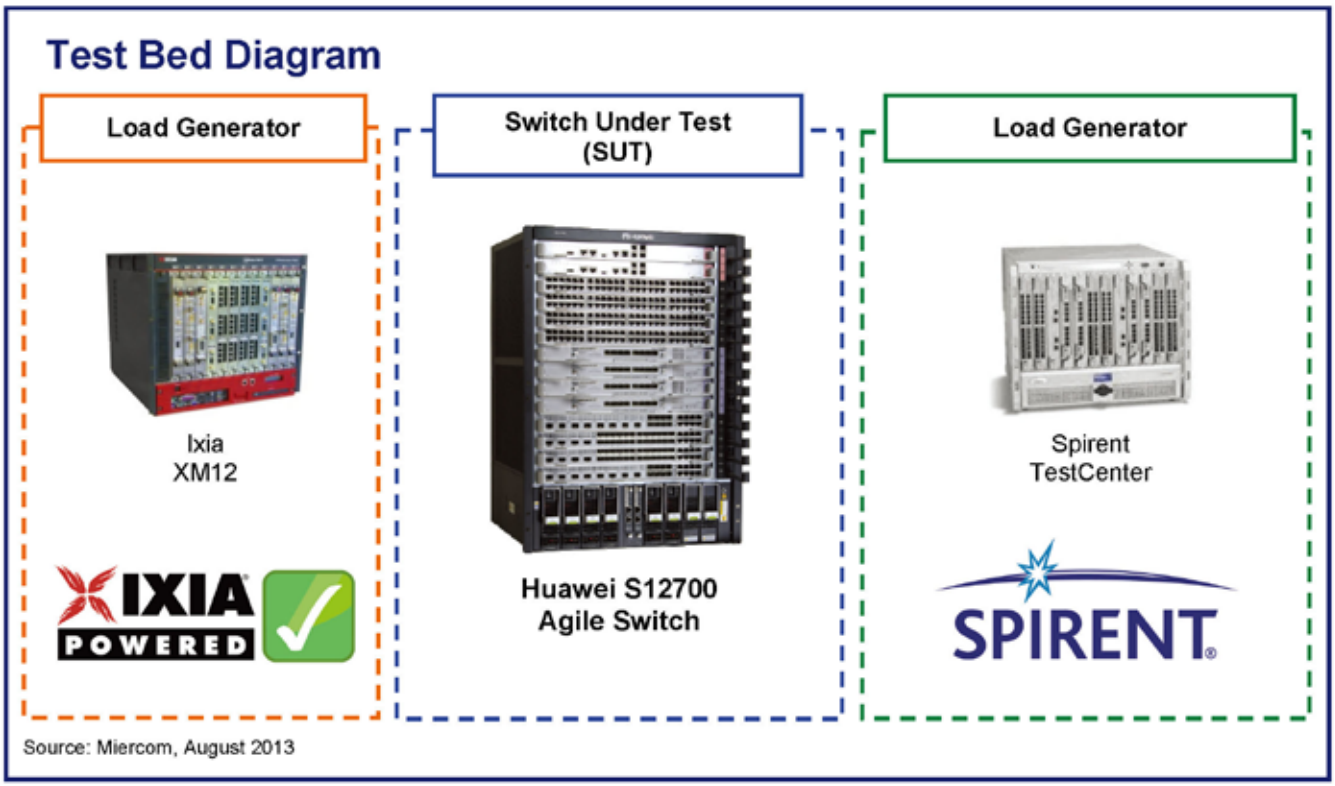


Diagram 7: Easy Operation with Commander



This topology was used for demonstrating deploying new devices, updating software and loading patches through SFTP.



How We Did It

The Huawei S12700 agile switch was evaluated for Software-Defined Networking (SDN) programmable capability, performance, features and energy efficiency. The Huawei S12700 agile switch chassis evaluated was running the latest firmware available. We tested the Huawei S12708 agile switch, however, while on-site, we also observed the operation of other switches in the S12700 series. Specific results apply to the Huawei S12708 switch, but general implementation procedures are the same for all models in the Huawei S12700 series agile switches.

For performance testing, Miercom and Huawei engineers used load generators to ensure that the maximum potential of the switch was validated. For feature testing, the load generators were configured to specifically test certain functionalities to verify that they were working appropriately and routing correctly. Energy efficiency was determined by measuring energy consumption without any energy saving features enabled and then repeating the testing with these features turned on to compare savings.

State of the art, industry recognized test and measurement equipment was used in the testing. Two different traffic generators were used including the Ixia XM12 running IxNetwork version 5.50.121.48 and Spirent TestCenter running version 3.76.0076.

Utilizing RFC 2544, RFC 3918, and RFC 2889 standards for load testing, Miercom was able to obtain industry applicable metrics for latency, throughput, and other statistical measurements such as out of sequence errors and jitter to ensure validity of the metrics observed. Analyzing the statistics, we were able to produce accurate results for public distribution.

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 S12700 series agile switches was verified by Miercom in hands-on testing.

The switches proved fully programmable, full line rate throughput, and excellent resiliency and redundant fault tolerant configuration. Excellent, below industry average power consumption was noted while the switch was fully loaded in test scenarios.

The switches achieved the performance required for applicability in a campus core deployment and achieved the Miercom Performance Verified Certification.

Huawei S12700 Agile Switch

HUAWEI

Huawei Technologies, Co., Ltd.
www.huawei.com

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.

Miercom

Report SR130801 reviews@miercom.com www.miercom.com

Before printing, please consider electronic distribution

TEST REPORT
Tolly.

#213136
August 2013
Commissioned by
Huawei Technologies Co., Ltd

Huawei S12700 Series Agile Switches

Programmable Capability, Performance and Feature Validation

Executive Summary

Innovative services put new demands on the network. Centralized management, application and network decoupling as well as programmable capability are key features in high-end networking.

Using a fully programmable switching architecture, the S12700 Series Agile Switch allows fast, flexible feature customization and supports a smooth evolution to software-defined networking (SDN). According to Huawei, the S12700 series uses Ethernet Network Processor (ENP) chips and provides native WLAN AC functions to help build a wired and wireless converged network.

Tolly engineers verified Huawei S12700 series' programmable capability which supported forwarding standard and non-standard packets with user-defined flows.

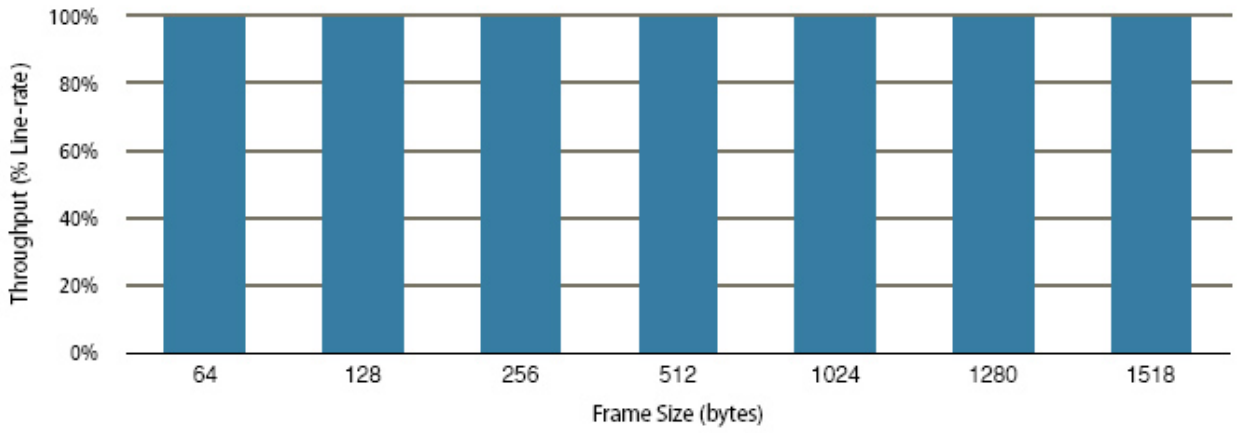
Tests also showed that the Huawei S12700 Series Agile Switch under test delivered 100% line rate throughput at all frame sizes tested scaling up to 384 10GbE ports with switch fabric module N+1 redundancy. See Figure 1.

The Bottom Line

Huawei S12700 Series Agile Switches:

1. Are SDN ready with the support of Protocol Oblivious Forwarding (POF) and Full Programmability
2. Support switch fabric module N+1 redundancy with line-rate full-mesh traffic across 384 10GbE ports
3. Provide million-plus MAC and FIB table capacity
4. Support copying packets on mirroring ports to 64 observing ports simultaneously

Huawei S12708 Agile Switch Layer 2 10GbE Ethernet RFC2544 Throughput
384 10GbE Ports in Full-mesh across Eight Interface Modules
(as reported by HUTAF Tesgine 2.0 version 100.002.00.027)



Note: Eight ET1D2X48SEC0 48x10GbE ports interface modules on one S12708 Agile Switch were tested. Test results were the same with either 3 or 4 ET1D2SFUD000 switch fabric modules.

Source: Tolly, July 2013

Figure 1

Executive Summary (Con't)

Tolly engineers verified Huawei's S12700 Series Agile switches in multiple areas including programmable capability, switch fabric module N+1 redundancy, MAC, ARP, FIB tables' capacity, N:64 port mirroring and CFM OAM features. See Table 1.

Test Results

Programmable Capability

Tolly engineers evaluated two aspects of the Huawei S12700 Agile Switches' Protocol Oblivious Forwarding (POF) support and programmable capability.

First, Tolly engineers verified that the S12700 could encapsulate/decapsulate packets with non-standard headers and forward packets with user specified flows. This feature gives users the possibility to define their own protocols to forward packets. One typical user case with this feature is location-based forwarding. Packets can be forwarded according to the Ethernet ports' building, room, etc.

Secondly, Tolly engineers verified that the S12700 can match standard packets with headers like Ethernet type, IP destination, MAC destination, etc. and then take actions like forwarding, dropping or modifying according to the user-customized flow table.

Performance

Switch Fabric Module N+1 Redundancy

Tolly engineers verified that, with either 3 or 4 fabric modules, the S12708 can always provide 100% line-rate full-mesh throughput using 384 10GbE ports across 8 interface modules with 64-, 128-, 256-, 512-, 1024-, 1280- and 1518-byte frame sizes. See Figure 1.

Fabric Connection per Slot

Tolly engineers verified that the S12708 could pass 100% line-rate cross-board traffic (480Gbps bidirectional, 960Gbps aggregated) between two 48x10GbE ports interface modules with zero-loss using 64-, 128-, 256-, 512-, 1024-, 1280- and 1518-byte frame sizes. See Figure 2. As a result, 480Gbps fabric connection per slot was verified in the test.

Huawei Technologies, Co., Ltd

S12700 Series Agile Switches

Performance Evaluation and Feature Validation

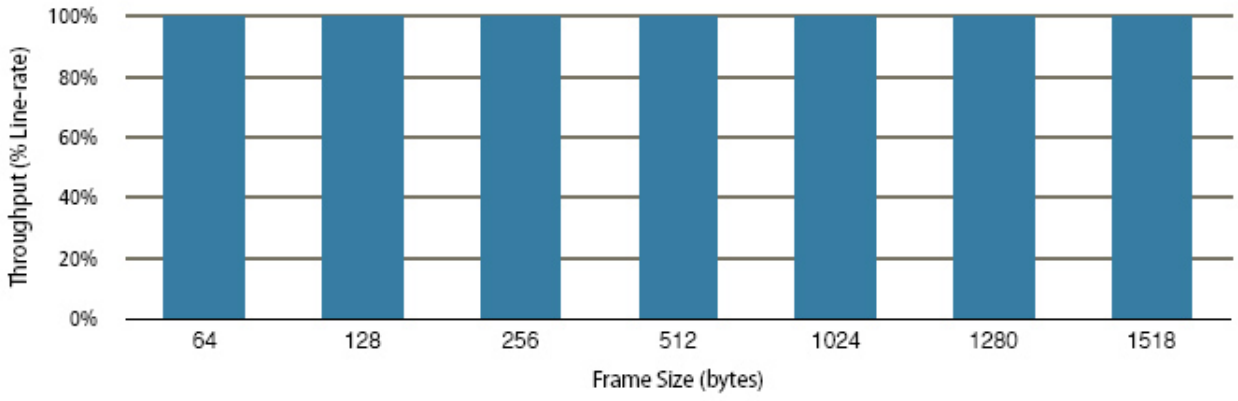
Tolly. Certified

Tested July 2013

Capacity

Tolly engineers evaluated the capacity of S12700 series' MAC table, ARP table, FIB table, port buffer, NetStream and ACL rules. See Table 1.

Huawei S12708 Switch Layer 2 10GbE Ethernet RFC2544 Throughput
96 10GbE Ports across Two Interface Modules - Traffic Distribution Mode: Backbone
(as reported by HUTAF Tesgine 2.0 version 100.002.00.027)



Note: Two ET1D2X48SEC0 48x10GbE ports interface modules on one S12708 switch were tested. Each port on each interface module sent traffic to all 48 ports on the other interface module. 960Gbps aggregated throughput were demonstrated between two interface modules for all frame sizes tested.

Source: Tolly, July 2013

Figure 2

MAC Table Capacity

The S12700 supported 1,048,576 addresses in its MAC table. Traffic matching all MAC addresses in the MAC table passed through without loss.

ARP Table Capacity

The S12700 supported 262,144 entries in its ARP table. Traffic matching all entires in the ARP table passed through without loss.

FIB Table Capacity

The S12700 supported 3,000,000 IPv4 routes in its FIBv4 table. Traffic matching all routes in the FIBv4 table passed through without loss.

The S12700 supported 1,000,000 IPv6 routes in its FIBv6 table. Traffic matching all routes in the FIBv6 table passed through without loss.

Port Buffer

Tolly engineers verified that one 10GbE port on the ET1D2S08SX1E 8x10GbE port interface module supports 244ms buffer with line-rate traffic.

NetStream Capacity

1,048,576 bursts, each with a unique source IP address, were sent through an S12700 switch. Tolly engineers verified that S12700's NetStream function could analyze all 1,048,576 entires and forward the information to a specified port.

ACL Capacity

256,000 ACL rules were applied to one S12700 switch. Each rule pointed to one exclusive MAC address. Tolly engineers verified that 256,000 ACL rules could all work to block traffic.

Features

N:64 Port Mirroring

The S12700 supports N:64 port mirroring. Tolly engineers tested mirroring 3 ports to 64 ports. All 64 ports received all traffic mirrored from the 3 ports.

CFM OAM

Connectivity Fault Management (CFM) is a protocol for Operation, Administration and Maintenance. Tolly engineers verified that Huawei S12700 sent out and received CFM monitoring packet every 3.3ms.

Test Setup & Methodology

Test Environment

One Huawei S12708 and one S12712 switch were used in the test. See Table 2.

Test Methodology

Layer 2 Throughput

Eight Huawei HUTAF Tesgine 2.0 (each with six Multiport 10G Data Generation and Analysis Boards) were used to run the RFC2544 throughput tests.

Full-mesh: traffic from each port to all other ports.

Backbone: traffic from each port to all ports on the other interface module.

Huawei S12700 Series Agile Switches
Tolly Certified Features/Functionality

	Feature Description
✔	POF Support and Programmable Capability
✔	Switch Fabric Module N+1 Redundancy
✔	MAC table capacity: 1,048,576
✔	ARP table capacity: 262,144
✔	FIBv4 table capacity: 3,000,000
✔	FIBv6 table capacity: 1,000,000
✔	10GbE port buffer on ET1D2S08SX1E line card: 244ms with line-rate traffic
✔	NetStream Capacity: 1,048,576 entries
✔	ACL Capacity: 256,000 rules
✔	N:64 Port Mirroring
✔	3.3ms CFM OAM

Source: Tolly, July 2013 Table 1

Tolly.

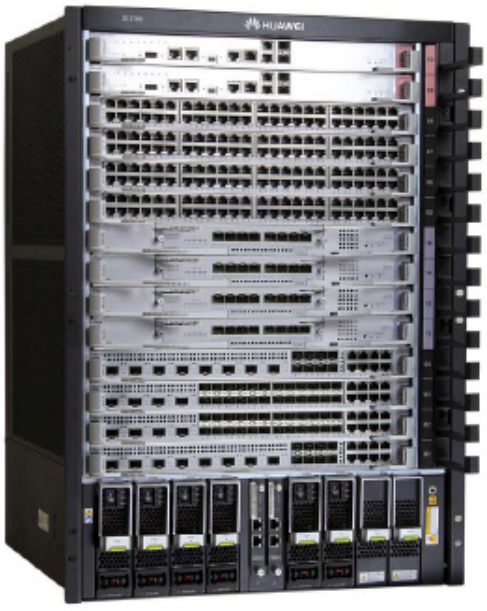
Huawei S12700 Series Agile Switches Performance and Features #213136

Device Under Test

Product	Software Version
Huawei S12708, S12712 Switch Chassis	Huawei Versatile Routing Platform (VRP) V200R005C00
ET1D2MPUA000 Main Processing Unit (MPU)	
ET1D2SFUD000 Switch Fabric Unit	
ET1D2X48SEC0 48-Port 10GBASE-X Interface Card	
ET1D2G48SX1E 48-Port 100/1000BASE-X Interface Card	
ET1D2S08SX1E 8-Port 10GBASE-X Interface Card	

Source: Tolly, July 2013 Table 2

Performance Test Bed



Huawei S12708 Agile Switch

384 10GbE links

8 x HUTAF Tesgine 2.0 (each with six Multiport 10G Data Generation and Analysis Boards)

Note: Eight ET1D2X48SEC0 48x10GbE ports interface modules were equipped on the S12708 switch to provide 384 10GbE ports.

Source: Tolly, July 2013 Figure 3

Tolly.

Huawei S12700 Series Agile Switches Performance and Features #213136

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at: http://www.tolly.com

Test Equipment Summary

Vendor	Product
Huawei	Avenue 蝴蝶HUTAF Tesgine HUTAF Tesgine 2.0 Traffic Generator/Analyzer Version: 100.002.00.027

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

213136-iv-2--yx-wt-2013-08-01-VerM

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Next-Generation Networking for the Smart Enterprise Campus

Sponsored by: Huawei

Rohit Mehra
August 2013

EXECUTIVE SUMMARY

Today, network administrators are under pressure to meet demanding business requirements. They must provide users with high levels of application availability, ensure network security, and provide flexibility to incorporate future services and applications as business needs change.

Nowhere is this truer than in the campus network, a critical link through which users interact with applications and data. A variety of trends have placed greater demands on the campus network in recent years, including the explosion in mobile devices in the enterprise brought about by the consumerization of IT and bring your own device (BYOD). Campus networks must handle increasing use of cloud services and data-intensive applications, including video and VDI. As mobile devices become the norm, the environment must incorporate wireline and wireless seamlessly and securely. Yet at the same time, network administrators must introduce simplicity and greater levels of manageability to reduce their own burden.

To address these requirements, Huawei has launched a new series of campus networking products that combines wireless and wireline networks into a single converged network. The series introduces policy-based management at the user level and at the application level so that administrators do not have to worry about specific ports or topologies. It also provides higher quality of service (QoS) through the introduction of new technologies designed to tailor QoS to specific user and application needs and to detect and bypass failures in the network.

With this innovative new approach, the Huawei campus solution not only is designed to improve the user experience while providing support for key trends in today's enterprise but also is intended to simplify the management burden and provide automated monitoring and control while leaving the door open to new network services and application needs in the future and greater levels of programmability and network virtualization. It even provides a direct upgrade path to software-defined networking (SDN) when the organization is ready to take that step. The Huawei campus solution provides enterprise networks with agility to enable rapid changes to services and applications.

SITUATION OVERVIEW: COMPLEX DYNAMICS OF TODAY'S ENTERPRISE IT ENVIRONMENT

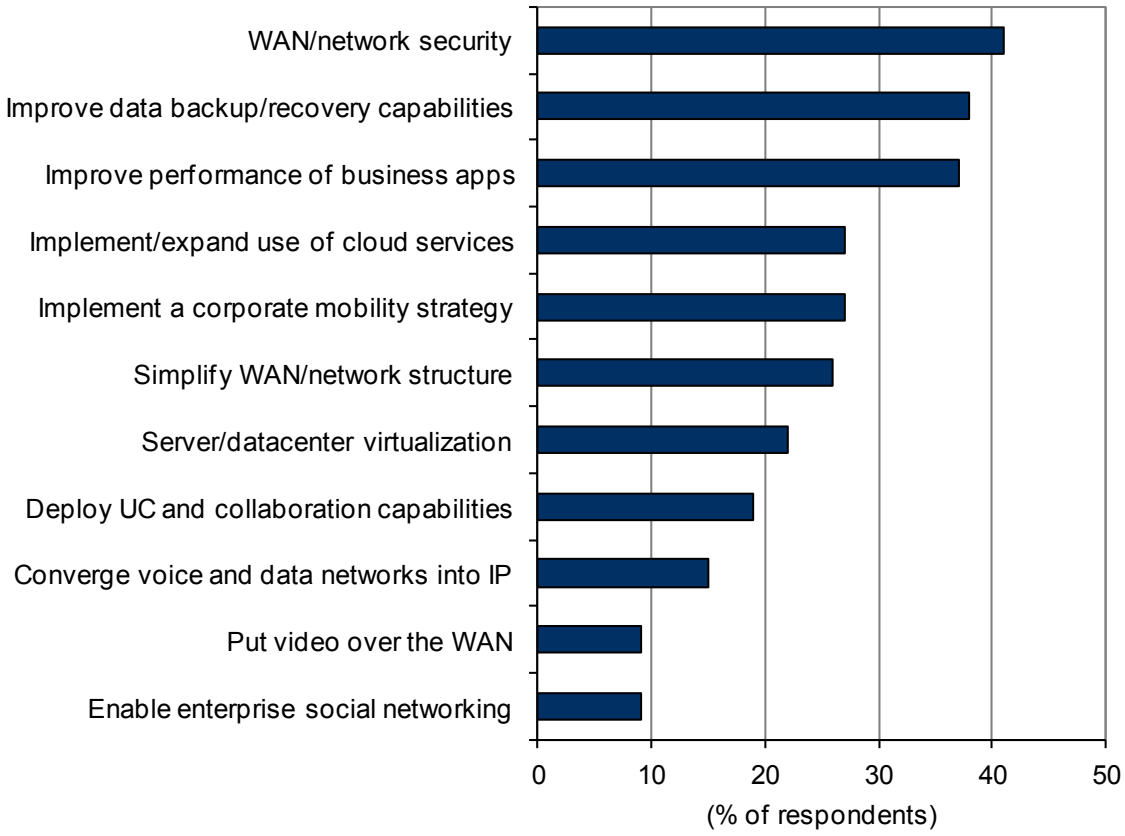
Enterprise network managers must balance a variety of needs, including providing users with high levels of application access and availability in a highly secure environment while still incorporating sufficient levels of flexibility to allow the introduction of new network services and applications as required in the future.

Figure 1 illustrates some of these conflicting demands. When asked to list their most important technology initiatives, network managers most frequently cited security and backup and recovery, followed closely by performance of business apps, cloud services, and mobile strategy. They also said it is important to introduce greater simplicity into their network environment. This shows how network managers are being pulled in multiple directions to balance conflicting demands from the enterprise.

FIGURE 1

Key Technology Initiatives: Performance, Security, and Backup

Q. Of the following technology initiatives, which three are the most important to your organization at the moment?



n = 1,212

Source: IDC's *U.S. WAN Manager Survey*, 2012

As the gateway to the enterprise IT infrastructure, the campus network is on the front line to support critical enterprise requirements, including consumerization of IT, cloud computing, and video and VDI. While these technologies have created opportunities for employees and the enterprise alike, they also have created challenges for network administrators.

Consumerization of IT

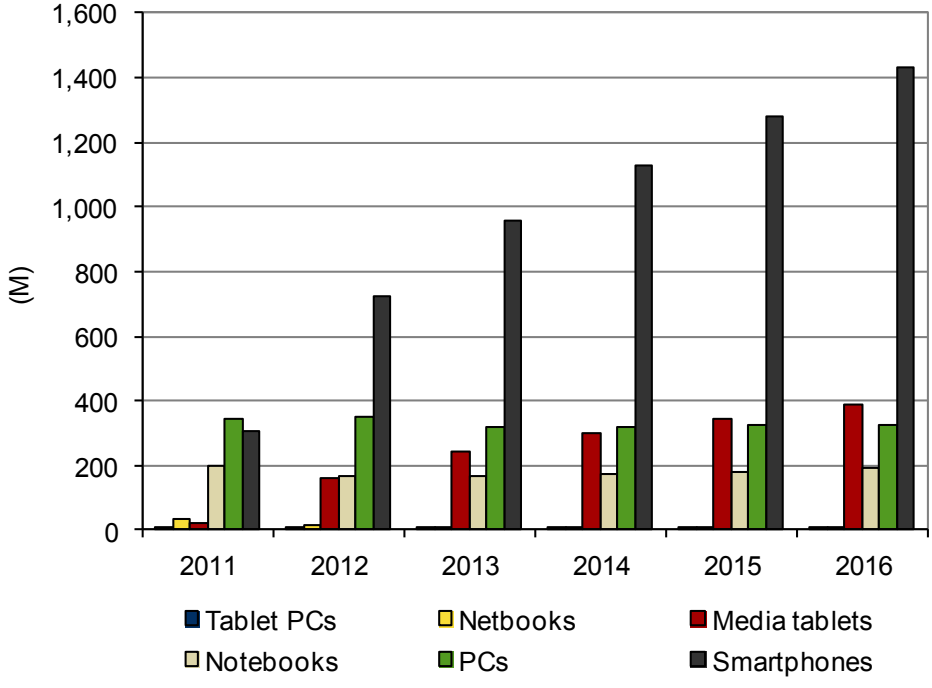
Consumerization of IT, in which technologies originally designed for the consumer market are being adopted for enterprise use, is having a major impact on today's enterprise IT environment. These technologies include mobile devices such as smartphones and tablets as well as applications such as social media and cloud file sharing. Originally brought into the enterprise environment by employees without permission from the enterprise, these devices and applications have become so widespread that enterprises have begun proactively supporting them.

Growth in Mobility and Bring Your Own Device

The poster child for the consumerization of IT is the explosion of smart mobile devices in the enterprise. While IDC research has shown that PCs remain the most important device for getting work done, information workers are increasingly reliant on mobile devices, including smartphones and tablets, for work purposes. Figure 2 shows the growth forecast for these devices.

FIGURE 2

Worldwide Mobile Device Shipments, 2011–2016



Source: IDC, 2013

While some mobile devices are owned and supplied by the enterprise, a large number continue to be employee owned or purchased. A recent IDC study speaks to the magnitude of the impact these devices have on the business: In 2012, 68% of employee-owned devices (i.e., BYOD) were being used to access enterprise applications — up sharply from the 45% that were doing so in 2010.

Even as the use of mobile devices has made employees more productive and businesses more competitive, IT organizations are scrambling to support these devices while maintaining security and control. Another recent IDC study showed that while 83% of IT respondents believe that tablets and similar devices will be integral to how their organizations will conduct business in the future, 80% believe that IT's workload will increase as employees bring consumer devices into the workplace.

In the few short years that employees have been bringing their own devices to the office for work, the question is no longer whether IT should support them but how it can provide the foundation to manage and secure devices while providing an appropriate user experience for application access. IT needs to put in place device-aware policies at the user level to ensure that users can access applications in the manner most appropriate to their needs.

Cloud Computing

Another major trend in enterprise IT is cloud computing. Most IT organizations realize the benefits cloud can bring, including reducing complexity in their environment, easing the workload for internal IT staff, and reducing the variety of skill sets they need to keep in-house. It can also help IT more rapidly scale compute resources when required and adjust to shifting business requirements.

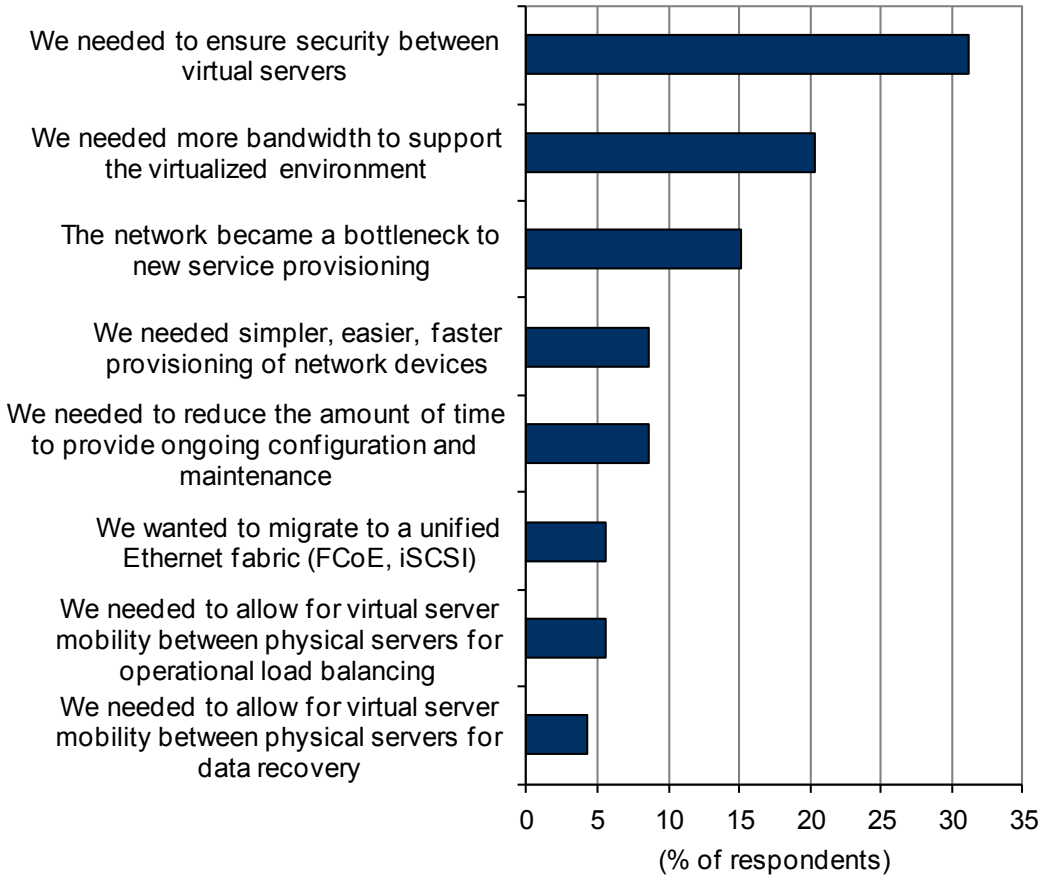
IDC has witnessed significant growth in cloud computing and expects it to continue. Worldwide revenue from public IT cloud services exceeded $21.5 billion in 2010 and will reach over $70 billion in 2015, representing a compound annual growth rate (CAGR) of over 25%. This rapid growth is over four times the growth projected for the worldwide IT market as a whole (6.7%).

IDC expects that a significant number of new cloud rollouts will consist of private cloud deployments as enterprises look to realize the complementary benefits of keeping some cloud resources in-house while leveraging public cloud services for the remainder. As shown in Figure 3, security, bandwidth, and provisioning are major concerns for enterprises looking to implement private cloud.

FIGURE 3

Drivers for Rearchitecting the Network to Support Private Cloud

Q. What was the main reason you needed to rearchitect the network to support private cloud?



n = 251

Source: IDC's *Virtualization Survey*, 2012

Cloud services complement and reinforce the trend toward BYOD and mobile device growth in the enterprise. Cloud-enabled enterprises provide application access over BYOD in a secure manner. It is important to note that BYOD itself is not sufficient to enable enterprise mobility; rather, cloud-based applications and services that are connected with mobile devices enable workers to conduct critical business functions.

Businesses cannot afford cloud services to become inaccessible for any reason — including the network. As more employees depend on the cloud for day-to-day activities, the campus network must deliver consistent, high-quality performance. This is particularly true for mission-critical cloud-based applications for which quality of service and availability cannot be compromised.

Wired and Wireless Convergence

Traditionally, wired and wireless networks have operated in separate realms. Wireless networks have been deployed as overlays to the wireline network, with separate policies, tools, and management. This introduces risk as policies and practices can be applied inconsistently across wireline and wireless networks, increasing the administrator's burden and driving up management costs and complexity.

The growth of mobile devices has placed greater demand on the wireless network. As more business-critical applications are accessed across the wireless network — through both mobile devices and laptops — enterprises can no longer afford to treat wireless networks differently than wireline networks. By unifying wired and wireless networks into a single converged infrastructure, businesses can gain greater levels of manageability and improve user experience. They can improve levels of performance and flexibility and improve their security and policy stance.

Increasing Video and VDI

The use of video on the enterprise desktop is quickly becoming a common method for employees to communicate with each other as well as with customers, partners, and suppliers. In a recent IDC survey, over one-third of all organizations reported that they currently use some type of video, such as desktop videoconferencing or telepresence, and another one-third indicated that they plan to do so within the next one to two years. Yet video introduces specific challenges into the network, including large data flows, bursty traffic, and high degrees of sensitivity to packet loss.

The virtual desktop is also seeing increased growth within IT environments, with the worldwide market expected to exceed $2 billion in 2013. By enabling desktops to be managed and administered from a central location, organizations can achieve significant operational cost savings and greater levels of security because they can maintain greater levels of control over desktop patches and upgrades.

Security

IT must provide users with seamless access to applications and services, whether housed in the enterprise datacenter or delivered via the Internet. But at the same time, IT needs to maintain security and control over its network. This becomes more challenging as more data and applications move to the cloud and a greater number of enforcement/demarcation points are introduced into the network.

Security must be provided on multiple fronts from business practices and policies to provisioning, management, and operations. Organizations must ensure that policies are constantly kept in sync and up to date across their networks so that, for example, once an employee leaves the organization, IT can quickly act to deny access to any sensitive data.

Impact on the Campus Network

The campus network is a vital link enabling communication and collaboration both across and outside the enterprise. To enable users to access the applications and resources they require and support the emerging trends discussed previously, the campus network must adhere to a number of requirements:

- **Cloud readiness.** The network must support the ability for users to access compute resources via public cloud or in a public/private cloud model in a secure manner while still providing high quality of service.

- **Content awareness.** Users accessing different applications via different devices place different levels of demand on the network. The network should understand which applications and users represent mission-critical needs and/or are highly sensitive to latency and adjust the service quality accordingly.

- **Flexibility to support advanced network services.** To ensure flexibility and organizational agility, the network must support new applications and services as needed. Campus networks must be architected such that they are neither a hindrance nor a bottleneck to introducing new applications.

- **Simplified, automated management.** IT organizations must manage increasing complexity in the network in the face of limited budget and staffing. Campus networks must incorporate features that ease the deployment and management burden so they can focus their efforts on higher value-added activities.

- **Policy-based approach to supporting business applications.** To reduce manual effort and ensure the most effective use of administrative staff time and resources, the network should support delineated policies to control access and priorities for the use of network resources.

- **Network automation and programmability.** To provide investment protection, the network architecture must enable introduction of new network services and features without having to rip and replace the current network infrastructure. One of the best ways to do this is through automation and programmability, which enables networks with greater agility to adapt to new changes and services in the future.

- **A path to supporting software-defined networking (SDN).** SDN takes automation and programmability to the next level. By separating the control plane from the switching plane and providing network virtualization and programmability, SDN has the potential to transform the networking world much like virtualization transformed server computing. Companies introducing networking equipment today should ensure that the equipment is able to support SDN if and when their requirements demand it.

HUAWEI'S NEXT-GENERATION CAMPUS NETWORK

In August 2013, Huawei introduced a new series of next-generation campus networking products that consists of:

- **Smart Campus Controller.** The controller delivers policy-based coordination and control of the campus networking environment. It handles unified authentication and path computation and keeps track of network topology and resources.
- **S12700 Agile Switches.** These programmable Agile Switches provide routing and policy execution based on the commands received by the campus controller. They are based upon the Huawei Ethernet Networking Processor (ENP) chip and are available in two models — S12708 and S12712 — in 2013. ENP will also be available in S9700, S7700, and other access layer switches in the near future.

Unlike traditional networks in which policies must be implemented and managed at the device level, the Huawei campus approach enables network administrators to coordinate and control the network as a seamless whole — both wireless and wireline — with no need for management down to the device or service level.

User Policy-Based Approach

The traditional network view is based on devices, ports, and topologies rather than users. If different policies have to be applied for specific users, the administrator must manually translate users to ports and assign permissions, a very cumbersome process.

In contrast, with the Huawei campus approach, administrators don't need to know the details of the network topology or devices. Administrators set policies defining permissions and application access priorities at the user level. These policies are stored in a user/application database, which is referenced by the Smart Campus Controller to send appropriate instructions to the Agile Switches. When a user comes onto the network, the controller automatically applies all control and configurations to the network devices for that user.

Unified Wired/Wireless Approach

The Huawei campus solution combines wireless and wireline networks into a single converged wireless/wireline network with unified authentication, permissions, and automatic deployment of QoS. Its built-in broadband remote access server (BRAS) technology provides unified user management capabilities and greater control over the user environment.

With traditional campus network topologies, the wireless network is treated as an overlay with its own set of policies, permissions, management, and controls. In contrast, the innovative Super Virtual Fabric (SVF) functionality found in the Huawei campus networking solution virtualizes both wired switches and wireless access point (AP) ports into a single network with uniform forwarding, control, and management of data.

With SVF, administrators can treat their wireless and wireline network as if it were one big switch. Huawei calls this a "Super Switch." A single, unified set of policies can be applied and administered on a per-user basis. Whether the user is accessing the network by wireline or wirelessly, the same policy is applied, which means the administrator doesn't have to configure the policy in two different places.

Providing Policy-Based Quality of Service

One of the hallmarks of the Huawei approach is its use of dynamic flow control and dynamic path planning to provide tailored quality of service to users. Policies can be set for groups of users and applications, and the network customizes the forwarding path to control latency as required.

The campus controller is aware of the user and the application, and the controller can automatically deploy virtual networks so that bandwidth and policies are applied to users and applications on an individual basis. For example, video traffic can receive higher priority than email, or development teams can receive higher quality of service than guest users. Policies can even be configured based on the location of the user, the time of day, and/or the device the user is carrying. By provisioning the network with certain minimum QoS parameters for certain users and applications, and appropriately reserving the required bandwidth, the organization can improve the perception of service quality for users and applications.

Automated Monitoring and Control

Another primary feature of the Huawei approach is the ease of network monitoring and control. In traditional networks, the administrator sees the topology of the network consisting of physical ports and devices. As the number of nodes and users increases, management of ports and devices becomes difficult and complex. With the Huawei campus approach, the administrator's view is of the users and applications as well as the policies and permissions that are specific to each of them. The network understands which users are hitting which ports and automatically applies the policies to the devices. This reduces the effort to configure and manage the network considerably.

Further, Huawei has introduced an innovative new technology it calls Packet Conservation Algorithm for Internet (iPCA), which is designed to determine the experience of the user, including packet loss and slow network performance. Traditional monitoring technologies such as bidirectional forward detection (BFD) and network quality analysis (NQA) are designed to perform only single-in/single-out detection and cannot be used to identify where failures lie between two points. In contrast, iPCA provides multi-in and multi-out quality monitoring and can be recursively applied to portions of the network, all the way down to a single device. This enables the network to detect failures and isolate them very quickly, improving quality of service to the user. All of this happens nearly instantaneously from the user's perspective.

Security

The Huawei Agile Switches include built-in support for firewalls, NAT, IPSec, and IPS in the company's next-generation value-added service cards and IPS, ADC, and ASG in its open service platform (OSP) cards. In the future, Huawei plans to support ASG, SSL VPN, and prevention of DDoS (distributed denial of service) attacks on its next-generation value-added service cards.

One of the innovative aspects of the Huawei approach is its treatment of DDoS attacks. In traditional networks, when one point in the network is attacked, the whole network could collapse. With the Huawei approach, when a DDoS attack is detected, automatic safety rules are issued at the access layer, blocking the attack. The controller isolates the affected resources and routes traffic around them so the rest of the network is not affected.

Another innovative security feature is location-aided authentication (LAA). LAA enables includes geolocation as one aspect of the authentication process. This can be used for a variety of purposes — for example, to block network access to users currently outside the campus, regardless of their log-in credentials.

Key Benefits of the Huawei Campus Networking Approach

The Huawei S12700 series was designed to support today's campus network demands and to adapt as business needs change. Some of the key benefits associated with the Huawei campus networking approach are as follows:

- **Support for BYOD, cloud computing, and video.** The policy-based approach at the core of the Huawei campus networking product family is designed to meet the needs of today's enterprise, with appropriate QoS provisions for cloud computing and video. Its unified approach to wireless and wireline networks is designed to address the needs of mobility and BYOD.

- **Adaptability for changing applications, users, and devices.** With the rapid pace of change, network administrators must ensure they have a network infrastructure that not only meets current needs but also offers flexibility for the future. While it is often difficult to extend traditional networks to accommodate new technologies, the Huawei programmable approach allows new technologies to be incorporated using software upgrades.

- **Simplified management.** The traditional network view is based on devices, ports, and topologies. In contrast, with the user- and application-based view of the Huawei campus network, the administrator doesn't have to know topology details. Traditional networks require manual configuration to deploy user-specific policies, but Huawei enables policies to be deployed automatically with a smart control mechanism.

- **Improved user experience.** Traditional networks can't detect user experience degradation or determine the causes of it. With its innovative iPCA technology, Huawei enables the network to automatically detect network failures and isolate their location.

- **Smooth evolution to SDN.** This approach takes advantage of Huawei's innovative ENP chip technology and a fully programmable architecture to enable the network to adapt with agility, responding to evolving business requirements today. It also provides investment protection by enabling a smooth transition to SDN technologies, including POF, SDN VPN, and parallel panel architecture (controller panel and routing panel), in the future.

OPPORTUNITIES AND CHALLENGES

IDC sees a number of opportunities and challenges for Huawei as it rolls out its new campus networking products.

Opportunities

- **Demonstrating thought leadership for the next-generation campus.** These products allow Huawei to paint its vision of where the next-generation campus is going. Instead of being just another set of boxes with higher feeds and speeds, this solution demonstrates Huawei's commitment to the next-generation campus, where the best of wired, wireless, security, and management can be brought together.

- **Establishing a foothold in the enterprise wireless market.** Huawei's presence in the pure wireless LAN enterprise market has been limited to date. The launch of this new converged campus wired/wireless offering provides the opportunity to command increased mindshare from the IT community and gain increased traction in the wireless space.

Challenges

- **Introducing programmability and smart infrastructure to the campus LAN.** To date, network programmability, virtualization, and SDN have focused on the datacenter, whereas the Huawei smart infrastructure product suite focuses on the campus. Huawei will need to educate the market about the need for and benefits of introducing intelligent networking into the campus environment.

- **Establishing leadership presence across geographies.** True to Huawei's geographic origins, the primary focus of the company to date has been in China and other Asian markets, with more limited presence in other geographies. Huawei's current geographic footprint could limit the ultimate take rate, despite the innovative, service-rich nature of Huawei's campus networking products.

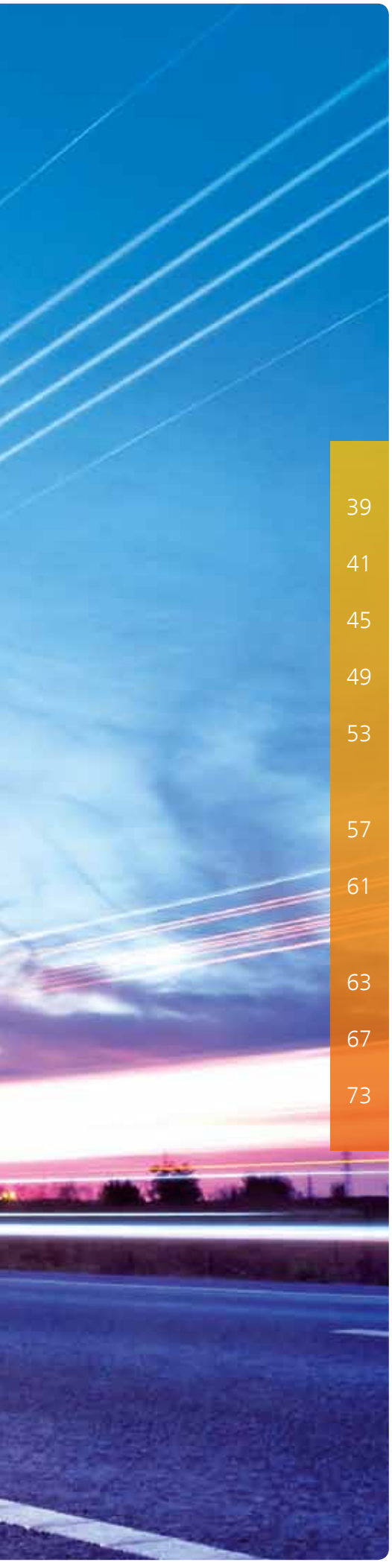
CONCLUSION

The enterprise campus network is the gateway through which users access applications, data, and services. Network administrators must ensure that campus networks can support trends such as consumerization of IT/BYOD, cloud services, video, and VDI while incorporating flexibility to meet future demand. In addition, they must do this while simplifying the network and minimizing their own management burden.

Huawei recently introduced a new series of innovative campus networking products incorporating the concepts of programmability and control, policy-based management at the user level and the application level, and wireless/wireline convergence. Consisting of a Smart Campus Controller and a series of Agile Switches, the Huawei campus networking solution is designed to improve the user experience, reduce the management burden, and increase network security, all while future proofing the campus network to enable the introduction of greater levels of virtualization and even SDN when required.

3

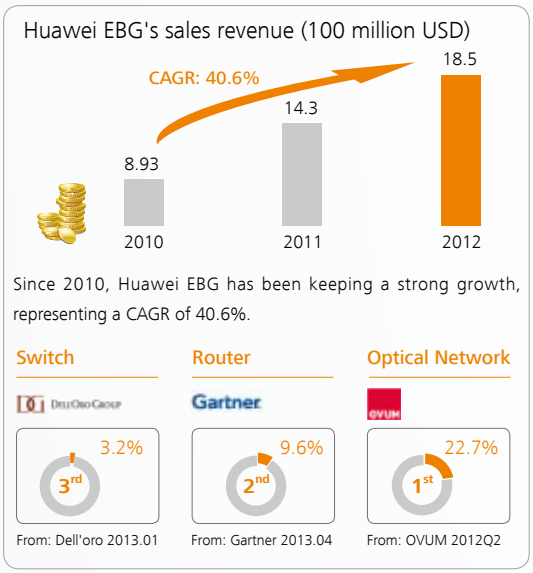
Huawei S12700 Agile Switch Technical Essays



IP Your Future

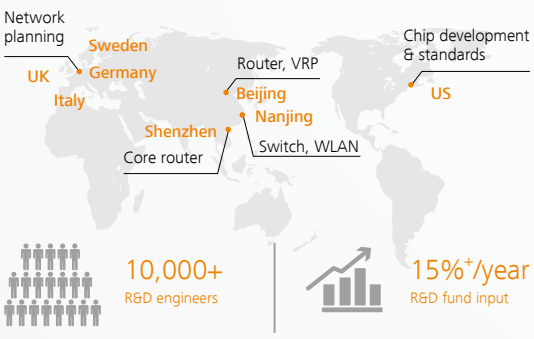
Huawei Enterprise Business Group (EBG) is a leading provider in the global communications market. We provide innovative and customized products, services and solutions, and respond with consistency and speed to your needs.

Huawei EBG Keeps Fast-Growing



According to global market share reports: Optical Network's is No.1(source: Dell'oro 2013); Router's is No.2 (excluding the North American market) (source: Gartner 2013); Switch's is No.3, which growth rate (more than 60%) is No.1(source: OVUM 2012).

Large R&D Inputs



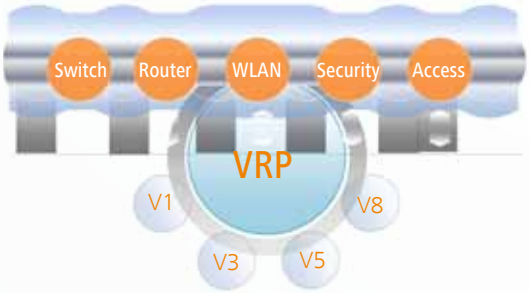
Huawei IP has more than 10,000 R&D engineers, and has established research and development centers in China, US, UK, Germany and other regions.

Huawei IP has increased R&D investment. The R&D investment to revenue ratio has been up to 15%, higher than the company benchmark of 10%.

Integrated Product Development (IPD)

With growth of business, company needs one advanced process to support business development. Huawei has invested 1.7 million USD, introduced IBM's advanced IPD process. Huawei continues to optimize the structured processes, heavyweight teams, governance systems, and IT enablers in the IPD domain to constantly improve IPD operational efficiency and product competitiveness. Huawei also develops products designed for marketing, manufacturing, procurement, servicing, and other purposes to boost end-to-end operational efficiency.

17 Years Accumulated Experience



7 million+	100+	10 million+
Devices	Countries	Codes

Huawei has a unique R&D cost structure which allows organic growth based on consistent hardware and software platform development. Huawei IP's five product portfolios, including Switch, Router, WLAN, Security and Access, based on VRP platform which has more than 17 years technology accumulation. So far, more than 700 million devices are stably operating in the existing network in more than 100 countries worldwide.

21 Years Rich Experience in Chipset

As the only company in China that has its proprietary core chip technologies, Huawei has always been convinced that chipset is the core competitiveness of company. Since Huawei established ASIC R&D center in 1991, the capacity of Huawei in-house chipset has achieved 400G and 1T, which is the leader in the industry.

1991: Established ASIC R&D Center.

2004: Rolled out its first router chip.

2009: Solar 2.0 chips lead the 100G market.

2012: Solar 3.0 chips lead the 400G/1T market.

2013: Industry's first Ethernet Network Processor (ENP) chip leads the fifth-generation switches.

Industry-Leading Automated Testing Factories

1500+	1700+	2300+	200,000+
WLANs	Routers	Switches	Test Cases/Month

Live Network Simulation

1:1 mirroring on the entire network enables accurate simulation of live network environments.

Automated Testing

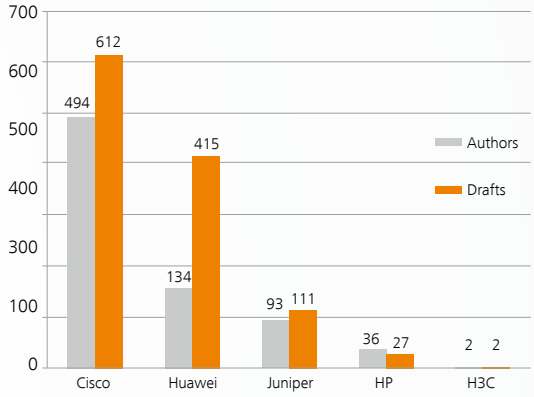
Fully automated test case coverage.
Rapid upgrading and delivery of stable versions.

Interoperability Test

Seamless compatibility with devices from mainstream vendors in the industry.

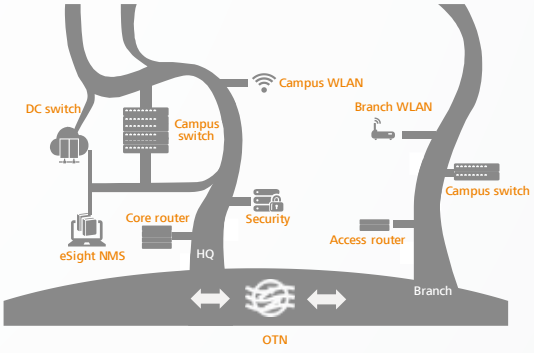
Huawei has established industry-leading 7*24 hours automatic test factories in Beijing, Nanjing, Shenzhen and Suzhou, which could simulate the real operating environments of the existing network, seamless compatibility with devices from mainstream vendors to ensure the stability of existing network equipment running.

Industry-Leading of Standards & Patents



Huawei actively contributes to standards in the industry. At the end of 2012, Huawei has drawn up 549 IETF documents, 41,948 Chinese patents, 14,494 foreign patents, 12,453 international Patent Cooperation Treaty (PCT) patents.

Product Family



Ethernet Switch Evolution

By Xu Ting

Dominant Ethernet Network Technology

Ethernet, a Local Area Network (LAN) link-layer technology with simple implementation and low costs, has become the basic and dominant technology in the bearer network field. As Fast Ethernet and Gigabit Ethernet emerge, Ethernet has become predominant in LANs and is becoming an important technology in Metropolitan Area Networks (MANs).

Ethernet was first documented in a memo that Robert Metcalfe of Palo Alto Research Center (PARC) wrote in 1973. In 1976, Metcalfe co-wrote "Ethernet: Distributed Packet Switching for Local Computer Networks," with David Boggs. At the end of 1977, Metcalfe and partners obtained the patent for a multipoint data communication system (with collision detection). This system was called Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Ethernet was born.

In 1979, Metcalfe left PARC and founded 3Com. He convinced Digital Equipment Corporation (DEC), Intel, and Xerox to work together to promote Ethernet as a standard. The universal Ethernet standard was published on September 30, 1980. At that time, there were two proprietary systems: Token Ring and ARCNET. These two proprietary protocols were soon replaced by Ethernet.

Evolution of Four Generations of Switches

From 1989, when the first-ever Ethernet switch was launched, Ethernet switches have made great improvements in forwarding performance. The switch interface rate has increased from 10 Mbit/s to 100 Gbit/s, and switching capacity has increased from dozens of megabits to dozens of terabits. With high performance and low cost, Ethernet switches are the most widely used network devices.

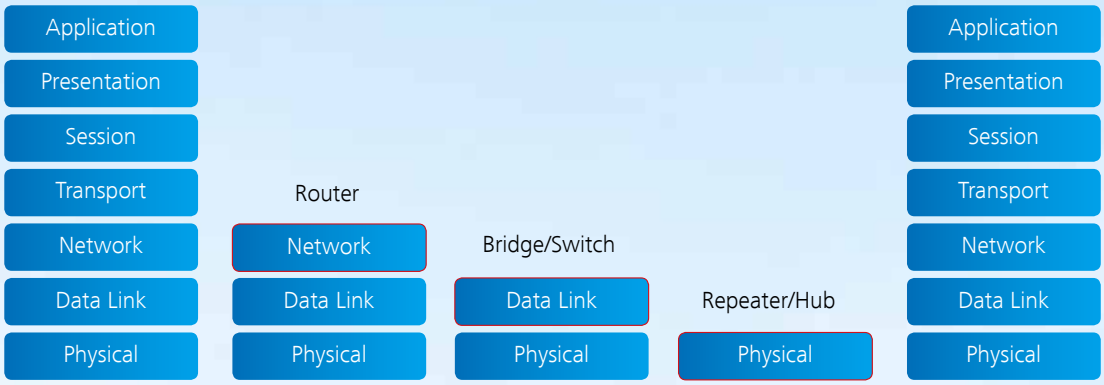
Early Ethernet devices such as hubs are physical layer devices and cannot isolate collision domains, which limits network performance. Early switches (network bridges) are Layer 2 devices that are able to isolate collision domains, greatly improving Ethernet performance. Today's switches not only provide Layer 2 forwarding, but also Layer 3 hardware forwarding based on IP addresses. There are even switches at Layer 4 or above.

According to the layer where switches work, switches are classified as Layer 2 and Layer 3 switches, and multiple layer and multiple service switches. The following describes switch development.

Predecessor of Switches: the Hub

Hubs are similar to switches in appearance.

A hub works at the physical layer (Layer 1) of the OSI model. It regenerates, shapes, and amplifies received signals to increase transmission distance, and is the central node.



A hub forwards received packets to all interfaces and can transmit one data frame at a time. All hosts connected through a hub are located in the same collision domain. All interfaces of a hub share bandwidth. A network built using a hub as the core is a shared Ethernet. When multiple hosts send data packets simultaneously, many collisions cause network performance to deteriorate.

Hubs are not switches, but played an important role during initial Ethernet network development. They have been deployed as access switches for a long time, and are often considered as Layer 1 switches.

Typical hubs include 3Com 3C16410 hubs and Cisco 1538 hubs.

Layer 2 Switch

Switches are developed based on multi-port bridges. The first Ethernet switch product (EtherSwitch EPS-700), invented by Kalpana, provided only seven fixed interfaces.

Original switches complied with the OSI model. They work at the data link layer and are also called Layer 2 switches. Layer 2 switches identify MAC addresses in data frames and select interfaces to forward packets based on MAC addresses. The algorithm is simple and easily implemented by the ASIC chip, so the forwarding performance of Layer 2 switches is high. Layer 2 switches solved the problem of hubs' collision domains, helped develop Ethernet switches, and greatly improved LAN performance.

Typical Layer 2 switches include Cisco 2960 series switches and Huawei 5700-LI switches.

Layer 3 Switch

Before VLANs were used, switches could only isolate collision domains, but could not isolate broadcast domains. When there was communication in the TCP/IP stack, broadcast or multicast protocol packets, such as ARP, RIP, and DHCP, were widely used. If there was only one broadcast domain on the network, broadcast packets were sent to the entire network, which affected network performance and created extra burdens on network hosts.

The network has been gradually integrated into people's daily lives. Network users have increased sharply, causing increased problems for broadcast domains. Though VLANs isolate broadcast domains on switches, packets between VLANs need to be forwarded by routers. Compared with switches, routers have high costs and low performance, and cannot meet requirements of high bandwidth. People began asking for Layer 3 switches that retain the advantages of high performance and low costs, and provide high bandwidth.

Early in Layer 3 switch development, ASIC chips could not independently complete Layer 3 forwarding. In 2002, Layer 3 switches performed very little routing, but much switching. This meant that they provided strong Layer 2 functions but low Layer 3 functions. ASIC chips were then developed that provided hardware-based route searches, enabling switches to implement hardware-based Layer 3 forwarding. Layer 3 switches were quickly replaced by switches providing hardware-based Layer 3 forwarding. Switches that provide hardware-based Layer 3 forwarding are also called routing switches.

Typical Layer 3 switches include Cisco 3750-X series switches and Huawei 5700-EI switches.

Multiple Service Switch

In recent years, especially after 10 GE was introduced, high-bandwidth services such as voice, video, and game services became very popular. The development and deployment of these services created new requirements for network devices such as security, reliability, and QoS, in addition to connection. To reduce networking costs and simplify management and maintenance, functions of network devices had to be integrated, adding multiple layer forwarding and value-added services.

Limited by the ASIC chip, multiple service switches used the model that combines Layer 2 and Layer 3 services and upper-layer value-added services. In practice, multiple physical devices were installed in the same chassis. The multiple service switches using this hybrid model did not provide integration.

Typical multiple service switches include Cisco 6500 series switches and Huawei S9700 series switches. Huawei's S9700 series switch uses distributed hardware forwarding architecture. It provides the maximum switching capacity the industry has to offer at 18.56 Tbit/s, up to 12 service slots, multiple layer hardware forwarding capabilities such as bridge, IPv4, IPv6, and MPLS, and value-added service capabilities such as load balancing, AC, firewall, and IPsec VPN.

The following table lists four generations of products.

Phase	Product	Typical Product	Forwarding Hardware	Usage
First generation	Hub	3Com 3C16410 Cisco 1538	ASIC	Shared LANs
Second generation	Layer 2 switch	Cisco 2960 Huawei S5700-LI	ASIC	Small-scale LANs
Third generation	Layer 3 switch	Cisco 3750X Huawei S5700-EI	ASIC	Small- and medium-scale LANs
Fourth generation	Multiple service switch	Cisco 6500 Huawei 9700	ASIC + multi-core CPU Hybrid model	Campus networks, MANs

Demands for Fifth-Generation Switches

In recent years, new services such as cloud computing, BYOD, SDN, Internet of Things, video, and Big Data have all become popular, with new requirements for high density, high performance, flexibility, and large-scale Ethernet. This also brings a new round of improvements in Ethernet switching technologies.

New services have the following requirements on Ethernet switches.

Full Programmability

Service flexibility is a major concern of switch developers. To increase switches' flexibility, vendors often use programmable ASICs for their multiple service capability. However, ASICs can provide only partial programmability; for example, user-defined packet parsing, and limited service flexibility, which cannot meet the quick turnaround required of new network services. Future switches must be fully programmable in order to meet those requirements. Programmable switches can provide new services simply by upgrading software, without having to replace hardware. This saves on initial investments. Fully programmable switches are also necessary for smooth migration to Service-defined Networks (SDN).

SDN will impact existing network architecture with simplified management, traffic optimization, and fast development. In addition to OpenFlow 1.3, formidable vendors compete vigorously to promote SDN for market share.

High Integration

Integration of network functions is required to reduce networking costs and simplify management and maintenance operations. It includes integration of switching and routing, triple play (voice, data, and digital television) carrier services, and calculation, storage, and communication in data centers.

As WLAN and BYOD networks develop, wireless users will continue to multiply. Currently, different devices are used to create access for users and manage their connections, causing a heavy burden for IT management and maintenance personnel. Fifth-generation switches must be able to implement wired and wireless convergence so that users are connected in a unified manner and unified policies are applied. In addition, accurate user and service management has become a necessity on campus networks.

Large Hardware Entry Resources

It is predicted that, by 2015, roughly 3.3 billion terminals will be connected to the Internet, out of which 70 percent of these terminals will transmit services for Internet of Things applications. As machine-to-machine technology for the Internet of Things is established, IPv6 will extend to industries such as energy, electricity, and transportation. And as the Internet of Things becomes more popular and gains widespread use, many more digital connections will be set up. Tomorrow's network devices must be equipped to provide more entries to allow for expansion over the next five to ten years.

Strong QoS Capabilities

Switches often face challenges in end-to-end QoS.

In the rich media era, the IP network transmits many real-time video services, which require high network bandwidth, short delays, and low packet-loss ratios. On the IP network, traffic is variable and gusty. To prevent service delays and added downtime costs caused by many discarded packets, network devices must be able to process traffic bursts and provide closely managed queue scheduling.

Network-level QoS detection and displays are often difficult to monitor on the IP network. To install new services, users need to accurately determine whether the network can accommodate these requirements. During service operation, users also need to detect changes in network quality to determine what decisive measures to take, such as whether to immediately switch services to a backup link.

In the past twenty years, traditional ASIC-based switches have become the most widely used network devices, with high performance and low cost. Yet, faced with the growing changes and challenges caused by the emergence of cloud computing, BYOD, SDN, Internet of Things, and Big Data, ASICs simply cannot meet these new service requirements because of their low flexibility. The ASIC chip cannot maintain switches' competitiveness, even with its hybrid model. The new generation switches must incorporate new, innovative technology to remain competitive, and optimize its lower-layer architecture. We call it **fifth-generation switches.**

ENP: Redefining Ethernet Forwarding Technology

By Lv Chao and Peng Xiaopeng

Ethernet Forwarding Technology Dilemma

Many counters such as throughput, delay, manageability, and security can be used to measure switch performance. Among all these counters, the most essential is forwarding technology.

The forwarding capacity of switches has increased from 10/100 Mbit/s to 1,000 Mbit/s or even 10 Gbit/s. The ASIC chip is the core of this increase. However, with the rapid development of video, mobile offices, BYOD, cloud computing, and the Internet of Things, the Ethernet needs to provide large-scale forwarding capabilities, permit flexible, smart control and easy management. So there are new requirements for the performance and flexibility of Ethernet switches now. Currently, switches support Layer 3 routing rather than merely provide Layer 2 switching functions. Despite this, they are mainly used to provide access for enterprise terminals, and cannot match the rapid development of new services in the cloud computing era. The root cause is that ASIC chips can only identify predefined protocols and use a fixed forwarding process.

ASIC: Fixed Architecture and Low Scalability

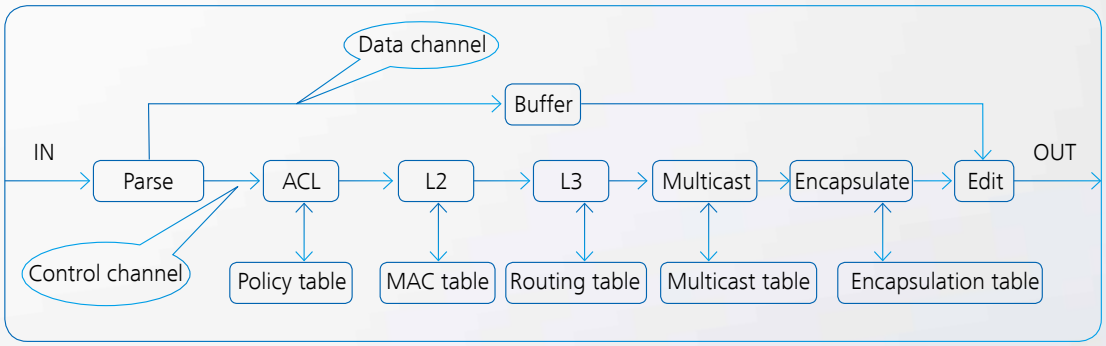


Figure 1: ASIC chip architecture

The biggest challenge that ASIC chips face is that the chips do not offer flexible extension; they can only parse predefined application protocols. The digital circuits must be redesigned to support new application protocols. Redesign is necessary even if a register is added to the chip. When a service is added, a module must be added, resulting in redesign of the entire chip. Chip manufacture often involves complex processes such as design, prototyping, and testing before delivery, which often takes more than two years. This kind of development cycle prevents device vendors from providing quick responses to service requests.

Commercial Network Processors (NPs) have been developed to replace ASIC chips. Can commercial NPs overcome the disadvantages of ASICs and become the choice for Ethernet switches?

Commercial NPs: Low Performance and High Power Consumption

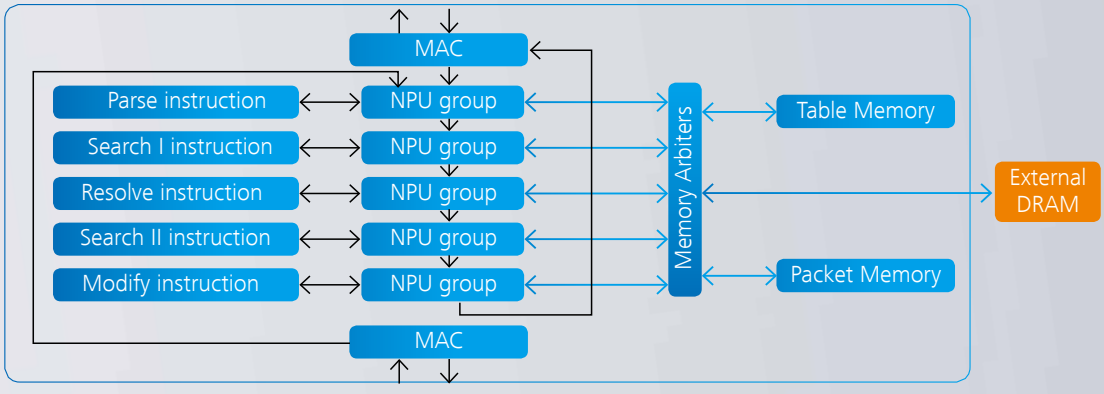


Figure 2 NP chip architecture

A commercial NP consists of a Network Processing Unit (NPU), instruction memory, table memory, packet memory, and table Dynamic Random-access Memory (DRAM). This design improves the flexibility of each module in NP. During operation, service processes need to be divided, but the instruction space of each NPU group is limited. If the instruction space is exhausted, the NP cannot support new services. When service processes are incorrectly divided, some NPU groups are heavily loaded, causing a bottleneck. As a result, although the NP has improved flexibility compared with the ASIC chip, its overall performance is still not satisfactory.

Although the programmable ASIC chip was developed to meet service scalability requirements to a certain degree, it is just a transition to something better. Should ASIC chips continue to be developed or should other technologies be used to improve switch forwarding?

ENP: Combines High Performance and Flexibility

The ASIC chip provides high performance and low power consumption, with an inflexible architecture. It cannot meet the requirements of fast-developing enterprise IT applications. Though a commercial NP is flexible, it provides low performance and high power consumption. Based on decades of experience in developing chip technologies, Huawei put forth its innovative Ethernet Network Processor (ENP), which integrates the high-performance features of ASICs and the flexibility of commercial NPs. The following figure illustrates the advanced characteristics of the ENP.

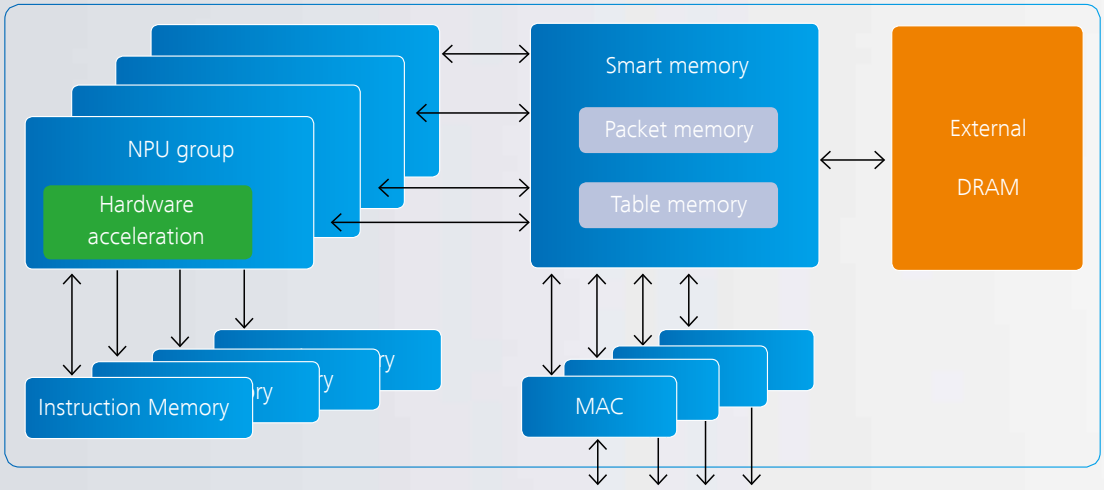


Figure 3 ENP chip architecture

Complete instruction space and hardware acceleration offset the disadvantages of commercial NPs:

The ENP can access complete instruction space because its NPU group is a disconnected group of commercial NPs. Each NPU group can execute instructions such as Parse, Search I, Resolve, Search II, and Modify. The ENP does not need to switch services to different NPU groups, which permits faster services. In addition, the ENP uses multi-threading technology, reducing the impact of delayed IQ access on NPU performance.

Huawei SmartMemory Solves Memory Access Performance Problem

Commercial NPs and ASICs separate calculation from storage units. As a result, their physical distance increases the exchanges between them. Data access is delayed and power consumption is high. If read-write operations are performed for the same address from multiple sources, addresses are latched to ensure data consistency. This may cause access bottleneck.

Huawei ENP has an integrated SmartMemory. The storage unit integrates calculation and determination capabilities. This reduces exchanges between the primary calculation unit and SmartMemory, greatly improving efficiency between the calculation unit and storage unit.

SmartMemory integrates the Huawei-developed search engine, co-processor, and traffic management. It provides all algorithms for memory operations such as search, calculation, and read-and-write just like that of commercial NPs or ASICs, but these algorithms can be invoked by any functional unit of the ENP.

Millions of Flow Entries and Hybrid OpenFlow

The SDN solution, based on Hybrid OpenFlow, uses OpenFlow and traditional routing planes to forward and control traffic, and enables the traditional network to migrate to SDN. With the programming capability and a maximum of 16M flow tables, ENP-based switches can forward both OpenFlow packets and traditional Ethernet frames, facilitating migration from traditional networks to SDN.

ENP's Low Power Consumption Comparable to ASIC Chip

The ENP provides all necessary functions of multiple chips and also reduces power consumption. On a switch, chips consume power. More chips mean more power consumption. Generally, two chips run on a switch. One chip forwards packets, and the other chip buffers packets, which provides more entries and a large buffer. Huawei integrates both chips into a single chip, effectively reducing power consumption.

Chip power consumption includes 40% static and 60% dynamic power. Static power consumption is proportional to a transistor's working voltage. The ENP uses an advanced voltage controller to reduce static power consumption. The transistor's working voltage can be adjusted according to electrical attributes during chip production.

Changing the transistor's working voltage and clock frequency reduces dynamic power consumption. The ENP integrates Huawei's innovative speedometer to detect internal traffic on the chip and automatically adjust the working clock frequency. For example, let's assume that the original clock frequency is 400 MHz. If the frequency is reduced to 300 MHz, the dynamic power consumption is reduced to 75 percent of the original power consumption. In addition, when network traffic slows, the ENP can disable idle NPU groups to further reduce power consumption.

ENP – the Best Choice for the Future

As the Ethernet continues to improve, it will provide more secure, higher speed, and higher quality services. These services will offer smart manageability, flexibility, and intelligent adaptation to future-generation Ethernet products and technologies – the core of a company's competitiveness. To enable Ethernet switches so they can provide integrated data, voice, communication, video and mobile office services, Huawei developed the ENP chip, which is capable of line-speed forwarding and low power consumption comparable to commercial ASIC chips and is more flexible than commercial NPs. The ENP will inevitably redefine Ethernet core forwarding technology and become the de-facto technology for next-generation Ethernet switches.

Demand an Agile Switch on Agile Networks

By Du Pingzhou

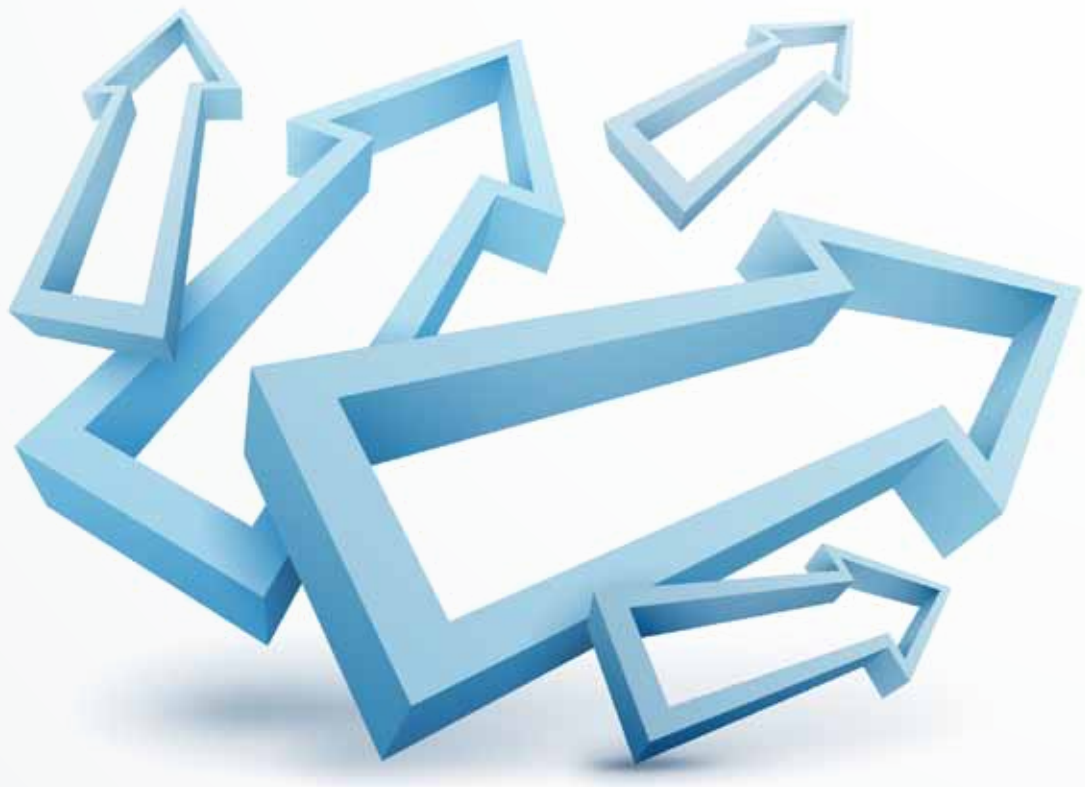
Hello, Agile Networks

After many years of silence, the Ethernet has entered the stage of technology innovation stage. New applications such as cloud computing, mobile Internet, video, social network, and the Internet of Things are emerging quickly. These applications require the development of switching technology, performance, architecture, service quality, intelligent management, and energy conservation.

New applications require network to provide high speed, a smooth architecture, and intelligence capability. For example, cloud computing requires controllable scalability of virtual resources. This cannot be done with ASIC chips. Traditional Ethernet switches do not have fault location and performance-monitoring capabilities, while the Agile network must be able to automatically detect and locate faults and measure end-to-end network performance. In addition, an entire IP network can be virtualized into a switch to automatically detect and configure new service nodes.

Generally, a network should have the following characteristics:

- Innovative services launching: controllable resource scalability (network resource virtualization, but not device virtualization) and Software-defined Network(SDN)
- Mobile policy: manageable and mobile resources on the entire IP network
- Innovative operation and maintenance: network awareness and global security association



Technical Requirements of Agile Networks

High reliability: Due to the development of BYOD, desktop cloud, and SDN, enterprise networks need to connect to remote VPN users along with fixed and wireless users. Enterprise networks are required to provide increasingly high reliability because faults on network core switches affect many services for an increasing number of users.

Programmability: With the rapid development of enterprise networks, the contradictions between fast service development and slower network deployment are becoming increasingly obvious. The cycle of enterprise service revolution is often two or three years, while network devices are replaced every five years. Device programmability converges with new service development strategies and negates the need for frequent network equipment replacements.

Large tables: Since IPv4 addresses are exhausted and IPv6 addresses are being adopted very slowly, IPv4 and IPv6 addresses must coexist on enterprise networks. IPv6 addresses occupy twice as many entry resources as IPv4 addresses, so switches must provide more entries. This means core switches must be highly scalable to meet entry resource requirements of future services.

Three Highlights of Huawei S12700 Agile Switches

All switch vendors face requirements of high reliability, scalability, and programmability on core switches. Therefore, Huawei builds its S12700 agile switch series with core router platform technology to meet these requirements.

The S12700 CSS2 inherits hardware-based switching fabric cluster technology of core routers to implement network-layer high reliability. Currently, high-end switches provide high reliability of the main control board, card, power module, and fan module. Above all, reliability of the entire network needs to be ensured through the network architecture. Huawei S9700/S7700, in contrast, uses innovative Cluster Switching System (CSS) technology to ensure network reliability. On a Huawei S9700 or S7700, Memory Protection Units (MPUs) provide cluster interfaces for interconnection. S12700 improves the switching fabric cluster based on CSS and promotes Cluster Switch System Generation2 (CSS2). As shown in Figure 1, Switch Fabric Units (SFUs) provide cluster interfaces for interconnection. Each SFU supports up to 8x10GE cluster cards, and the total cluster bandwidth is 640Gbit/s. In the future, an SFU will support up to 6x40GE cluster cards, and the total cluster bandwidth will reach up to 1.92 Tbit/s, which is much higher than that of CSS technology. CSS technology exchanges data twice, while CSS2 exchanges data between chassis only once. CSS2 has a delay of only 21 μs,which is the industry's lowest inter-chassis delay and 60 percent of the industry average. In stack scenarios, traditional network vendors who use CSS technology require every switch to have at least one MPU. Compared to CSS technology, CSS2, on the other hand, uses a single MPU to manage the entire cluster. As long as one MPU is present in the cluster, the cluster can work normally, implementing 1+N backup. Mainstream vendors cannot provide these technologies. Huawei S12700 ensures network reliability using the CSS2 hardware-based cluster and 1+N backup of CSS2.

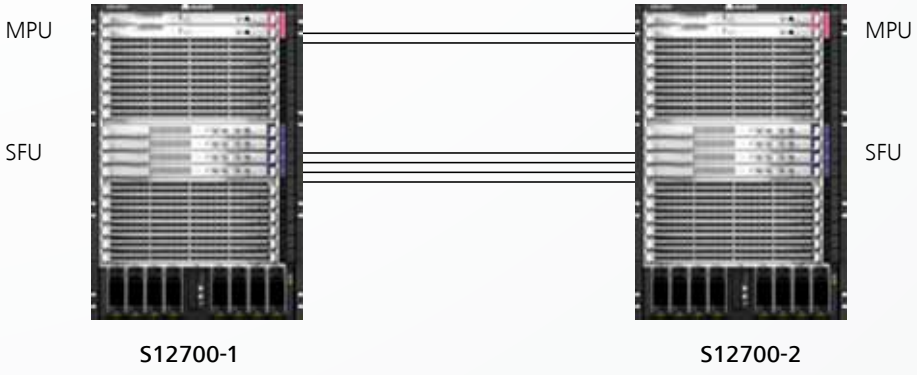


Figure 1 S12700 CSS2

S12700 uses Huawei-developed Ethernet Network Processor (ENP) that provides full programmability. ENP is a new processor customized by Huawei for the Ethernet. It inherits the flexibility and entry buffer of traditional NPs, and provides low power consumption and high performance, with higher ratings than that of the ASIC.

Table 1 Differences between ENP, NP, and ASIC

Chip	Performance	Flexibility	Integration	Power Consumption	Entry
ASIC	High	Low	Medium	Low	Low
NP	Medium	High	Medium	High	High
ENP	High	High	High	Low	Medium

The main highlight of the S12700 is the programmability of the ENP chip. Its forwarding architecture and processes are changed by the continuous upgrade of micro codes. This results in the ability to match the service requirements of the next10 years with a simple one-time investment. S12700 has built-in native access controller and broadband remote access server capabilities. S12700 also enhances user management and provides external interfaces in the control plane. The forwarding plane includes forwarding resources, forwarding processes, and packet encapsulation is fully programmable. As a result , S12700 is flexible and better able to support future SDN development.

S12700 implements high scalability with service capabilities of high-end routers. S12700 provides four mainstream cards: 48GE optical interfaces, 48GE electrical interfaces, 4 x 10GE+24GE optical+8 Combo interfaces, and 8 x 10GE+8 Combo interfaces. Figure 2 shows S12700 cards compared with the ASIC cards.

Figure 2 S12700 cards


48GE auto-negotiation electrical interfaces


48GE auto-negotiation optical interfaces


4*10GE+24GE optical interfaces+8Combo


8*10GE+8Combo

Item	MAC	ARP	FIB	NetStream	Buffer
Huawei X1E Card	1M	256K	3M	1M	1.5G
Commercial ASIC Card	512K	64K	512K	8K	8M
Number of times	2	4	6	128	192

Large routing and MAC tables are important components in solving the issues caused by ever-growing expansion of IPv4/IPv6 networking and the Internet of Things. A large buffer solves problems caused by bursts of traffic and congestion of high-speed services such as HD video services, large searches of data in data centers, and batch image transfers.

As wired and wireless traffic like Ethernet voice, data, and video increase, networks transmit combinations of multiple services from different users. Different services require different QoS levels. Even the priority of the same service originating from different users varies. For example, voice services have higher network requirements than data services, while Telepresence services demand lower latency than voice services and VIP users have higher priorities than common users. S12700 provides 5-level QoS. It can schedule traffic based on services and provide hierarchical QoS deployment. With large-capacity NetStream flow tables, S12700 can better analyze enterprise network traffic and offer visualized applications.

S12700 provides industry-leading switching technology performance, structure, service quality, intelligent management, and energy conservation, enabling development of advanced enterprise network services now and into the foreseeable future.

Easy to Use Quickly Building a User- and Service-Centric Next-Generation Network

By Shen Ningguo

Enterprises are seeing the continuing rise of Bring Your Own Device (BYOD) in the workplace. Statistics show that, for example, BYOD is widely used in the commercial industry with about 60 percent of employees using their own devices at work. Similar new applications are emerging rapidly, which bring new challenges to enterprise networks: enterprise applications on Social Networking Services (SNS) platforms, wireless access, wide coverage areas, and network openness.

To meet these challenges, enterprises must quickly build user- and service-centric next-generation networks. The core requirement of such networks is that Operation and Maintenance (O&M) should be transformed from focusing on network management to focusing on user management. This kind of transformation is difficult because focusing on user management changes network management from a static to a dynamic structure, greatly increasing network instability and management complexity. To adjust to such a change, enterprises have to build an easy-to-use network.

Enterprises' Next-Generation Challenges

Enterprises are facing a huge wave of transformation.

Enterprise Applications on SNS Networks: An enterprise can build its own SNS network. Employees can improve their capabilities of sharing, communicating, and cooperating. Employees will be allowed to access their company's SNS platform, pose personal problems, and seek solutions or solve problems posed by others. Those can effectively improve internal communication, boost employee morale, and more efficiently handle problems or complaints raised at work.

Wireless Access: Network terminals are not limited to just desktop PCs and laptops but also can be smart terminals that transmit office applications. In this case, Wi-Fi is the most suitable option for these terminals to access wireless networks. Enterprises need to build their own Wi-Fi wireless network inside the campus.

Wide Coverage Area: With the internationalization of enterprise operations, work specialization and conduct, and IT service management applications, today's enterprise IT system not only need cover their entire global branch office network, but also allow employees to access the network anytime, anywhere. These WAN connections become part of an enterprise network, enabling the enterprise network to expand seamlessly.

Network Openness: Wireless access and wide coverage areas require open networks. But openness poses a great challenge to security and the traditional security model of enterprise networks. Traditional network security is based on a closed network model that uses Network Access Control (NAC) to manage wired access ports. These access ports are very limited, for they cannot connect to networks without identity authentication. However, with open networks, they are based on a newer and more scalable security model that provides users reliable, open network access methods, and assigns appropriate rights based on user access, terminals, and software environments.

How to Evolve to a Next-Generation Network

Enterprises have a variety of requirements for next-generation network construction: uniform policy enforcement for wired and wireless integration, user-friendly video experience, flexible and scalable wireless network access for more devices, higher capacity at a lower OPEX, various IPv6 functions, simplified O&M and network management, and precise detection of network resources. Currently, most enterprises focus on the following requirements:

1) Seamless Network Coverage: Traditional networks use wired access to implement full coverage only in office areas; a few areas such as conference rooms are covered by wireless networks. This type of coverage does not support BYOD and does not allow social networks to be permanently online. Next-generation networks require that office areas should be deployed with both wired (Ethernet) and wireless access (Wi-Fi). In addition, remote access must be supported, and users must be allowed to access the campus network from external networks. Wireless network coverage enables employees and partners to access the campus network anytime, anywhere.

2) Precise Detection of User Identity and Terminal Type: In traditional networks, user identity and terminal types are detected based on authentication of wired switch ports. When the BYOD is introduced, the wireless network coverage automatically requires that a network device has its user identity, terminal type, and usage environment precisely detected. In this way, security and service guarantee policies can identify and monitor a particular user's whereabouts; for example, a user who goes online using multiple terminals. Immovable PCs in R&D zones have full rights and can access internal technical documents and other sensitive information. These R&D lab PCs are solely used for internal development purposes. Portable laptops or tablet PCs operating in open zones cannot be used to access top secret information but only regular, non-sensitive documents. PCs in open zones are generally used for daily office work activities and in conference room settings. Personal tablet PCs can be mounted on the rear side of a security sandbox and hold the same level of access rights as that of laptop PCs. Tablet PCs can be used for office

work and in conference room environments. Tablet PCs that are not equipped with a security sandbox have the same rights as that of mobile phones and can access internal resources such as yellow pages and internal social networks.

3) Rich Media: Future enterprise networks must support not only traditional data and voice services, but also rich media such as real-time video services to improve communication efficiency and reduce communication costs. Unlike voice service, real-time video service has high requirements like delay, bandwidth, and packet loss ratio (video quality). Traditional video service is rather limited and can be transmitted only by building a private network, but this is not feasible. In next-generation enterprise networks, users will be able to obtain real-time video services on any terminal. Next-generation enterprise networks will inevitably require real-time video service detection and service guarantees.

4) Flexible Rights Control and Access Records: Traditional networks can perform only large-granularity access control through virtual LANs due to the limited rights controls of low-price access switches. Next-generation enterprise networks must perform different, more powerful access rights control on different users and terminals. In addition, in open networks, users' behaviors must be recorded in detail for subsequent post-event audits, further requiring network devices to have powerful traffic analysis and recording capabilities.

5) Limited Investment and Simplified Management: Although network functions must be continuously enhanced and updated, traditional enterprise networks have marginal infrastructures. Investment in networks is controlled, and network management labor resources are limited. As a result, enterprise managers will not accept state-of-the-art, costly network architecture or a brand-new solution that puts high requirements on network management. Therefore, maintaining the original solution's compatibility while making sure existing networks remain intact and simplifying network management are the keys to build next-generation networks.

Huawei S12700 Agile Switches Deliver Better User Experience

To provide faster and better network services, Huawei has introduced its industry-leading components which include Unified User Management, service provisioning, and management simplification, in the recently launched S12700 Agile switches. Huawei's ME60 Multi-Service Control Gateway (MSCG) series BRAS provides fine-grained, simplified, high-quality broadband remote access services for hundreds of millions of China Telecom users. Those industry-leading components are vital parts of the Huawei S12700 Agile switch series.

The Huawei S12700 series are specifically designed and oriented to serve next-generation enterprise networks. Huawei has also developed new, dedicated Service Process Units (SPUs) for BYOD networks to help users implement quick network upgrades.

The Huawei S12700 is fully compatible with all existing enterprise networks. Powerful user management functions can be introduced without the hassle of upgrading or reconstructing widely deployed access and aggregation devices but, instead, only has to upgrade core and aggregation devices to provide new services. In addition, the centralized user management mechanism can significantly reduce user and service management workload. The Huawei S12700 offers the following competitive features:

1) Unified Wired and Wireless User Access and Unified Local and Remote User Authentication: The Huawei S12700 supports access of wired, wireless, and remote users at the same time as well as full-scale authentication technologies. The Huawei S12700 enables users to access campus networks through various methods. It is capable of precisely detecting users and providing all-round security protection.

2) Full-Scale User Detection Mechanism: The Huawei S12700 provides a built-in terminal detection mechanism that works with external servers to precisely detect the terminal type, software version, and software environment (including malicious and virus software) of users.

3) Centralized User Policy Control Mechanism and Policy Delivery Mechanism: The Huawei S12700 can be managed by an authorized server in a centralized manner to perform complete access rights control and provide QoS guarantees for users.

4) Service Assurance: By introducing the ME60's five-level hierarchical scheduling mechanism based on user or service granularity, the Huawei S12700 can precisely detect services and provide fine-grained protection for user services to ensure high quality real-time video services.

5) Behavior Check and Audit: The Huawei S12700 includes the high-capacity NetStream, and is therefore capable of recording users' network access behaviors for subsequent post-event behavior checks and audits.

6) Service Customization: Based on Huawei's proprietary Ethernet Network Processor (ENP), the Huawei S12700 can customize differentiated service processing logic through software upgrades to satisfy a wide variety of service requirements.

These competitive features enable the Huawei S12700 to assist you in quickly building a user- and service-centric next-generation network.

Huawei S12700 Opens the T-bit AC Era

By Zhang Junguang

In February 2013, the Dell'Oro Group released a market report predicting that Wireless LAN (WLAN) market revenue will exceed USD $11 billion in 2017, an increase of nearly 50 percent compared to 2012. It appears that the WLAN has a bright future. What drives this exponential increase in wireless networks includes WLANs used by Internet Service Providers (ISPs), a rapid increase in enterprise mobile applications, a surge in wireless-based video services, BYOD, and the development of gigabit Wi-Fi (IEEE 802.11ac). New applications also present new challenges for existing network architectures such as uniform policy for wired and wireless integrated management.

But the biggest new trend in wireless networks is that more and more large enterprises are beginning to regard WLANs as production-oriented networks that can run key services. The rises of BYOD and wireless offices have led to a huge growth in the size of wireless enterprise networks. Additionally, more and more functions are bundled into Access Points (APs) and Access Controllers (ACs), continuously increasing user costs.

Currently, most wireless networks use Fit AP architecture, which requires an AC to perform centralized data forwarding. This makes AC performance critical. Meanwhile, with the growth of GE wireless networks, AC performance can become a network bottleneck. Solving this bottleneck is becoming a challenging task for the industry.

The History of Wireless Networks

AC Performance: Customers' Pain Point

Early wireless networks were positioned more as a supplement for wired networks in enterprise offices. Advantages of an overlay model included low network construction cost and full reuse of old networks. The AC, meanwhile, was connected to a core or aggregation device. In this early phase, a typical enterprise would usually deploy, at most, dozens of APs. Today, large enterprises deploy thousands.

- Enterprises then began using the Fat AP method. The main advantage of the Fat AP is that a wireless network can be easily deployed without reconstructing the existing wired network. However, these Fat APs not only need to instantly process wireless access, but also provide complex switching and routing functions. The sheer number of such complex and independent APs considerably increased the workload and O&M of an enterprise's network.
- Fit AP was then developed to alleviate and solve this workload problem.
- Now, centralized and independent ACs manage Fit APs to operate in a more unified and efficient manner. In this way, functions of the Fit APs are greatly reduced, and network management is simplified.

The increasing popularity of wireless networks and BYOD have led to a huge growth in the size of wireless enterprise networks. Today, wireless signals can cover all areas within an enterprise, paving the way for wireless network services is becoming a main part of the modern office work style.

Let's look at a large enterprise with a sizable workforce of 20,000 employees as an example. If each employee has a personal tablet PC or mobile phone, then one employee is equal to two terminals, and the enterprise will then have a total number of 40,000 terminals. Assuming each AP covers 20 terminals on average, a total of 2,000 APs must be deployed. Currently, a single box AC can generally manage up to 256 or 512 APs at a given time, certainly no more than 1,000. To manage 2,000 APs, at least two or three independent ACs are required. If the AC needs to be backed up, at least four to six ACs are required. The overall deployment and management of such a number of ACs alone will considerably increase the enterprise's initial investment and O&M costs.

Shortcomings of Industry Solutions

When the forwarding capacity of a single AC becomes a bottleneck for wireless network development, one of the most commonly used methods in the industry is to increase the number of ACs, including independent ACs and Access Control Units (ACUs) on chassis switches. However, this method has the following shortcomings:

1) Insufficient Network Resources

In mainstream wireless networks, ACs are connected to aggregation switches in bypass mode. Therefore, to increase the number of ACs, the aggregation switches must provide more ports. Reserved device space and ports for ACs are insufficient in traditional network plans, and increasing the number of ACs is accomplished only with considerable difficulty.

2) Complicated Management of an Increased Number of ACs

An increased number of ACs leads to inconvenient device management. When there is only one AC, data is centralized on only one AC, and only one copy of data needs to be configured. When there are multiple ACs, multiple copies of data must be configured and be consistent with each other. When the configuration needs to be modified, all the ACs must be synchronized. As a result, errors might be caused. In addition, when the number of ACs is increased, reliability of the AC devices cannot be ensured. ACs are the cores of a wireless network. Any device fault may cause the entire wireless network to break down.

3) Wired and Wireless Overlay Networks Lead to High O&M Costs

In many existing networks, a WLAN network is overlaid on wired networks. Data configuration, policy control, and network management of wired and wireless networks must be performed separately, increasing overall network Operation

and Maintenance (O&M) costs. Each ACU on a chassis switch functions as an independent AC node that uses the slot and power supply of the switch. Unified management of the entire switch cannot be implemented entirely.

4) AC Performance Is Insufficient for IEEE 802.11ac High Bandwidth

Bandwidth of 802.11n-based 3x3 MIMO is only 450 Mbit/s. When 802.11ac-based 3x3 MIMO is deployed, the air interface bandwidth increases to 1.3 Gbit/s. In addition, coding efficiency on 802.11ac-enabled devices is high. Aside from air interface costs, the available bandwidth is 1 Gbit/s, bridging the bandwidth gap between wired and wireless networks and bringing a promising future to enterprise wireless applications. Nevertheless, the workload of ACs performing centralized forwarding increases considerably. Assuming there are 2,000 APs and the oversubscription ratio is 3:1, the forwarding capacity of the AC should be: 660 Gbit/s (2,000 APs x 1 Gbit/s/3). The average forwarding capacity of traditional ACs in the industry today is 10 Gbit/s, which cannot meet the service requirements of the 802.11ac protocol.

Huawei Solutions

Advantages of Huawei S12700 Native AC

Huawei S12700 agile switches use high-performance Ethernet Network Processor (ENP) chips, which solve the AC performance bottleneck and have launched the Terabit (T-bit) AC era.

1) Industry's First T-bit AC

Traditional AC functions can be implemented by independent physical devices or independent physical cards on chassis switches. The T-bit AC of the Huawei S12700 core switch is based on advanced ENP technology that integrates AC and Ethernet forwarding functions. Each card supports 80 Gbit/s of line-speed forwarding, which is two times or more than the industry average. When fully loaded, the AC device can support a maximum of 960 Gbit/s line-speed forwarding and is capable of managing 4,000 APs at a single time.

In addition, the AC device provides encapsulation and decapsulation of Layer 2 and Layer 3 data forwarding

capabilities through T-bit Control And Provisioning of Wireless Access Points (CAPWAP). Furthermore, the number of APs and accessing users managed by Huawei's S12700 T-bit native ACs are significantly multiple times than traditional independent ACs.

2) Native ACs Lower Users' Investment Costs

Customers do not need to purchase independent AC devices or other AC cards, but can use the functionalities of Huawei's S12700 native AC and Unified User Management to simply realize the convergence of wireless & wired users entirely. These native ACs occupy no additional slot space or port resources, saving customers' investment. In addition, the Huawei S12700 native AC features high scalability and flexibility, enterprise customers just need to add relevant line cards to meet the growing size of their wireless networks smoothly.

3) Real Convergence of Wired and Wireless Networks

The Huawei S12700 native AC introduced the excellent experience "AC managing APs" to "core switches managing access switches." as the creativity. Ethernet Service Interface Cards (SICs) with built-in native AC have the ability to unify management, policy, and forwarding of wired and wireless networks firstly in the industry. They also integrate wired and wired networks, greatly reducing enterprise network O&M costs, and promoting enterprise IT service innovation.

4) T-bit AC Era Is Upcoming

With the rapid development of WLAN technology, when 802.11ac WLAN products use 4x4 MIMO 160 MHz bandwidth, wireless network bandwidth can reach up to 3.5 Gbit/s. In contrast, centralized ACs cannot satisfy such large bandwidth requirements.

Huawei's answer is to launch a hierarchical AC solution. Use the cloud AC to implement the unified management of the whole network APs and business services in the upper layers; in the lower layers, aggregation switches forward wireless service according to the principle of proximity. This hierarchical AC solution lowers the performance requirements of centralized forwarding ACs.

Summary

Huawei S12700 agile switches have solved the issue of AC performance bottlenecks by means of experience and innovative technology. The functionality of native T-bit ACs which is the leading solution in the industries, integrates wired and wireless networks and, at the same time, greatly reduces enterprise network O&M costs and promotes enterprise IT service innovation.

Zero Configuration for Network Access

– Making Campus Network Management More Agile

By Zhang Jun

Data center networks have driven many technological innovations recently, leaving enterprise campus networks out of the public eye. If cloud computing, SDN, flat network architecture, virtualization, and new O&M policies are promoting transformation of data center network architecture, can enterprise campus networks remain unchanged?

For now, the campus network market seems quiet, but a revolution is coming, Campus network construction is service motivated. As new services continue to emerge, campus networks will require innovations in bandwidth, scalability, reliability, mobility, security, and network management. Huawei believes that no matter how technologies develop, the key to innovating campus networks is extensive collaboration between services and the network, for example, collaboration between cloud computing and elastic campus network structure, collaboration between multimedia services and network reliability and visualization, and collaboration between BYOD and wireless service security. Collaboration helps enterprises improve efficiency, increase revenue, and reduce TCO.

Zeus Kerravala, principal analyst of ZK Research, adds: "Cloud computing will bring dramatic changes to campus networks, because cloud computing will increase network traffic. Traditionally, a campus network transmits only local data center traffic, while cloud computing traffic is transmitted directly from branches or campus network to the cloud platform. This traffic model puts higher demands on campus network core devices and the backbone."

Experts agree that, with a firestorm of change on the horizon, campus networks will also require innovations in Operations and Maintenance (O&M) to manage the transformation.

Constant Upgrades and Patches Challenge Campus Networks

A typical campus network consists of core switches, aggregation switches, and access switches. A small-sized campus network requires dozens of access switches, whereas a medium-sized campus network needs hundreds of them, and a large-sized campus network deploys thousands. Each access switch must be configured with parameters such as port VLAN, Network Management System (NMS) IP address, Access Control List (ACL), and Quality of Service (QoS). During software upgrades or patch installs, configuration operations must be repeated, creating heavy workloads and errors.

The fast growth of wireless terminals, including tablets and smartphones, presents another major challenge. A campus network must provide robust Wi-Fi service to handle increasing wireless traffic. More and more WLANs are deployed in campus networks with mature Access Controller(AC) + Fit Access Point(AP) WLAN architecture. In this architecture, the AC acts as the device management controller for the WLAN system, managing and configuring APs. The APs provide WLAN access services for users. The APs are plug-and-play devices that do not require configuration and provide simple functions. Since both the configuration and management of APs are centralized on the AC, the APs no longer function as independent Network Elements (NEs).

The AC serves as the policy controller of a WLAN network as well. The AC obtains policies from the policy server, and then delivers the policies to APs through Control and Provisioning of Wireless Access Points (CAPWAP) tunnels. The APs execute the management and control policies on wireless users. The AC + Fit AP WLAN architecture significantly reduces the configuration workload for APs, simplifies AP software upgrade, and facilitates effective execution of policy controls.

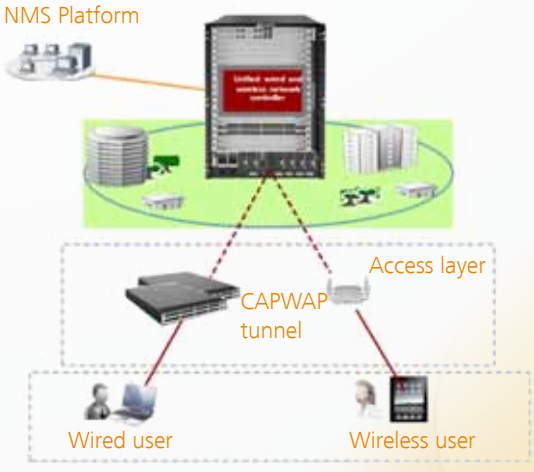
To extend the benefits of this working model to campus networks, Huawei applied its vast knowledge and experience learned from "AC managing Aps"

to the development of "core switches managing access switches" and the integration of wired and wireless networks. An integrated wired and wireless campus network brings much more efficiency and simplification to network management, allowing users to enjoy a consistent network experience.

Huawei Offers the Industry's First "Zero Access Layer Configuration" Solution

In the era of "data is king," a huge amount of production and business data is transmitted on wired and wireless converged networks. Network management must adapt to changes in the campus network architecture. For example, uniform management of wired and wireless users and uniform configuration of wired and wireless services becomes increasingly important in the era of Big Data.

To help customers adjust, Huawei launched the industry's first "Zero Access Layer Configuration" solution, which uses Huawei S12700 series agile switches as core switches. This solution applies the simplified wireless AC + Fit AP model to wireless networks, preventing the need for configuration updates over masses of access switches. In addition, the solution formulates a uniform user or network template by extracting the same attributes of wired and wireless networks, thereby implementing seamless and secured uniform wired and wireless management. As a result, network maintenance personnel do not need to learn and manage two sets of configuration commands and data for separate networks, reducing network O&M costs.



- **Zero-Configuration Deployment**

As the preceding figure shows, both the access switch and the AP download configuration data from the built-in wired and wireless controller in the Huawei S12700 through CAPWAP tunnels. The Huawei S12700 manages access devices including the AP and the access switch in a unified manner providing zero-configuration deployment.

- **Automatic Upgrade**

The Huawei S12700 Series Agile Switches manage version files for access switches and APs. Using the MAC address and IP address of devices, number of users, and number of access ports in Up status, the Huawei S12700 can perform automatic upgrades according to service requirements, which prevents network congestion caused by disordered scheduling during batch upgrades.

- **Plug-and-Play**

If an access switch or AP fails, the other switch or AP automatically obtains both version and configuration from the S12700 based on the network topology. No repeated operations need to be performed. The new access switch or AP offers instant plug-and-play performance right after replacement.

- **Integrated Template**

Unified authentication of wired and wireless users, a uniform policy configuration template for before and after user authentication, and the delivery of configurations to access switches and APs through the Huawei S12700 eliminates O&M problems caused by maintaining separate configuration profiles for wired and wireless networks, ensuring a consistent experience for both wired and wireless users.

iPCA – the Secret of Agility

By Liu Bi

In Pursuit of "Visible" Agile Networks

The increasing complexity of network infrastructure requires improvements in network management. Now, network management is changing toward visualization, automation, and intelligence. Among these changes, visualization of end-to-end traffic and security policy management stand out as the critical improvements needed for network management and maintenance.

According to a Gartner report, proactive network performance problem prevention now drives the majority of Operation and Maintenance (O&M) investments, representing 27% of total investment. The next two driving forces are fast network troubleshooting and Service Level Agreements (SLAs), accounting for 15% and 12% of investment respectively.

Traditional IP networks have many "invisible" maintenance issues. For example, traditional network management provides only network performance data, and network administrators are typically unaware of service data on the network. In other words, service performance is invisible. This invisibility results in low fault-location efficiency. Routes are also invisible. And because network administrators have no knowledge of service transmission paths, they cannot take measures to prevent network failures caused by route flapping.

How can these blind spots be eliminated?

Huawei believes that the traditional passive network O&M model should be replaced by a new network O&M model that actively monitors end user experiences and accurately identifies failure points and vulnerabilities. This new network O&M model will help customers quickly find security risks and take corrective actions.

An Evaluation of Traditional Fault Diagnosis

Network quality diagnosis and evaluation are the two core issues of network maintenance. Typically, IT managers cannot determine whether a potential risk exists in the network or where a fault occurs. What's more, they cannot make an objective evaluation of the performance and quality of services, such as video, voice, and network access. Performance and quality diagnosis in traditional campus networks also lacks effective End-to-End (E2E) fault location. As a result, fault diagnosis remains not only time-consuming and difficult, but it fails to meet user requirements.

Network performance fault diagnosis and quality evaluation are essential to reliable network operation. Already industry-backed research teams and standard organizations are engaged in establishing applied technical research and standards. One such standard is the Y.1731, which is an Ethernet layer OAM protocol established by ITU-T. Y.1731 performs single-ended packet loss statistics collection and dual-ended packet loss statistics collection as well as one-way delay statistics collection and two-way delay statistics collection to determine Ethernet performance and locate faults. ITU-T also establishes G.8113.1, which is an OAM protocol for MPLS-TP transmission. In addition, IETF, another leading international standard body, formulated the RFC6374 (Packet Loss and Delay Measurement for MPLS Networks) and RFC6375 (a Packet Loss and Delay Measurement Profile for MPLS-Based Transport Networks) for collecting MPLS performance statistics and locating MPLS faults.

Because the preceding protocols cannot be used on IP networks, RFC5357 (a Two-Way Active Measurement Protocol) and RFC4656 (a One-way Active Measurement Protocol (OWAMP)) are used for IP network performance statistics collection and fault detection. Meanwhile, Cisco has put forward its own proprietary Service Assurance Agent (SAA) Solution, while Huawei uses the Network Quality Analysis (NQA) mechanism to respond to the requirements of IP networks for maintainability and operability. All these fault detection mechanisms have one common characteristic: they all use an indirect measurement method, require insertion of dedicated detection packets, and calculate the detection packet-loss ratio to indirectly derive the service packet-loss ratio. IP communication is connectionless, so the path through which detection packets pass is not necessarily the one through which service packets pass. As a result, the detected path quality cannot accurately characterize the service packet transmission quality.

iPCA Technology

O&M in enterprise campus networks focuses on not only network function and performance but also user experience and network quality. iPCA (Packet Conservation Algorithm for Internet) technology, featured in Huawei's S12700 series agile switches, can quickly detect any user's video and voice service quality and instantly locate faults occurring on network links, cards, and even chips, greatly improving O&M efficiency. iPCA makes networks easy to operate and maintain, bringing about an essential change in enterprise campus network O&M.

iPCA is a pipe-monitoring technology that detects network quality using direct measurement. iPCA can measure network packet loss, delay, jitter, and traffic as well as implement precise fault location through hop-by-hop fault detection. Huawei's S12700 agile series switches feature flexible programmability and iPCA technology. The S12700 greatly improves network quality detection with precise fault location capabilities while reducing network O&M costs.

To solve problems with current detection methods, such as long fault-detection time, fuzzy fault scope determination, and inferior quality evaluation precision, Huawei introduced its fully programmable S12700 series agile switches equipped with Ethernet Network Processor (ENP) chips to implement the iPCA solution, enabling the S12700 to perform precise O&M in enterprise networks.

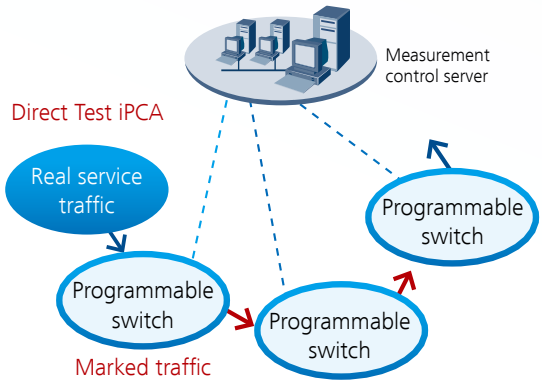


Figure 1 Working process of iPCA

As shown in Figure 1, the working process of the iPCA solution consists of two parts: measurement control servers and agile switches. The measurement control servers receive requests to perform detection on the target service traffic, inform agile switches of performing detection, collect statistics from each agile switch, and perform calculations and generate reports.

The iPCA offers the following advantages:

Huawei's Patented Technology: Solving Problems in IP O&M

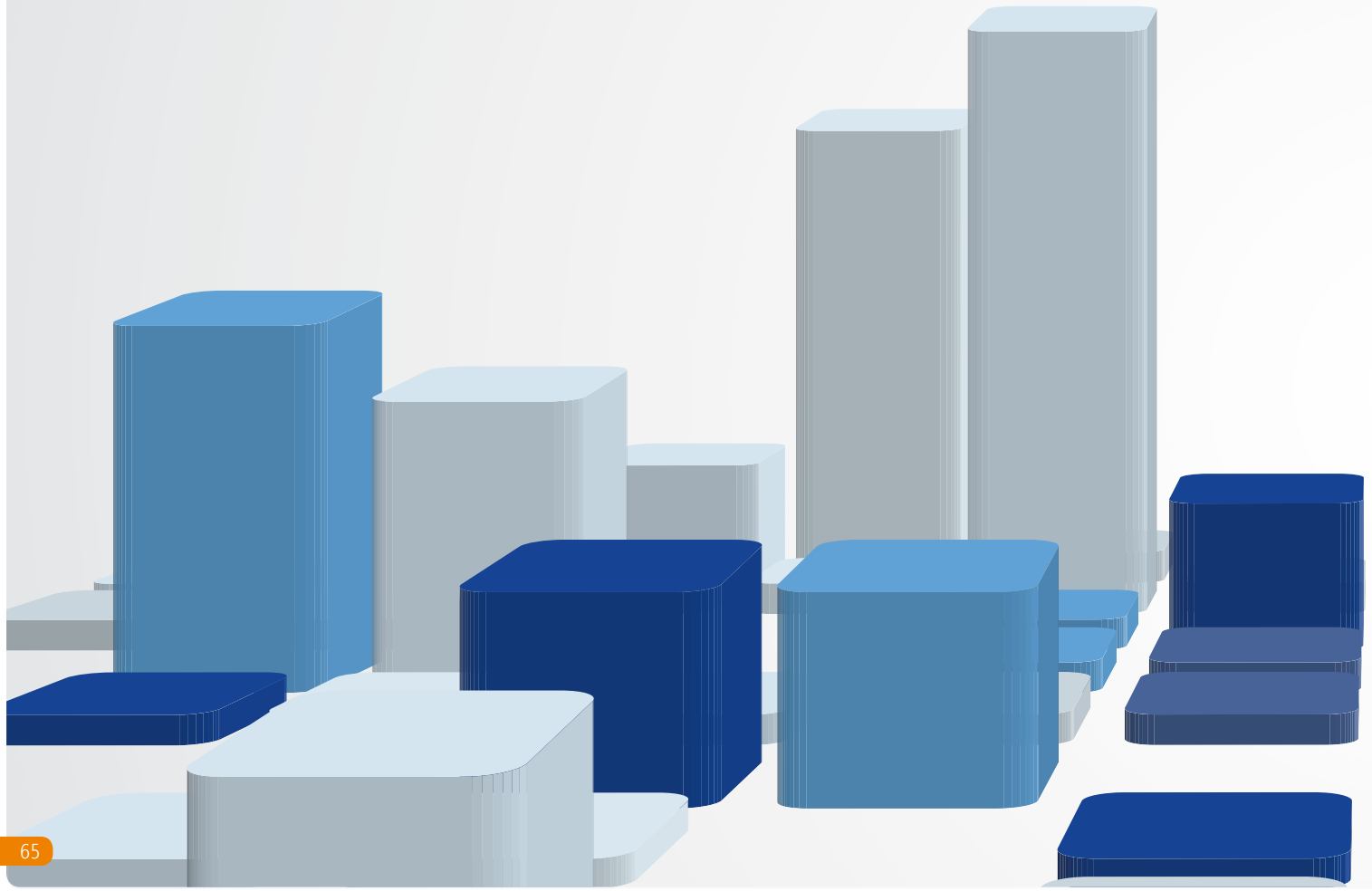
Huawei creatively uses the only reserved bit (Bit 0 in the Flags field) in the IPv4 packet header to mark the target service traffic. Most of the services that use IP for communications must use standard IP packet headers. This marking method does not rely on the service type, but instead allows the device to perform hardware processing more easily.

Direct Detection Mechanism: Implementing Precise Fault Detection

iPCA directly measures service traffic quality without sending test traffic. The detection path is the same as the actual service path. Faults on links, cards, and even chips can be located.

ENP: Allowing Detection of Any Service Traffic

To perform fault detection on target service traffic, the service traffic must be differentiated and marked. Performance of traditional switches in this area is minimal. Traditional switches can only differentiate service traffic by using a limited resource, the Access Control List (ACL), and by marking service packets by using the CPU. As a result, traditional switches cannot be deployed on a large or massive scale. Huawei's S12700 series switches are based on Huawei's patented ENP technology and can support up to 256K ACLs. The S12700 can identify any service traffic and mark the service traffic using microcodes, accelerating line-speed forwarding capability.



iPCA Scenarios

iPCA can be deployed in many scenarios including campus, Smart Grid, IP RAN, and Internet Service Provider (ISP) leased line environments. iPCA can quickly detect faults in video, voice, and wired and wireless applications by measuring packet loss ratios, delay, and jitter.

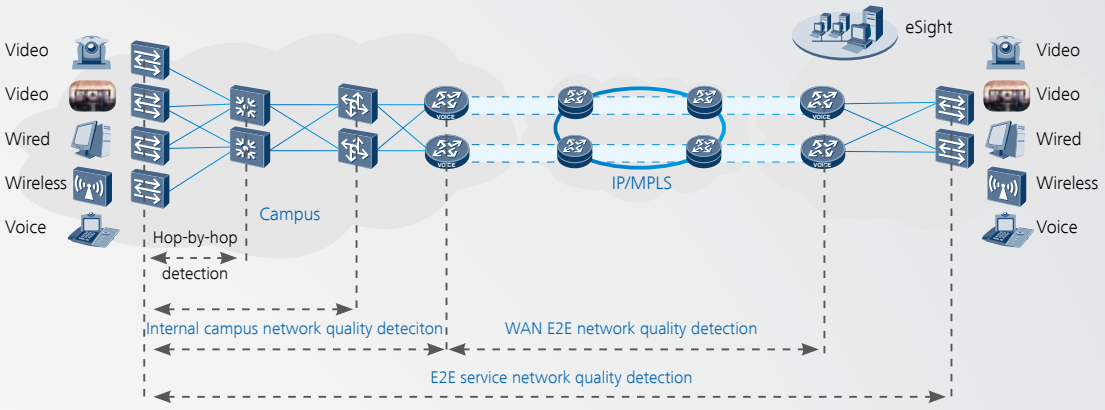


Figure 2 Campus scenario with iPCA

As shown in above Figure for the enterprise campus scenario, iPCA can detect network performance indicators at the access, aggregation, and core layers and network segments of a WAN network, hop-by-hop. iPCA can quickly and precisely determine the fault scope and immediately locate the card or chip on the network where the fault is occurring, guaranteeing fast and accurate fault troubleshooting. Although WAN networks do not support the iPCA feature, the iPCA can analyze the campus ingress and egress at both ends of the WAN connection to determine if a fault occurred.

Converged Network and Unified User Management

By Xia Yangsong

Campus Network Requirements for Refined User Management

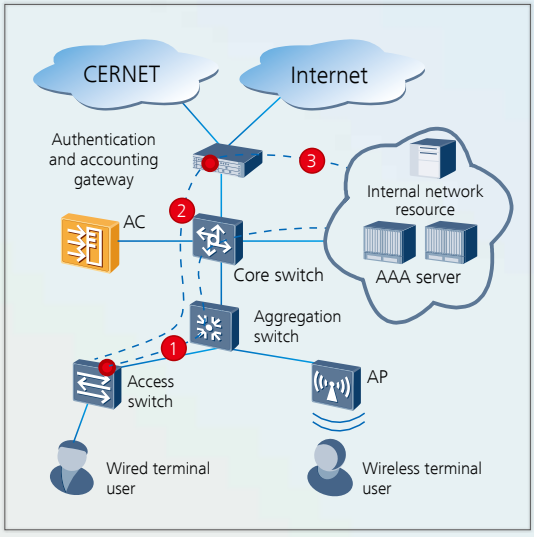
Education system reforms taking place globally and IT applications are accelerating the growth for basic education, higher education, and vocational education fields everywhere. These changes require networks with low equipment costs, self management, full wireless coverage, and comprehensive user management. Refined management of users, however, acts as the core requirement for the campus network.

To provide refined user management for education, device vendors in the industry offer two traditional user management solutions: one based on access and exit authentication and the other centered on independent Broadband Remote Access Servers (BRAS). The first solution places few requirements on switches, but its management capability is limited. The second solution supports refined user management, but users must purchase the expensive BRAS device separately.

Traditional User Management Solutions

Solution 1: User Management Based on Twice Authentications

In this solution, the access switch and authentication and accounting gateway control access to internal and external resources. Wireless users access campus networks through Aceess Controllers(ACs). Wired terminal users use the 802.1x client for the first identity authentication, the campus network access authentication. The access switch works as a Remote Authentication Dial-In User Service (RADIUS) client to interact with the Authentication, Authorization, and Accounting (AAA) server. After authentication, the access switch binds the access user to the MAC address, IP address, and physical port to ensure the authorized user has access to the internal resources on demand. When the user accesses external resources, the authentication and accounting gateway must perform a second authentication on the user. After this authentication is complete, the AAA server delivers the user's authorization information to the authentication and accounting gateway to enable accounting and monitor the user's online behavior.



Although simple in implementation, this solution has the following obvious defects:

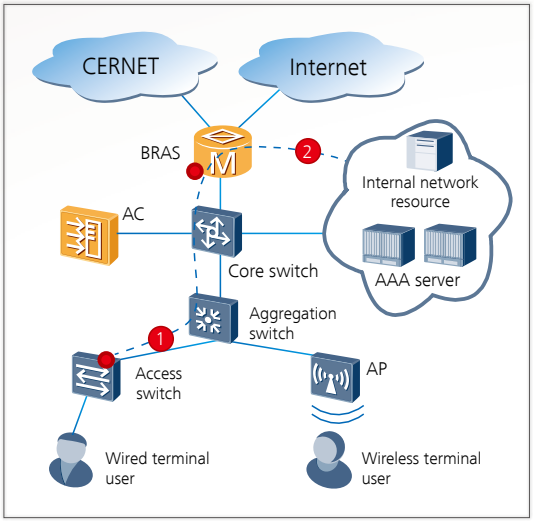
Excessive authentication points

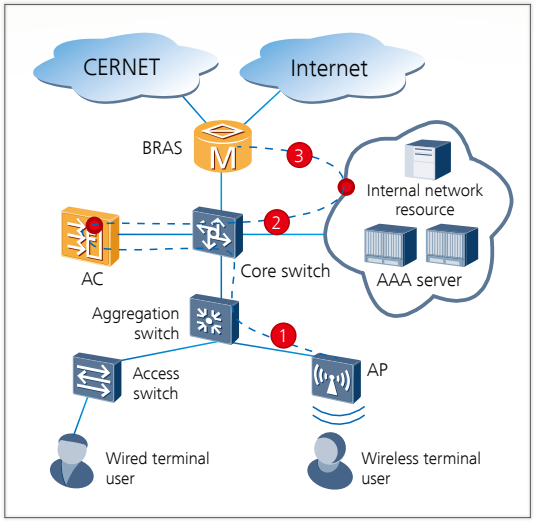
Wired users are authenticated through switches while wireless users are authenticated on the AC in a centralized manner.

Complex policy management

User access rights are controlled with an Access Control List (ACL) only. A medium-sized network requires thousands of ACLs, and a large-sized network requires tens of thousands of ACLs. The ACLs are deployed on different nodes, which complicates user management.

Solution 2: User Management Centered on stand-alone BRAS

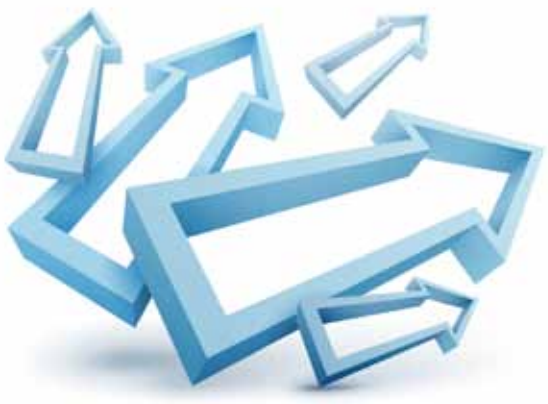




The BRAS is successfully deployed on carrier networks and now being introduced to campus networks. The BRAS provides multiple strong authentication and accounting functions: PPPoE authentication, IPoE + QinQ authentication, 802.1x authentication, portal authentication, traffic-based accounting, time duration-based accounting, prepayment, package-based accounting, accounting protection, or no accounting at all.

As shown in the preceding figure for wired user access, the access switch assigns a VLAN to each user to isolate access user traffic, ensuring unauthorized users cannot access the network. The access switch adds the Layer 1 tag to user traffic packets, and the aggregation switch adds the Layer 2 tag to user traffic. BRAS performs authentication on terminal users using PPPoE or IPoE protocol through QinQ encapsulation. Then BRAS sends an authentication request to the AAA server using the RADIUS protocol. After user authentication completed, the AAA server authorizes the BRAS and enables accounting to further implement integrated authentication and monitoring of both internal and external networks.

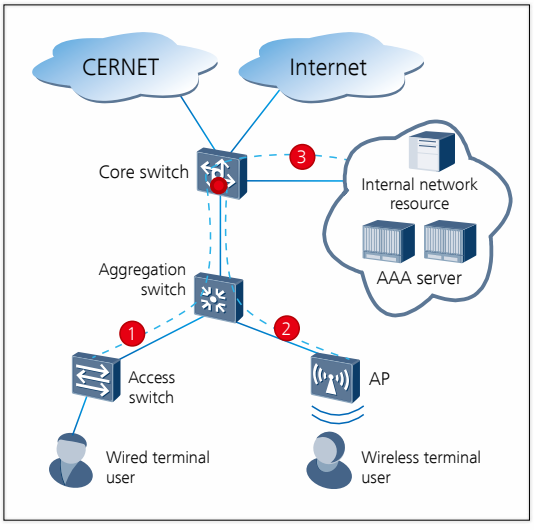
For wireless terminal (STA) users, the AC authenticates STAs, as shown in the preceding figure. Once authentication here is complete, the AAA server proceeds to perform admission authorization on the AC. In the meantime, the AAA server delivers the authorization information to the BRAS and completes access authorization to implement "one authentication for twice authorizations."



This solution features centralized authentication and simplified management by using a dedicated BRAS for user management. Nevertheless, this solution has the following drawbacks:

- Users have to purchase expensive BRAS devices independently.
- Difficulties remain in the association between the AC and BRAS because they are different physical devices.
- User authentication process is complex, and wired and wireless users cannot be managed in a unified manner.

Huawei Unified User Management Solution



Huawei offers the advantages of these two solutions in its Unified User Management Solution centralized on its own S12700 Series Agile Switches. The S12700's service card implements unified authentication of wired and wireless users. An independent user table is assigned to each user to implement user rights control, bandwidth control, and Quality of Service (QoS) control.

As the preceding figure shows, packets for wired terminal user authentication are transparently transmitted to the core switch through the access switch. At the same time, packets of STA user authentication are transparently transmitted to the core switch through a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel at the Access Point (AP). Then the core switch, with Unified User Management and built-in AC functions, sends the user's authentication information to the AAA server. After user authentication completed, the AAA server performs authentication, accounting, and behavior monitoring on the wired or wireless user through the core switch.

Compared to traditional user management solutions, the Unified User Management Solution provides the following advantages:

Unique Unified User Management and Native AC Function

Huawei's refined user management solution centers on its industry-leading S12700 Series Agile Switches, which provide Unified User Management and AC functions. Users can implement unified management of wired and wireless users without the needs to purchase BRAS, AC devices, or dedicated AC cards. This solution simplifies network deployment, reduces customer investments, and supports both IPv4 and IPv6.

Consistent Experience and Differentiated Services

The Huawei S12700 provides a consistent user experience no matter the access location or device, whether the user accessing the network directly from STAs with a smartphone or tablet PC, or from terminals running an Android Operating System (OS), or from wired terminals such as desktop PCs and video terminals. In addition, the S12700 supports full-scale, five-level Hierarchical Quality of Service (HQoS) scheduling and provides differentiated services for different levels of customers, fulfilling these key objectives:

- Same account for wired and wireless users
- Different network access speeds for internal and external networks
- Different costs for IPv4 and IPv6 deployment

Centralized Authentication and Access Layer Isolation

The Unified User Management authenticates wired and wireless users in a centralized manner, despite differences in the performance capabilities and access modes of access layer devices. Huawei's Unified User Management Solution supports multiple authentication modes including PPPoE, 802.1x, MAC address, portal, and IPoE. To satisfy diverse area and network Operation and Maintenance (O&M) requirements, the solution employs different authentication modes for differentiated management and control. For example, in the dormitory area, the PPPoE authentication mode can be used to prevent students from conducting malicious network attacks. In the teacher office area, IPoE + QinQ authentication mode can be used to simplify the authentication process without installing a PPPoE client. The simplest MAC address authentication mode can be used for dumb terminals, such as printers.

Simplified Policy Management and Cancellation of ACL Configuration

Traditional campus networks use "device-centered management." Bandwidth management and rights control is performed on users rather than ports only by using the limited ACL resources residing on switches. The S12700 uses a "user-centered management" design concept. Each user has an independent user list for user rights control, bandwidth control, and QoS control. The S12700 can authorize users based on user group, domain, and time. Upstream and downstream bandwidth (1 kbit/s) is also controlled. By using simple and flexible policy management, the S12700 allows for differentiated accounting according to time period, service type, and access address. Moreover, Huawei's Unified User Management solution can effectively conduct security policy association to improve security. For instance, a user can access a greater amount of teaching resources in a laboratory than in a dormitory building.

Summary

Huawei launched its Unified User Management Solution using proven technologies in carrier-grade products and enterprise environments. Huawei leverages the following capabilities in the Unified User Management Solution:

Solid foundation of switching and WLAN technologies: Huawei deploys mature switches and Wireless Local Area Network (WLAN) platforms, which are listed in the Challengers quadrant of Gartner's Magic Quadrant and widely used in various industries.

Excellent chip development capabilities: Huawei has in-depth chip R&D capabilities. Using Huawei's in-house Ethernet Network Processor (ENP), the S12700 implements line-speed forwarding and consumes little power like Application-Specific Integrated Circuits (ASICs) while providing flexible programmability.

In-depth understanding of campus networks: Huawei maintains its long-standing dedication to developing high-quality campus network solutions.

Huawei combines its industry-leading technologies and expertise with customer input to offer the innovative Unified User Management Solution to campus networks. The Unified User Management Solution offers truly refined user management and helps transform campus networks from "device- centered managemen" to "user-centered management. "

SDN Architecture-based Next-Generation Agile Campus Network

By Ji Ya'nan

Challenges for Campus Networks

Today's world is witnessing a huge change in services transmitted by campus networks. The services are changing from data service and a small number of voice and video services to real-time services such as cloud computing, mobile office, social media, and a great number of voice and video services.

Fast-Changing Services Bring Various Challenges to Live Networks.

1. Challenge Brought by Mobile Office: Static and Manual Configuration vs Dynamic Location + Dynamic Traffic

User-centric policy management is one of the core elements that ensure service security and experience. Currently, many enterprises use a manual and static configuration mode to manage policies. After many enterprises are globalized, employees often need to work remotely. Accordingly, security and Quality of Service (QoS) polices must be migrated to locations where users work. The manual and static configuration mode results in a large amount of workload and cannot quickly respond to user requirements. Consistent experience in mobile office is quite a tricky problem. When employees work remotely, they often suffer multiple problems such as high delay in network access, poor voice effect, and low work efficiency.

2. Challenge Brought by Network Security: Single-Node Protection vs Full-Scale Network Attack Behaviors

Considering security threats, enterprises usually deploy various security devices such as firewalls, Intrusion Prevention System (IPS) devices, and Data Loss Prevention (DLP) devices. However, these devices cannot interact with each other, and this kind of defense is single-node and static defense. Nowadays, enterprises are faced by the following security problems:

- Fuzzy security edge: Bring Your Own Device (BYOD) increases terminal security and information security threats, and enterprise globalization blurs the network edge.
- Diversified attack methods: According to statistics by Gartner, 75% of the security threats occur at the application layer, and more than 50% of the security threats are caused by an organizational team.
- Increasing unknown threats: A growing number of unknown threats are used to elude traditional security protection methods. In China, 17.98 million new viruses appeared in 2010 alone.

Network security threats are ubiquitous, and network attacks are complex and fast-changing. Therefore, today's networks need collaborative security protection over the entire network.

3. Challenge Facing Network O&M Personnel: Single-Node Protection vs Full-Scale Network Attack Behaviors

Two great challenges for Operation and Maintenance (O&M) are as follows:

- Quick service quality detection and fault location

Video and desktop cloud services are real-time services that require high network quality. For example, video service requires that the packet loss ratio should be lower than 10-6, while voice service requires that the packet loss ratio should be less than 10-2. The current network cannot detect problems such as mosaic and unclear hearing of which users are aware. This often leads to employees' complaints. What is worse, there are no quick and effective methods for troubleshooting faults after these problems are reproduced.

- Massive devices that need to be deployed and managed

Lots of access layer devices result in considerable manual and static configurations. In addition, wired and wireless networks cannot be managed in a unified manner.

4. Challenge Brought by Multiple New Services: Lagging Networks vs Fast-Changing Services

The rapid development of new services leads to a growing number of protocols and standards. The number of IETF RFCs increased from several hundred in the 80s to nearly 7,000 in 2009. Nowadays, if lease mode is used to deploy a new service, the service takes a couple of days to go online. However, it takes at least one year to develop a new device and at least two years to develop a chip. As a result, traditional networks cannot quickly adapt to the fast-changing services.

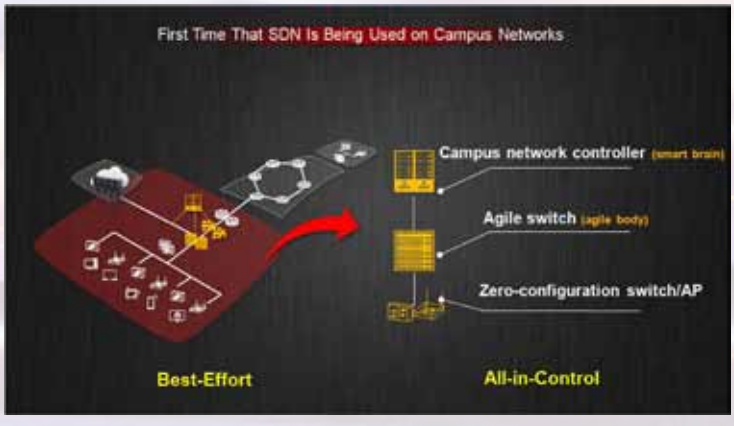
SDN Architecture-based Next-Generation Agile Campus Network

Campus network urgently needs a brand new architecture to quickly adapt to service development. Thanks to its Agile switches and campus network controllers, Huawei becomes the first device vendor in the industry to use the Software Defined Networking (SDN) architecture on campus networks. First, the campus network controller functions as a smart brain, implementing collaborative control and policy management over the entire network. Second, the Agile switches function as an agile body of the network, implementing agile awareness and execution of the policies. Finally, a large number of access devices such as switches and Access Points (APs) can go online without configuration, greatly simplifying network configuration and management. By using a brand new network architecture, Huawei has put forth five innovative solutions: ubiquitous service access, security collaboration, service detection and management, in-depth wired and wireless network convergence, and fully programmable network. Together these innovative solutions enable the network to provide professional services more agilely.

Innovation 1: Ubiquitous Service Access

Industry's First Service Experience-Centric Network Solution The Campus network controller provides O&M personnel with policy configurations including user group attributes and QoS that are oriented to service requirements. Users can access the campus network at any place. Campus network controllers can detect users' access position and automatically deliver policies to network control points such as aggregation switches and egress routers to perform security control and QoS scheduling, implementing ubiquitous policies. In the future, campus network controllers can associate with data center controllers to migrate users' service resources, for example, storage and desktop cloud Virtual Machines (VMs), together with the access location of user terminals to the nearest data center, implementing ubiquitous resource and ubiquitous experience.

Work groups are dynamically created based on identity so that employees who are thousands of miles away from the company can still work in ,seemingly, the same office. To ensure security protection, an enterprise assigns isolation domains by department or service. Each time a service isolation and network adjustment of a large campus involve adjustment of tens of thousands of configuration polices. Maintenance of the isolation domains is difficult, and errors are likely to occur. Huawei campus network controllers can provide work group-based vertical (south-to-north) and horizontal (east-to-west) access policy configurations and automatically deliver and execute the configurations after users access the campus network, building a ubiquitous virtual network.



Innovation 2: Security Collaboration, Implementing Distributed and Dynamic Detection as well as Full-Scale and Proactive Defense

Based on policy control, campus network controllers integrate the security log management center. Relying on highly efficient big data analysis and event association capabilities, the controllers can perform a collaborative analysis of security events on the entire network, accurately detect potential security threats, and associate with user security policies, implementing blocking by principle of proximity. For example, when the security log management center detects Distributed Denial of Service (DDoS) attacks on a user, it automatically delivers secure access policies at the access layer to isolate the user or directly force the user to go offline.

The controllers can also define untrusted traffic polices (for example, visitor traffic) and automatically direct the untrusted traffic to the security center for cleaning, which prevents potential threats and implements proactive defense.

Innovation 3: Service Detection and Management, Industry's First Technology That Enables the IP Network to Detect Service Quality

Traditional network quality detection methods such as Network Quality Analysis (NQA) and Y.1731 need to insert dedicated detection packets or confront packet disorder. The network quality detection precision of these detection methods is lower than 50%. Additionally, these technologies have multiple problems including a single monitoring object, limited application scenarios, and limited network types. Based on many years of technical research, Huawei has put forth the Packet Conservation Algorithm for internet (iPCA), which is the first technology that adds a proactive quality detection mechanism to traditional networks. iPCA implements real-time quality detection and fault location, therefore solving the difficulty in ensuring IP network experience. iPCA identifies and dyes service traffic packets and detects the dyed packets at both ingress and egress. In this manner, iPCA can detect quality parameters including packet loss ratio, latency, and jitter. This technology calculates service streams and implements real-time network quality detection during transmission of service data flows between users. Compared to traditional network quality detection methods, iPCA technology offers the following advantages:

- Zero traffic cost
- Applicable to any IP-based network type (unicast and multicast) and any network size.
- High fault location precision (card-level precision)

Innovation 4: In-Depth Wired and Wireless Network Convergence

Wireless Used as Wired Networks Through its unique programmability, Huawei's Agile Switches integrate functions, including Control and Provisioning of Wireless Access Points (CAPWAP) tunnel termination, of traditional Access Controllers (ACs), directly manages APs, and forwards traffic. In addition, on the management interface, an AP can be virtualized into a port to implement "Wired Network + Wireless Network = One Switch", greatly lowering requirements on skills of the O&M personnel after WLAN network deployment.

Wired Used as Wireless Networks Based on CAPWAP tunnels, Huawei's Agile Switches use the method in which wireless APs are managed to manage access switches to implement "Access Switch = AP, Aggregation Switch = AC." Similar to AP deployment, access switches can be deployed without configuration, which reduces the workload of deploying massive access layer devices.

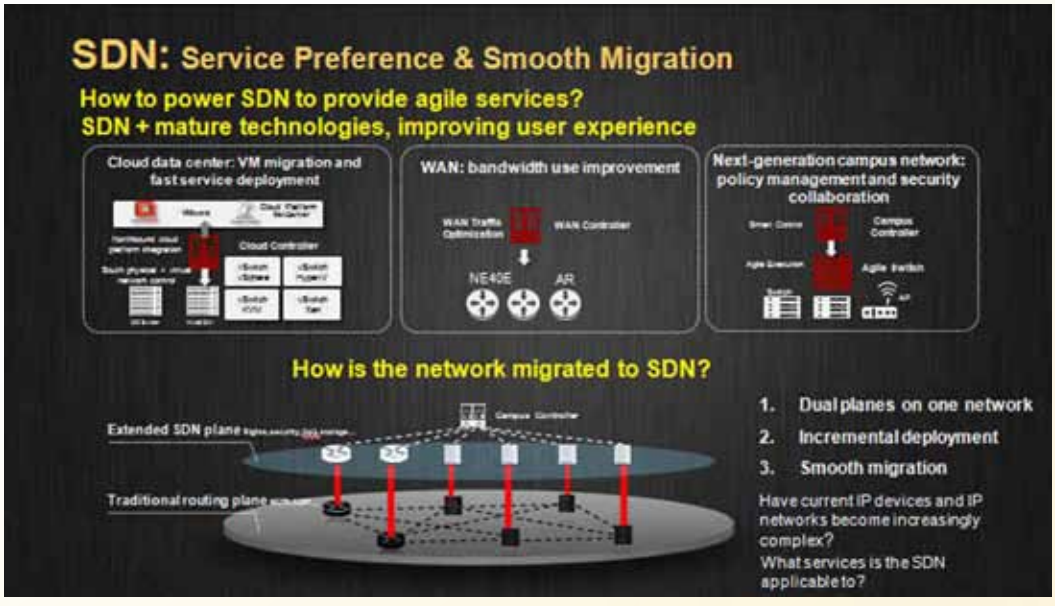
Innovation 5: Fully Programmable Network and Smooth Evolution

ASIC-based switches cannot flexibly adapt to the requirements of new services. Completely pure OpenFlow network deployment has potential risks. To prevent too frequent network upgrades and reconstructions and protect user investments, Huawei's agile switch-based, next-generation campus network provides full programmability, implements a smooth upgrade on the existing network, and uses the SDN idea plus mature technologies to solve the following actual problems of users:

- Dual planes on one network: traditional routing plane and SDN extended plane.
- Traditional services such as OSPF and BGP run on the traditional routing plane. New services and network problems that the traditional routing plane cannot solve, such as security policies, QoS, and service path optimization, run on the

SDN extended plane. This ensures that the innovative experience brought by SDN become available in advance without affecting the existing services.

- Incremental deployment: Uses the SDN architecture idea to design the network as a "Smart Brain" + "Agile Body"
- On the premise of ensuring the stability of traditional services, new services are incrementally deployed on demand. The network architecture can smoothly evolve into the SDN architecture.
- Smooth migration: Uses Huawei's unique Protocol Oblivious Forwarding (POF) technology and a large capacity of traffic entries as support for software and hardware capabilities to allow the enterprise network to become the fully programmable network in its real sense, protect enterprise users' existing network investments in a better manner, and enable the network to evolve into the SDN smoothly.

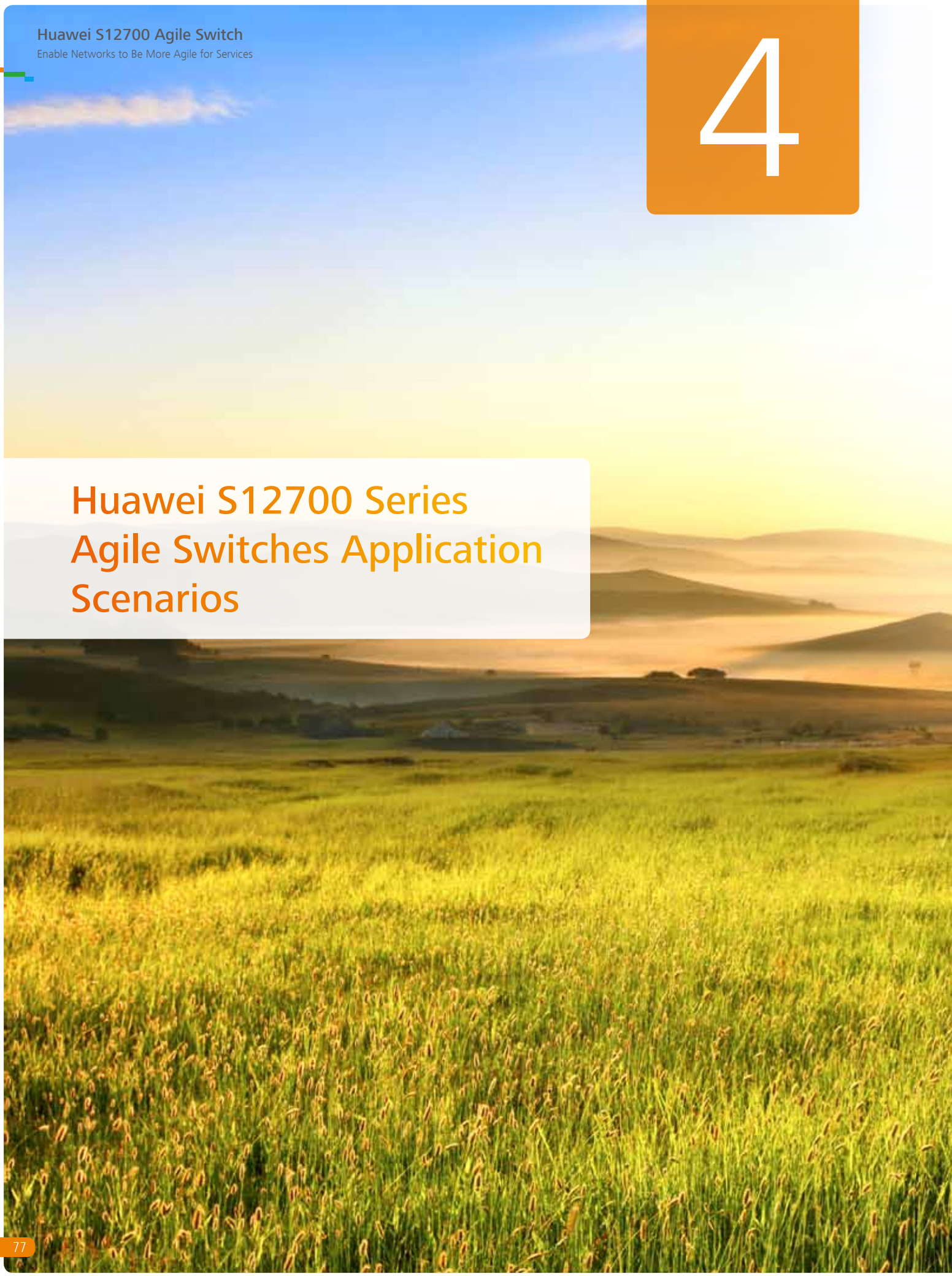


Summary

Huawei's SDN architecture-based next-generation agile campus network solves the problems of traditional campus networks, such as lack of user experience guarantee, low deployment efficiency, and low-speed response to service requirements. Services passively adapt to the traditional campus networks, while the next-generation agile campus network proactively adapts to various services. In this manner, a service-friendly network is created. Furthermore, the SDN architecture can be used to address users' live network problems and cam seamlessly evolve into the future network architecture, thereby allowing the network to provide professional services more agilely.

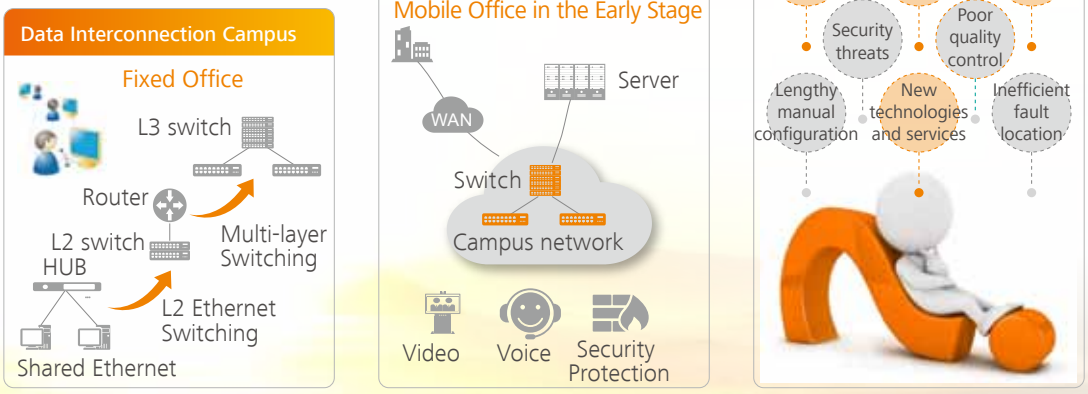
4

Huawei S12700 Series Agile Switches Application Scenarios



Large Enterprise Campus Networks

Evolution of Enterprise Campus Networks



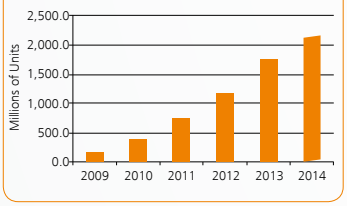
With the development of the IT technology, the working mode is also changed more and more fast, 20 years ago we worked on PC, 10 years ago we began to work on the laptop, now we worked with my own device, which we called it BYOD. And the change of working mode also faces many new challenges to our campus network.

BYOD Challenges for Campus Networks

Seamless Wired and Wireless Coverage

- Wireless Local Area Network (WLAN) chipset shipments are expected to hit 1.7 billion pieces by the end of 2013, a 70% increase compared to 2012.
- Deploying wireless networks over traditional fixed campus networks results in repeated software and hardware investments, which significantly increases CAPEX and OPEX.

Figure 1: Global Shipment Forecast for Wireless Local Area Networking (WLAN) Chipsets (Millions of Units)

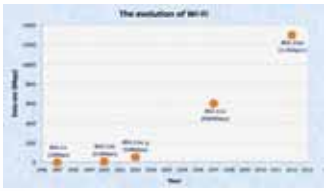


Ubiquitous Network Access

- In 2012, more than 1 billion smart terminals were shipped.
- In 2013, 1.2 billion employees are estimated to work remotely; 35% use mobile devices, which requires full Wi-Fi coverage.

Mobile Multimedia Service

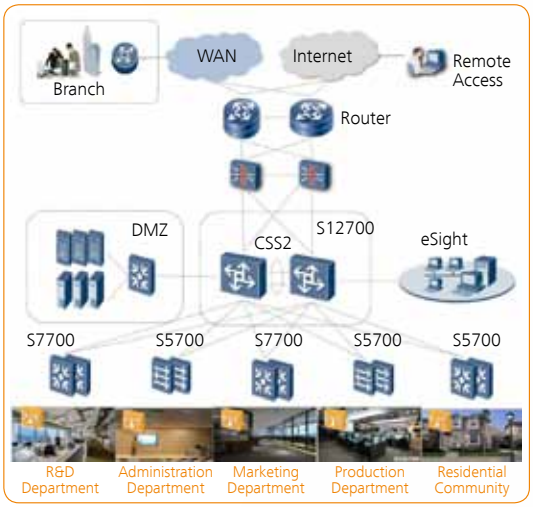
- Multimedia applications such as High-Definition (HD) video and teleconferencing lead to traffic surge, which requires high bandwidth to ensure a good user experience.
- Today, fifth-generation Wi-Fi technology 802.11ac are widely used. The current highest transmit rate is 1.3 Gbit/s, three times higher than that of 802.11n.



Because of the rapid development of wireless network, the standard 802.11b/g/n/ac is grow more and more fast, so the bandwidth of wireless network is also very big. And the benefit of the wireless network is we don't access the network with cable, also we can freely move to the other places in the campus, and no need to worry about the service interruption. So most of the enterprises were recommended to construct an independent wireless network, and this network is separated to the former wired network.

Nowadays many companies allowed their employee to take their own device to the company to do work. How to help the employee to work properly is the big problem that all the company must face it or resolve it. In the traditional way, we use the SSID and user account to identify the different user, but we can't identify which kind of device we used now, whether the device belong to company or the employee. How to deploy the different access right in different places even we use the same user account? How to deploy the different access right in different devices? How to deploy the different access right when the user is inside or outside of the company? These are all the problems must be solved in our new campus network.

S12700 in a Campus Network Solution



Wired and Wireless Network Convergence

- The S12700's native Terabit AC manages 4,096 APs.
- Wired and wireless network convergence reduces networking costs.

Unified User Management Policy

- S12700's Unified User Management enhances network security with unified authentication and unified policy.
- Strong user management capabilities and refined user control optimize usability.

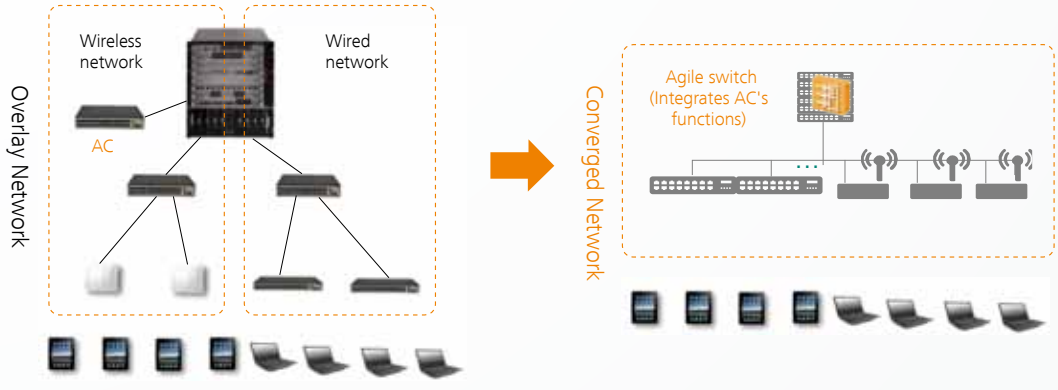
End-to-End (E2E) Precise O&M

- The advanced Network Management System (NMS) unifies wired and wireless device management.
- Graphical User Interface (GUI)-based network performance management implements refined traffic management.

According to Huawei's latest campus network solution, we deployed the S12700 at the core layer and S7700/ S5700 at the aggregation layer. This solution can solve a series of problem just like the integration of wired and wireless network, integration of network user management and many other things which all come with BYOD.

Wired and Wireless Network Convergence Slashes Networking Costs

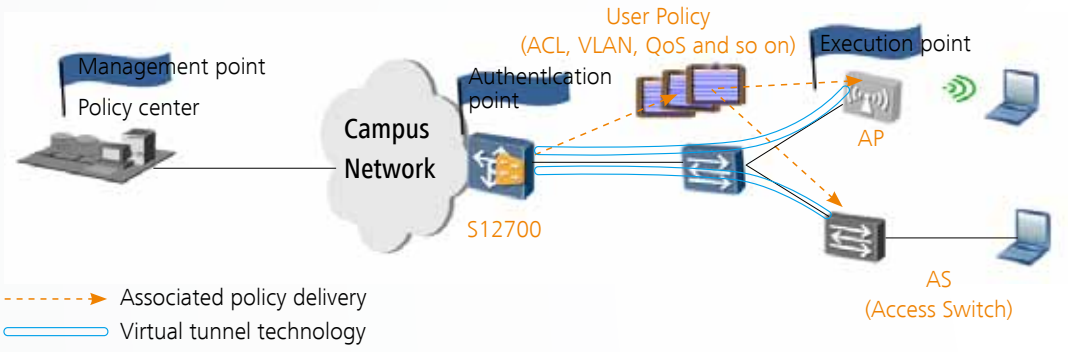
Evolution of Wired and Wireless Networking Models



S12700 support the native T-Bit AC, and it support 1Tbps switching capacity, compared with the 20Gbps switching capacity of normal AC in industry, the switching capacity has been improved for 400 times. AC will never be the bottle neck of the wireless network. In addition the native AC of S12700 can manage as more as 4000 APs, it can fulfill the wireless requirement of any size of campus network. With the S12700 we can support the real integration solution for wired and wireless campus network. Compared with the former separated wired and wireless networks it also can deduce the network TCO.

S12700's Unified User Management

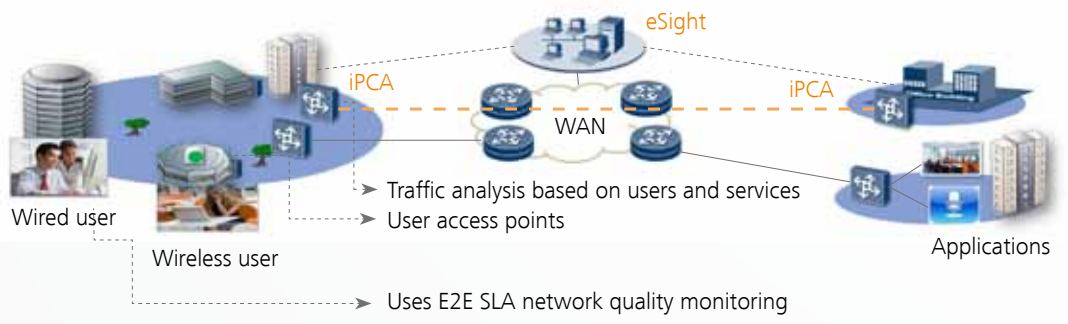
Unified User Management Model



The complexity of network user management will be reduced, because S12700 support the Unified User Management. Beside this S12700 also can provide security access, which can help the operation and maintainance team to achieve the fine 5W+1H (who/where/when/whose/what/how) user management.

E2E O&M for Unified Wired and Wireless Management

Unified Wired and Wireless Management Model



S12700 can support the iPCA(Packet Conservation Algorithm for Internet), which can support the across WAN failure detection. iPCA is a MP2MP measure mechanism , which can color the real IP traffic to detect the packet delay and loss, so it can help the maintainance team to diagnose the network failure as soon as possible.

Campus Networks for Schools

Evolution of Campus Networks for Schools

90s

LAN Era

- Desktop Personal Computer (PC)
- Teaching, experiments, and office assistance
- Standalone PC + Telnet

Low popularization with a single service

00s

Internet Era

- Desktop and portable PC
- Remote teaching, information retrieval, and network access for students
- Internet

Rapid development of wired networks

Today

Cloud Network Era

- Various types of mobile terminals
- HD remote teaching, Video on Demand (VoD), cloud services and Social Networking Services (SNS)
- Web 2.0

Wired and wireless convergence with a blurred campus edge

With the development of Internet/Intranet, education is stepping to the digit era, and the construction of the campus network will help the school to share the information and resource with the outside. For example in china, all the education department, schools, colleges and universities connect together with the CERNT (CERNT is Chinese education network), and CERNT also connected to the internet. Inside the campus, school administrative system, teaching management system, library system and other routine systems are all connected with the campus network.

The campus network already have 3 phases, first one is era which can only support some teaching experimentation and assistant working system. Second one is internet era, which can support the online remote classroom and information search. And now is the third phase, which can support the high definition remote classroom, teaching resource sharing, paperless classroom and so on.

Requirements on Network Devices

Wired and Wireless Convergence

Wired and wireless networks converge as one network, simplifying management of K-level APs and enabling smooth forwarding.

Refined User Management

Unified authentication management and effective policy controls support multiple user access to the campus network from various locations.

Simplified O&M Management

A simple network-level O&M solution is required to reduce complexity and manual tasks and adapt to rapid network upgrades and flexible capacity expansion.

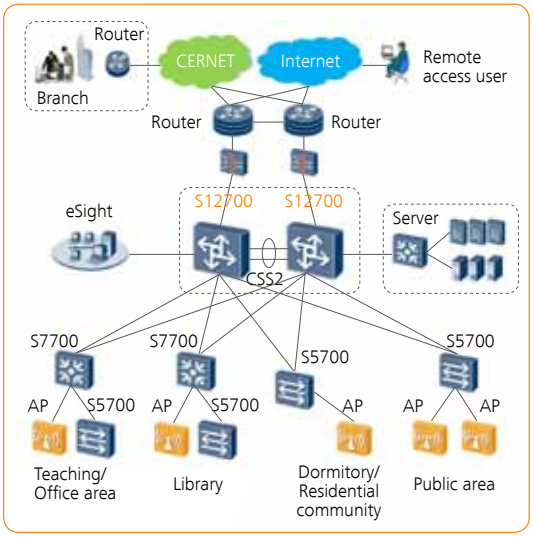
Cutting-Edge Network Technology

Network devices must be adaptive to next-generation networks and support programmability and SDN.

The challenges of campus network:

- College and universities normally have more than 10K teachers and students, if everyone have 2 or 3termial, the wireless network will need more than 1000 APs, how to meet the coverage and bandwidth requirements is the most important thing than should be considered by every network designer
- Different zone in the campus have the totally different access and authentication requirement, for example the teaching zone, LAB zone and living zone. In the campus network, we need a unified management and authentication node to manage the different terminals of different users in the different zones.
- The maintainance of the campus network was normally charged by the maintainance center, and with the development of the network, the campus is becoming more and more complicated, we need a unified NMS to manage all the devices and services in the network.
- The campus network of colleges and universities must afford some research mission, so the network must meet the requirement of the next generation network to support some SDN features.

S12700 in Campus Network Solutions for Schools



Networking Solution

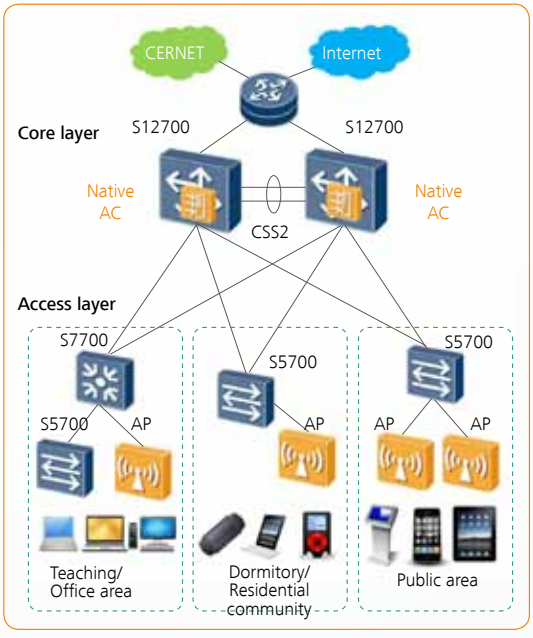
- Gigabit access + 10 GE aggregation + 100 GE core
- Core layer is deployed with S12700, native AC, and Unified User Management to simplify the network architecture.
- Horizontal virtualization + vertical virtualization, high reliability, and easy management

Customer Benefits

- Terabit AC manages 4,096 APs, ensuring full coverage.
- Unified authentication and unified policy ensure networking flexibility.
- Access devices are plug-and-play, ensuring simplified configuration and easy management.
- SDN opens the future of campus networks for schools.

We recommended GE at access layer and 10GE in the aggregation layer, and 100GE at the core layer in the latest generation campus solution for colleges and universities. And S12700 support native AC and Unified User Management, which can solve a series of problems, such as unified wireless and wired network and the unified wired and wireless user management.

Wired and Wireless Network Convergence for a Seamless Campus Network



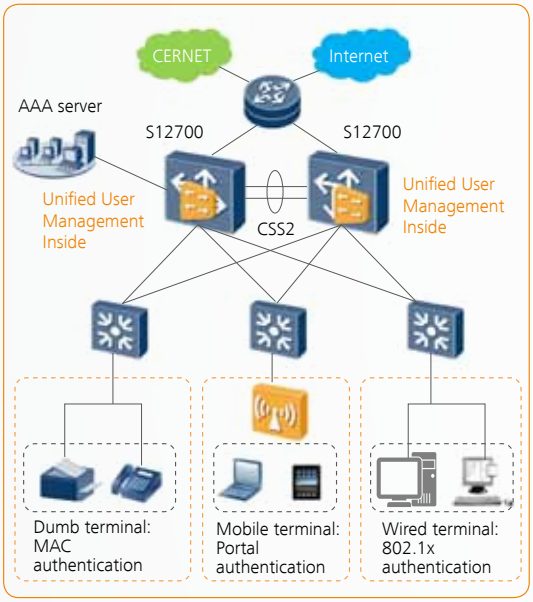
Integrating AC

Core layer S12700 with native Terabit AC satisfies the requirements of wireless terminal users for ubiquitous network access at any time.

- Converged forwarding: The native Terabit AC can manage 4,096 APs and 65,536 users, managing all APs in the campus network, implementing management convergence and forwarding convergence, and eliminating the forwarding bandwidth bottleneck of external or card ACs.
- Reliable access: AC hot standby ensures uninterrupted wireless access and enhances campus network reliability.
- Highly efficient management: Access switches and APs are managed in a unified manner through a unique technology, creating the industry's first access layer Zero-Touch network and simplifying campus networks.

S12700 support native T-Bit AC, can manage 4K APs and 64K users, the native AC can integrate the forwarding and control plane of the wireless network. Compared with traditional AC, the native AC will never be the bottle neck of the whole network. Beside this S12700 also can support AC hot backup, which can insure that 7*24 hours wireless service experience.

Refined User Management and Control for a Secure Campus



Unified Authentication and Unified Policy

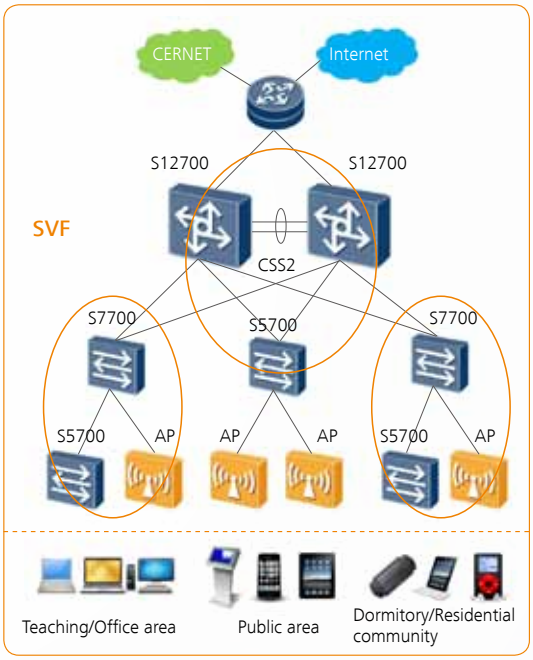
The core layer S12700 with native BRAS provides cost-effective and secure access and policy controls.

- Unified Authentication: Multiple integrated authentication modes such as MAC authentication, Portal, and 802.1x satisfy a range of user requirements for ubiquitous network access in different areas.
- Unified Policy: Gateway, policy server, and policy execution devices are integrated. Policy management and control are dynamically performed based on users to implement management restructuring.
- Ultra-large capacity of ACLs: The S12700 supports 256,000 ACLs on native cards to implement refined user-level policy deployment.

The Unified User Management of S12700 can support MAC, Portal, 802.1x and many other authentication modes, which can provide economic and security access and policy control for the campus network.

S12700 integrate the authentication gateway, policy servers and policy execution function together, which can adjust the user right dynamically, based on the identifying of user, terminal, time and location information.

Plug-and-Play Access Devices for an Agile Campus



Virtualization Simplifies O&M

Super Virtual Fabric (SVF) provides the simplest management for campus networks.

- Simplified management: The S12700 can virtualize wired and wireless devices into a management Network Element (NE). Access switches and wireless APs are plug-and-play and need zero configuration, greatly improving campus network management efficiency.
- Lowered costs: Access devices only expand ports without any control. Small-sized box devices can be used to cut campus network investment.

S12700 support SVF (Super Virtual Fabric), which can virtualize the access switch and access point (AP) as a line card or wireless port of the S12700. Hundreds of wired and wireless devices virtualized as one device, this will significantly simplify the management and expansion of the network.

S12700 can provide the programmability, because S12700 is based on the ENP (Ethernet Network Processor) chipset, and this chipset was produced by Huawei, and it's specially designed for Ethernet switch.

With this ENP chipset, S12700 switch can meet the research and expansion requirement for the colleges and universities in the next 5 to 10 years.

Metropolitan Area Network Core

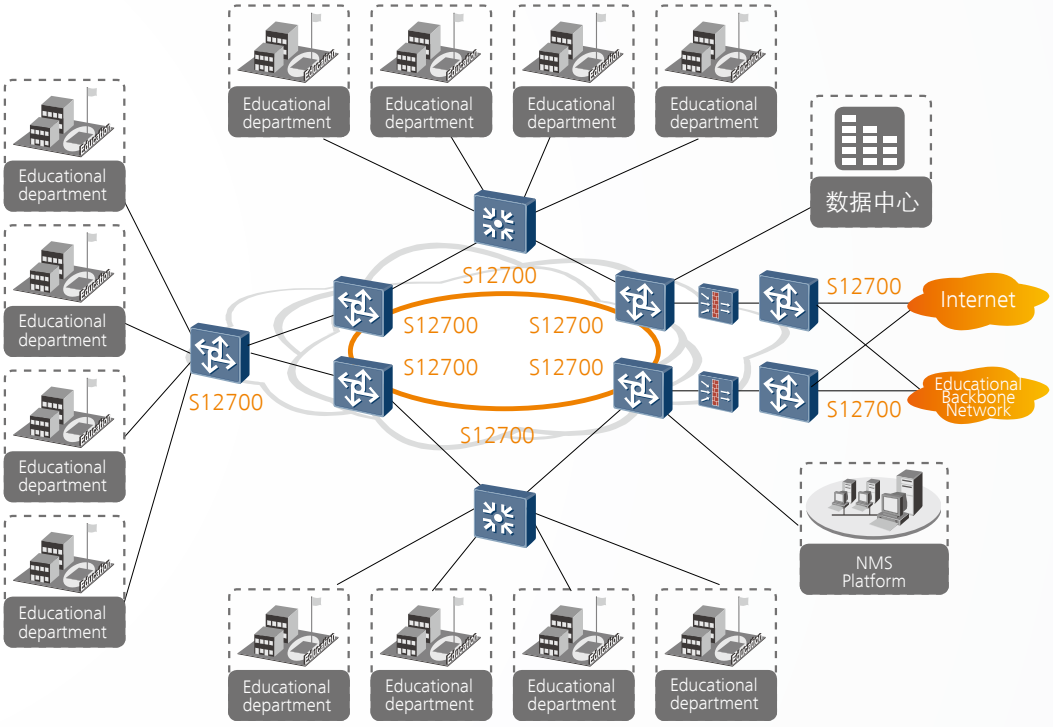
Development of the Educational Metropolitan Area Network

In the cloud era, education network resources will be centralized. Taking advantage of the extraordinarily powerful computing capability and massive teaching resources, education networks provide a wide variety of applications such as digital library, online teaching, and remote assistance to college and university students and scientific research institutions. Requirements of educational MAN construction are focused on high cost-effectiveness, Long Term Evolution , and multi-service transmission.

Educational MAN Requirements in the Cloud Era

- Lower CAPEX boosts cost effectiveness.
- High network reliability and simple O&M trim OPEX.
- Supports GE, 10 GE, 40 GE, and 100 GE, a minimum 10-year life cycle evolution, and easy network expansion.
- As educational networks are oriented to research fields so that new technologies can be easily used, networks must have multiple service transmission capabilities.

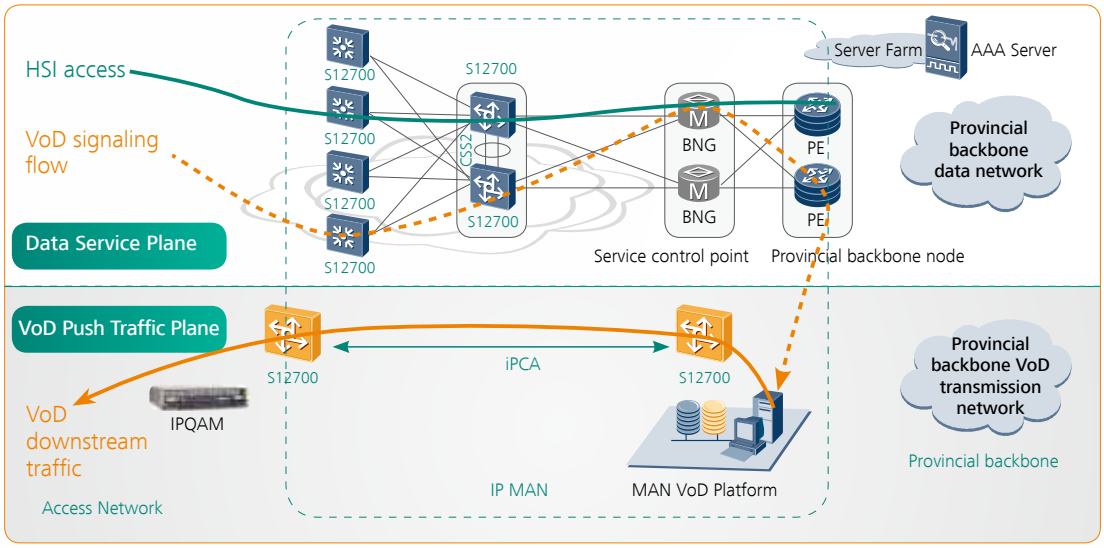
Huawei Educational MAN Solution



Customer benefit:

- Modular network can be easily managed and expanded, all the education departments can access to the network
- 100G core +40G aggregation，fulfill the network expansion in next 10years, protect customer's investment.
- The whole network was based onS12700 agile switch, which can provide high reliability, easy maintenance and low OPEX
- Deploy switch in whole network， reduce CAPEX
- SDN ready core switch, new service can be supported rapidly

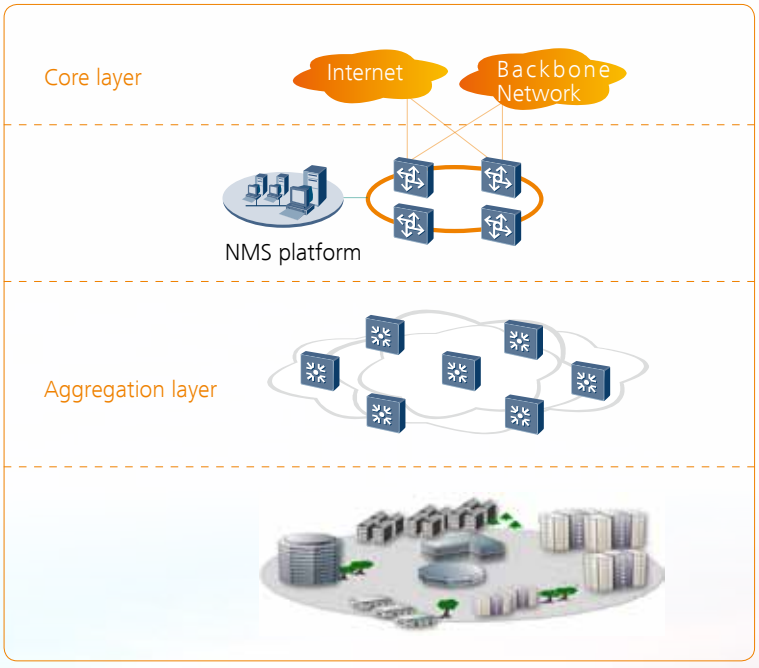
Huawei Broadcast and TV MAN Solution



Broadcasting & TV MAN architecture is divided into two planes: data service plane and VoD forwarding plane. The data service plane transmits common network access services and VoD signaling traffic, and the VoD forwarding plane to transmits VoD downstream data traffic.

The data service plane consists of the MAN aggregation network, service control points, and MAN cores or provincial nodes. In the Huawei Broadcasting & TV MAN Solution, the MAN aggregation network comprises S12700 series agile switches, multicast services are recovered within 100 ms if a fault occurs, and users do not sense the service switching process. Based on traffic volumes, the VoD forwarding plane can use S12700 series agile switches to build a flattened two-layer (core layer and access layer) network, which simplifies network operation and maintenance (O&M) and management.

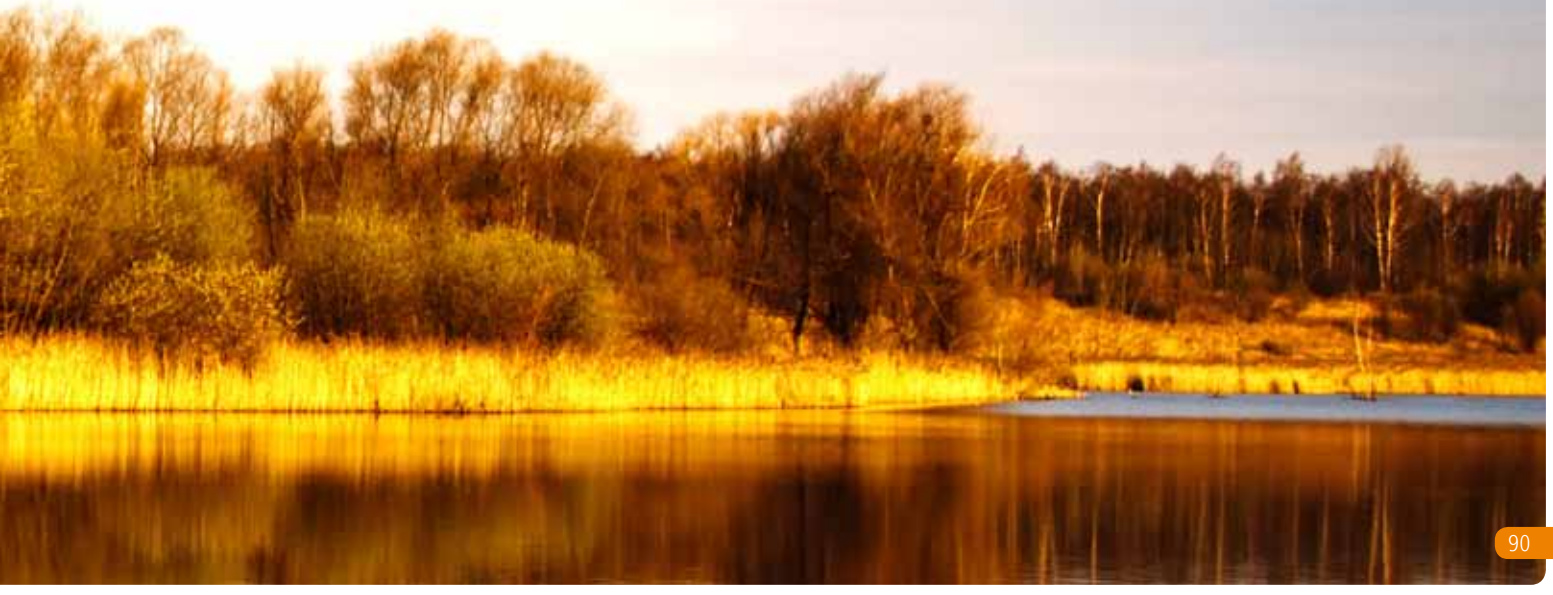
MAN High Bandwidth and Large-Capacity Table Entries Solution: High Network Performance



In order to accommodate the requirements for MAN development, Huawei has put forth a network solution featuring high bandwidth and large capacities of entries using S12700 series agile switches to help customers build high-performance and evolvable MAN networks.

The core layer uses 100 Gbit/s bandwidth for across-node interconnections. Using core router platform technologies, the S12700 agile series switches have 3M FIB entries, satisfying the performance requirements of the Internet and provincial backbone network route importing. The aggregation layer uses 40 Gbit/s uplink bandwidth and 10 Gbit/s downlink bandwidth for networking. Each node has 256K ARP entries and 1M MAC address entries, satisfying large-scale Layer 2 and Layer 3 networking requirements. In addition, each node has 256K ACL rules, and therefore can perform fine-grained control of MAN network traffic.

The S12700-based MAN solution uses a pure switch networking architecture, greatly reducing customer investment costs. Additionally, the S12700's features of high bandwidth and large capacities of entries meet requirements for large-scale MAN applications and non-blocking network construction, protecting customers' existing investments over a long period of time. Huawei S12700 series agile switches have full programmability, and therefore can assist customers in building future-proof, infinitely evolvable Software-Defined Networking (SDN) MAN networks.



Huawei Wireless Medical Network Solution

Why We Need Medical Informatization

Medical Accidents

Efficiency and Service

Information Leakage

In the US, 100,000 people die on a yearly basis due to medical accidents, among which 68% can be prevented through medical informatization.

Doctors need to obtain the complete medical history of a patient for a proper treatment.

Patients need more humanized and varied medical services and have the right to know their conditions.

In 2009 in Tennessee America, the leakage of medical data involved 1 million people and result in US$25 million loss. In 2012 in a city of China, information of 140,000 newborns was leaked.

Trends of Medical Industry

Informatization

Registration fee room, pharmacies, doctor workstations, PACS, EMR, and ICT infrastructure...

Digital Hospital

Medical Informatization

Collaboration and sharing between medical institutions

Health records, collaboration between medical and public health institutions, medical emergency response, and remote healthcare...

Health Management

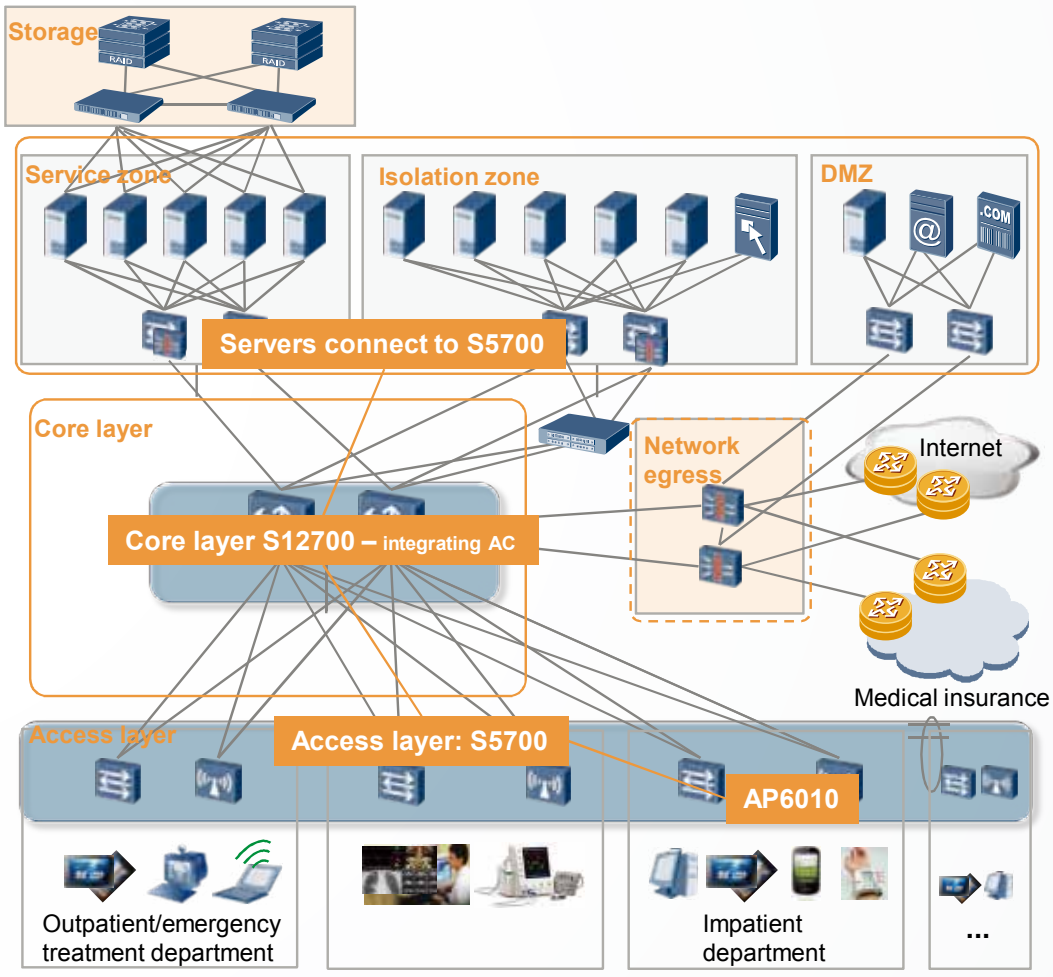
Personalized health services

From treatment to prevention: personal health management and first aid.

Traditionally, doctors must prepare patient medical records and charts for conducting rounds, with nurses manually noting down doctors' orders. This is inefficient, and leaves room for transcription errors and a delay in patient information being documented, all of which increase the risk of medical errors.

Hospitals urgently need the capability to support mobile rounds so that doctors can have full access to patient records to properly diagnose and treat patients. Nurses can be freed from tedious paper work. Mobile rounds will improve hospital efficiency and service quality.

Huawei Wireless Medical Network Architecture



Network security

- Access control for different security zones
- Anti-attack mechanisms against malicious codes on key edge nodes

Intrusion detection

- Multiple intrusion detection mechanisms detect attack traffic and improve system security

Host security

- Monitor intranet users when they access the Internet.
- Deploy terminal security protection.

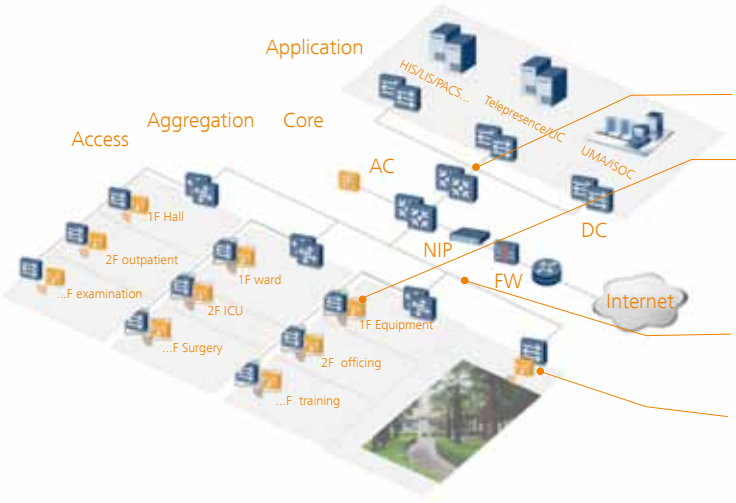
Application security

- Ensure core service security and provide application-level protection for key services.
- Audit users' online behaviors and operations concerning databases.

Management requirement

- Conduct periodical vulnerability scanning and bug fixing.
- Report detected or potential security vulnerabilities.

Huawei Wireless Medical Network Solution



How to ensure network reliability, especially for the wireless network.

Huawei CSS: 10 ms convergence rate. 99.999% reliability of a single device. VRRP/RSTP and other features ensure network reliability.

Exclusive wireless stabilization technology: Patented baseband interference isolation, automatic channels, and power adjustment ensure a stable wireless network.

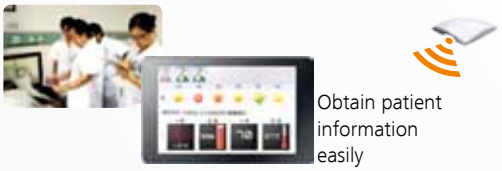
How to support high-speed wireless access to PACS.

Cluster + line-speed forwarding: Full line-speed GE/10GE forwarding and 100% link utilization . The bandwidth of Huawei CSS is four times the industry average.

No.1 wireless coverage area and throughput: Industry-leading single-band 450 Mbps/dual-band 900 Mbps bandwidth increases the coverage area by 30% and the throughput by 20%.

Quality Services: Wireless Ward Round and Healthcare

Solution 1: Wireless ward round



Obtain patient information easily

Medical record query
Enter/change doctor advice

Next...

Tablets help facilitate the work.

Solution 2: Bed nursing

or

Cart + mini computers + wireless card + battery

Car + Tablet

Patient condition check/doctor advice
Record/implement the advice
Healthcare knowledge teaching

Next...

Carts carrying healthcare equipment and tablets help realize mobile healthcare.

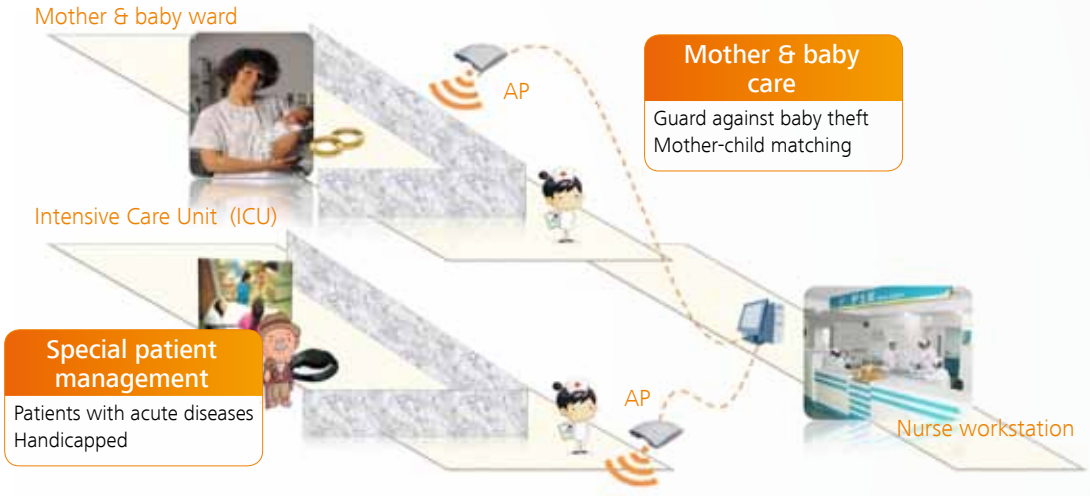
The wireless network could improve doctors' work efficiency and reduce their errors in giving advice after warding round.

The doctors could obtain any patient's information easily through wireless network services.

They could query medical records of any patient which was recorded by the former doctors.

They could input or change their advice conveniently for sharing with other doctors

Patient Management: Wireless Location



How to prevent mistakes in baby taking and even baby theft?

Wrist straps sound the alarm when mothers and babies are mismatched.

The wrist strap can locate the wearer. Attempts to remove the wrist strap or move out of a particular area will sound the alarm. .

How to quickly locate special patients?

The WLAN chip in the wrist strap implements wearer location within 3 meters.

Values of Wireless Medical Network Solution

Hospital: Easy to work, to serve the community

- Interior processes improved
- Information becomes sharable and easy access
- Improve service quality and strengthen reputation
- Operating cost lowered

People: Enjoy high-quality medical service

- Time spent on waiting is shortened
- Timely medical care and more precise diagnosis
- Convienience in medical care
- Medical cost is lowered and becomes more transparent

Hospital Managers: Grasp the overall situation and timely response

- Better understanding of healthcare resources
- Correct decision-making and efficient policies
- Full control of hospital's revenue and expenditure

5

Huawei S12700 Series Agile Switches Datasheet

S12700 Series Agile Switches

Huawei S12700 series agile switches are designed for next-generation campus networks. Using a fully programmable switching architecture, the S12700 series allows fast, flexible function customization and supports a smooth evolution to Software-Defined Networking (SDN). The S12700 series uses a Huawei Ethernet Network Processor (ENP) and provides a native Wireless Access Controller (AC) to help build a wired and wireless converged network. Its Unified User Management capabilities deliver unified user and service management, and Huawei's Packet Conservation Algorithm for Internet (iPCA) supports hop-by-hop monitoring of any service flows, helping manage services in a more refined way. The S12700 series runs the Huawei Versatile Routing Platform (VRP), which provides high-performance L2/L3 switching services and rich network services, such as Multiprotocoal Label Switching (MPLS) VPN, hardware IPv6, desktop cloud, and video conferencing. In addition, the S12700 series offers a variety of reliability technologies, including in-service software upgrade, non-stop forwarding, Cluster Switch System Generation2(CSS2), a switch fabric hardware clustering system that allows 1+N backup of Main Processing Units (MPUs), hardware Eth-OAM/BFD, and ring network protection. These technologies help improve productivity and maximize network operation time, reducing Total Cost of Ownership (TCO).

The S12700 series is available in two models: S12708 and S12712.

S12712

S12708

Product Characteristics

Make your network more agile and service-oriented

- The high-speed ENP chip used in the S12700 series is tailored for Ethernet. The chip's flexible packet processing and traffic control capabilities can meet current and future service requirements, helping build a highly scalable network.
- In addition to providing all the capabilities of common switches, the S12700 series provides fully programmable open interfaces and supports programmable forwarding behaviors. Enterprises can use the open interfaces to develop new protocols and functions independently, or jointly with other vendors, to build campus networks that meet their needs.
- The ENP chip uses a fully programmable architecture, on which enterprises can define their own forwarding models, forwarding behaviors, and lookup algorithms. This architecture speeds service innovation and enables the provisioning of a customized service within six months, without replacing hardware. In contrast, traditional Application Specific Integrated Circuit (ASIC) chips use a fixed forwarding architecture and follow a fixed forwarding process. For this reason, new services cannot be provisioned until new hardware is developed to support the services, which can take one to three years.
- Supports Protocol Oblivious Forwarding (POF), which allows multi-stage network deployment and fast service provisioning.

Deliver abundant services more agilely

- The S12700 series' native ACs allow enterprises to build a wireless network without additional AC hardware. Each S12700 switch can manage 4,000 APs and 64,000 users. It is the first core switch that provides T-bit AC capabilities, avoiding the performance bottleneck on independent AC devices. The native T-bit AC capabilities help organizations better cope with challenges in the high-speed wireless era.
- The S12700 series' unified user management function authenticates both wired and wireless users, ensuring a consistent user experience no matter whether they are connected to the network through wired or wireless access devices. The unified user management function supports various authentication methods, including PPPoE, 802.1X, MAC, and Portal authentication, and is capable of managing users based on user groups, domains, and time ranges. These functions visualize user and service management and enable the transformation from device-centered management to user-centered management.

Provide more agile fine granular management

- iPCA, Packet Conservation Algorithm for Internet, changes the traditional method of using simulated traffic for fault location. iPCA technology can monitor network quality for any service flow at any network node, at any time, and without extra costs. It can detect temporary service interruptions within one second and can identify faulty ports accurately. This cutting-edge fault detection technology turns "extensive management" into "fine granular management."
- Super Virtual Fabric (SVF) technology can not only virtualize fixed-configuration switches into S12700 switch line cards but also virtualize APs as switch ports. With this virtualization technology, a physical network with core/aggregation switches, access switches, and APs can be virtualized into a "super switch," offering the simplest network management solution.
- The S12700 series manages access switches similar to the way an AC manages APs, saving the laborious configuration on access switches. It manages access switches and APs uniformly through CAPWAP tunnels, allowing access switches and APs to connect to the network with zero configuration.

Industry-leading line cards

- Using Huawei's advanced ENP chips, the S12700 series supports several million hardware entries, leaving traditional switches far behind. The S12700 series provides 1M MAC address entries and 3M Forwarding Information Base (FIB) entries, meeting requirements of route-intensive scenarios, such as the Metropolitan Area Network (MAN) for a television broadcasting or education network. Providing 1M NetStream entries enables fine granular traffic statistics for college campus networks and large-scale enterprise campus networks.
- The S12700 series provides a 1.5 GB buffer on each line card to prevent packet loss upon traffic bursts, delivering high-quality video services. Traditional switches only provide 4 MB buffer per card, which cannot ensure high-quality video stream transmission.
- The S12700 series supports high-density line-speed cards, such as 48 x 10 GE and 8 x 100 GE line cards. Each S12700 chassis can provide a maximum of 576 x 10 GE ports and 96 x 100 GE ports. This large port capacity fully meets the requirements of bandwidth-consuming applications, such as multimedia video conferencing, protecting customer investments.

End-to-end reliability design

Device-level reliability: CSS2 switch fabric hardware clustering technology

- Based on back-to-back clustering technology, widely used on high-end core routers, the S12700 series employs second-generation switching fabric hardware clustering technology, CSS2, an enhancement to CSS switching fabric clustering technology.
- CSS2 technology connects cluster member switches through switch fabric unit hardware channels; therefore, cluster control and data packets need only be forwarded once by the switch fabric units and do not go through service cards. Compared with traditional service port clustering technologies, CSS2 minimizes the impact of software failures, reduces service interruption risks caused by service cards, and also significantly shortens transmission latency.
- CSS2 supports 1+N backup of MPUs. This means a cluster can run stably as long as one MPU of any chassis in the cluster is working normally. In a cluster connected by service ports, each chassis must have at least one MPU working normally; therefore, CSS2 is more reliable than traditional service port clustering technologies.
- CSS2 prevents a cluster from splitting. Cluster control and data packets are transmitted over independent channels. Even if all links between switch fabric units fail, the cluster will not split because these packets can still be transmitted over the control channels between MPUs. In a cluster connected by service ports, control packets and data packets are forwarded through links between service cards. Once a link between member devices fails, control packets and data packets will be lost, causing the cluster to split.

Network-level reliability: End-to-end hardware protection switching

- The S12700 uses a series of link detection and protection switching technologies, such as hardware Eth-OAM, BFD, G.8032, and Smart Ethernet Protection (SEP), to realize 50 ms end-to-end protection switching. These technologies help build a campus network that responds quickly to topology changes and provides the most reliable services.

Product Specifications

Item	S12708	S12712
Switching capacity	12.32/27.04 Tbit/s	17.44/37.28 Tbit/s
Packet forwarding rate	6,240 /9,120 Mpps	9,120/12,960 Mpps
MPU slots	2	2
SFU slots	4	4
Service card slots	8	12
Redundancy design	MPUs, SFUs, power supplies, and fan modules	
CSS2	1+N backup of MPUs in a cluster	
	Up to 1.92 Tbit/s cluster bandwidth, 21 us inter-chassis transmission latency	
Wireless network management	Native AC	
	AP access control, AP region management, and AP profile management	
	Radio profile management, uniform static configuration, and centralized dynamic management	
	Basic WLAN services, QoS, security, and user management	
	Deployment of ACs on different network layers	
User management	unified user management	
	PPPoE, 802.1X, MAC, and Portal authentication	
	Traffic- and time-based accounting	
	User authorization based on user groups, domains, and time ranges	
VLAN	LNP, access, trunk, and hybrid interface type	
	Default VLAN	
	VLAN switching	
	QinQ and selective QinQ	
	MAC address-based VLAN assignment	
ARP	256K ARP entries	

Item	S12708	S12712
MAC address	1M MAC address entries	
	Dynamic MAC address learning and aging	
	Static, dynamic, and blackhole MAC address entries	
	Source MAC address filtering	
	MAC address limiting based on ports and VLANs	
Ring network protection	Spanning Tree Protocol (STP) (IEEE 802.1d), RSTP (IEEE 802.1w), and MSTP (IEEE 802.1s)	
	SEP	
	Bridge Protocol Data Unit (BPDU), root protection, and loop protection	
	BPDU tunnel	
	G.8032 Ethernet Ring Protection Switching (ERPS)	
IP routing	3M IPv4 routing entries	
	1M IPv6 routing entries	
	IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP	
	IPv6 routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+	
Multicast	128,000 multicast routing entries	
	IGMPv1/v2/v3 and IGMP v1/v2/v3 snooping	
	PIM-DM, PIM-SM, and PIM-SSM	
	Multicast Source Discovery Protocol (MSDP) and Multiprotocol Extensions for BGP (MBGP)	
	Fast leave	
	Multicast traffic control	
	Multicast querier	
	Multicast protocol packet suppression	
	Multicast Call Admission Control (CAC)	
	Multicast ACL	

Item	S12708	S12712
MPLS	Basic MPLS functions	
	MPLS Operations, Administration, and Maintenance (OAM)	
	MPLS Traffic Engineering (TE)	
	MPLS VPN/VLL/VPLS	
Reliability	Link Aggregation Control Protocol (LACP) and E-Trunk	
	Virtual Router Redundancy Protocol (VRRP) and Bidirectional Forwarding Detection (BFD) for VRRP	
	BFD for BGP/IS-IS/OSPF/static route	
	Non-Stop Forwarding (NSF) and Graceful Restart (GR) for BGP/IS-IS/OSPF/LDP	
	TE Fast ReRoute (FRR) and IP FRR	
	Eth-OAM 802.3ah and 802.1ag (hardware)	
	ITU-Y.1731	
	Device Link Detection Protocol (DLDP)	
	In-Service Software Upgrade (ISSU)	
QoS	256,000 ACLs	
	Traffic classification based on Layer 2 headers, Layer 3 protocols, Layer 4 protocols, and 802.1p priority	
	ACLs and actions such as Committed Access Rate (CAR), re-marking, and scheduling	
	Queuing algorithms, such as SP, WRR, DRR, SP + WRR, and SP + DRR	
	Congestion avoidance mechanisms, including (WRED) and tail drop	
	5-level H-QoS	
	Traffic shaping	
Configuration and maintenance	Terminal access services such as console port login, Telnet, and SSH	
	Network management protocols, such as SNMPv1/v2/v3	
	File uploading and downloading through FTP and TFTP	
	BootROM upgrade and remote in-service upgrade	
	Hot patches	
	User operation logs	

Item	S12708	S12712
Security and management	MAC address, Portal, 802.1x, and Dynamic Host Configuration Protocol (DHCP) snooping triggered authentication	
	RADIUS and HWTACACS authentication for login users	
	Command line authority control based on user levels, preventing unauthorized users from using command configurations	
	Defense against DoS attacks, Transmission Control Protocol (TCP) SYN Flood attacks, User Datagram Protocol (UDP) Flood attacks, broadcast storms, and heavy traffic attacks	
	1K CPU hardware queues for hierarchical scheduling and protection of protocol packets on the control plane	
	Remote Network Monitoring (RMON)	
Value-added services	Firewall	
	Network Address Translation (NAT)	
	IPSec	
	Intrusion Protection System (IPS)	
	Load balancing Analog Digital Conversion (ADC)	
Buffer capacity	1.5 GB per card	
Energy saving	Energy Efficient Ethernet (802.3az)	
Dimensions (H x W x D in mm)	663.95 x 442 x 489, 15U	832.75 x 442 x 489, 19U
Weight (empty chassis)	19.8 kg	38.45 kg
Operating voltage	DC: –38.4V to –72V AC: 90V to 290V	
Total power capacity	6,600W	6,600W

Ordering Information

S12700 basic configuration	
LE2BN66ED000	N66E DC assembly rack (eight 60A outputs, maximum 2,200W per output, 600 x 600 x 2,200 mm)
LE2BN66EA000	N66E AC assembly rack (four 16A outputs, maximum 2,500W per output, 600 x 600 x 2,200 mm)
ET1BS12708S0	S12708 assembly chassis
ET1BS12712S0	S12712 assembly chassis
Monitoring unit	
EH1D200CMU00	Centralized monitoring unit
Main processing unit	
ET1D2MPUA000	S12700 main control unit A, optional clock
Switch fabric unit	
ET1D2SFUA000	S12700 switch fabric unit A
ET1D2SFUC000	S12700 switch fabric unit C
ET1D2SFUD000	S12700 switch fabric unit D
100M/1000M Ethernet electrical interface cards	
ET1D2G48TEA0	48-port 10/100/1000 BASE-T interface card (EA, RJ45)
ET1D2G48TEC0	48-port 10/100/1000 BASE-T interface card (EC, RJ45)
ET1D2G48TX1E	48-port 10/100/1000 BASE-T interface card (X1E, RJ45)*
100M/1000M Ethernet optical interface cards	
ET1D2G24SEC0	24-port 100/1000 BASE-X interface card (EC, SFP)
ET1D2G48SEA0	48-port 100/1000 BASE-X interface card (EA, SFP)
ET1D2G48SEC0	48-port 100/1000 BASE-X interface card (EC, SFP)
ET1D2G48SX1E	48-port 100/1000 BASE-X interface card (X1E, SFP)
100M/1000M Ethernet electrical and optical interface cards	
ET1D2T36SEA0	36-port 10/100/1000 BASE-T and 12-port 100/1000 BASE-X interface card (EA, RJ45/SFP)

S12700 basic configuration	
10 GE optical interface cards	
ET1D2X04XEA0	4-port 10G BASE-X interface card (EA, XFP)
ET1D2X04XEC1	4-port 10G BASE-X interface card (EC, XFP)
ET1D2S04SX1E	4-port 10G BASE-X and 24-port 100/1000 BASE-X and 8-port 10/100/1000 BASE-T combo interface card (X1E, RJ45/SFP/SFP+)
ET1D2S08SX1E	8-port 10G BASE-X and 8-port 100/1000 BASE-X and 8-port 10/100/1000 BASE-T combo interface card (X1E, RJ45/SFP/SFP+)
ET1D2X12SSA0	12-port 10G BASE-X interface card (SA, SFP+)
ET1D2X16SSC0	16-port 10G BASE-X interface card (SC, SFP+)
ET1D2X48SEC0	48-port 10G BASE-X interface card (EC, SFP+)
40 GE optical interface cards	
ET1D2L02QSC0	2-port 40G BASE-X interface card (SC, QSFP+)
ET1D2L08QSC0	8-port 40G BASE-X interface card (SC, QSFP+)
Cluster service subcard	
EH1D2VS08000	8-port 10G cluster switching system service unit (SFP+)
Service processing cards	
EH1D2PS00P00	Open Service Platform (OSP) card**
ET1D2FW00S00	Firewall service card - 10G
ET1D2FW00S01	Firewall service card - 20G
ET1D2FW00S02	Firewall service card - 40G
ET1D2IPS0S00	IPS service card
ACU2	WLAN ACU2 wireless access controller card***
Optical transceivers	
FE-SFP optical transceiver	
S-SFP-FE-LH40-SM1310	Optical transceiver, eSFP, FE, single-mode module (1,310 nm, 40 km, LC)
S-SFP-FE-LH80-SM1550	Optical transceiver, eSFP, FE, single-mode module (1,550 nm, 80 km, LC)

S12700 basic configuration	
GE-SFP optical transceiver	
SFP-1000BaseT	Copper transceiver, SFP, GE, electrical interface module (100m, RJ45)
eSFP-GE-SX-MM850	Optical transceiver, eSFP, GE, multimode module (850 nm, 0.5 km, LC)
SFP-GE-LX-SM1310	Optical transceiver, SFP, GE, single-mode module (1,310 nm,10 km, LC)
S-SFP-GE-LH40-SM1310	Optical transceiver, eSFP, GE, single-mode module (1,310 nm, 40 km, LC)
S-SFP-GE-LH40-SM1550	Optical transceiver, eSFP, GE, single-mode module (1,550 nm, 40 km, LC)
S-SFP-GE-LH80-SM1550	Optical transceiver, eSFP, GE, single-mode module (1,550 nm, 80 km, LC)
eSFP-GE-ZX100-SM1550	Optical transceiver, eSFP, GE, single-mode module (1,550 nm,100 km, LC)
10 GE-XFP Optical transceiver	
XFP-SX-MM850	Optical transceiver, XFP, 10G, multimode module (850 nm, 0.3 km, LC)
XFP-STM64-LX-SM1310	Optical transceiver, XFP, 10G, single-mode module (1,310 nm, 10 km, LC)
XFP-STM64-LH40-SM1550	Optical transceiver, XFP, 10G, single-mode module (1,550 nm, 40 km, LC)
XFP-STM64-SM1550-80 km	Optical transceiver, XFP, 10G, single-mode module (1,550 nm, 80 km, LC)
10 GE-SFP+ Optical transceiver	
OMXD30000	Optical transceiver, SFP+, 10G, multimode module (850 nm, 0.3 km, LC)
OSX010000	Optical transceiver, SFP+, 10G, single-mode module (1,310 nm,10 km, LC)
OSX040N01	Optical transceiver, SFP+, 10G, single-mode module (1,550 nm, 40 km, LC)
OSXD22N00	Optical transceiver, SFP+, 10G, single-mode module (1,310 nm, 0.22km, LC,LRM)
LE2MXSC80FF0	Optical transceiver, SFP+, 10G, single-mode module (1,550 nm, 80 km, LC) (only for 8-port 10G BASE interface cards)
SFP-10G-USR	Optical transceiver, SFP+, 10G, multimode module (850 nm, 0.1 km, LC)
SFP-10G-ZR	Optical transceiver, SFP+, 10G, single-mode module (1,550 nm, 80 km, LC)
SFP-10G-AOC3M	AOC optical transceiver, SFP+, 850 nm, 1G to 10G, 0.003 km

S12700 basic configuration	
SFP-10G-AOC10M	AOC optical transceiver, SFP+, 850 nm, 1G to 10G, 0.01 km
SFP-10G-BXU1	10G Base, Bi-Directional (BIDI) optical transceiver, SFP, 10G, single-mode module (TX1270 nm/RX1330 nm, 10 km, LC)
SFP-10G-BXD1	10G Base, BIDI optical transceiver, SFP, 10G, single-mode module (TX1330 nm/RX1270 nm, 10 km, LC)
SFP-10G-ZCW1511	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,511 nm, 70 km, LC)
SFP-10G-ZCW1471	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,471 nm, 70 km, LC)
SFP-10G-ZCW1491	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,491 nm, 70 km, LC)
SFP-10G-ZCW1531	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,531 nm, 70 km, LC)
SFP-10G-ZCW1551	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,551 nm, 70 km, LC)
SFP-10G-ZCW1571	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,571 nm, 70 km, LC)
SFP-10G-ZCW1591	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,591 nm, 70 km, LC)
SFP-10G-ZCW1611	Optical transceiver, SFP+, 10G, single-mode module (CWDM, 1,611 nm, 70 km, LC)
40 GE-QSFP optical transceivers	
QSFP-40G-SR4	Optical transceiver, Quad Small Form-Factor Pluggable (QSFP), 40G, multimode module (850 nm, 0.15 km, MPO) (connecting to one QSFP+ optical transceiver)
QSFP-40G-iSR4	Optical transceiver, QSFP, 40G, multimode module (850 nm, 0.15 km, MPO) (connecting to four SFP+ optical transceivers)
QSFP-40G-LR4	40G Base-LR4 optical transceiver, QSFP+, 40G, single-mode module (1,310 nm, 10 km, LC)
QSFP-40G-eiSR4	40G Base-SR4 Optical transceiver, QSFP+, 40G, multimode module (850 nm, 0.3 km, MPO) (connecting to four SFP+ optical transceivers)
BIDI-SFP optical transceivers	
SFP-FE-LX-SM1310-BIDI	Optical transceiver, eSFP, FE, BIDI single-mode module (TX1310/RX1550, 15 km, LC)
SFP-FE-LX-SM1550-BIDI	Optical transceiver, eSFP, FE, BIDI single-mode module (TX1550/RX1310, 15 km, LC)
SFP-GE-LX-SM1310-BIDI	Optical transceiver, eSFP, GE, BIDI single-mode module (TX1310/RX1490,10 km, LC)
SFP-GE-LX-SM1490-BIDI	Optical transceiver, eSFP, GE, BIDI single-mode module (TX1490/RX1310,10 km, LC)

S12700 basic configuration	
LE2MGSC40ED0	Optical transceiver, SFP, GE, BIDI single-mode module (TX1490/RX1310, 40 km, LC)
LE2MGSC40DE0	Optical transceiver, SFP, GE, BIDI single-mode module (TX1310/RX1490, 40 km, LC)
SFP-GE-LX	1000Base-BIDI optical transceiver, SFP, GE, single-mode module (TX1490 nm/ RX1310 nm,10 km, LX)
Power modules	
PAC-2200WF	2,200W AC power module F (black)
PDC-2200WF	2,200W DC power module F (black)
Software	
ET1SBSM25000	S12700 V200R005C00 software
Documentation	
ET1IV2R5C0C0	S12700 Series Agile Switches Product Documentation (Chinese)
ET1IV2R5C0E0	S12700 Series Agile Switches Product Documentation (English)

* The X1E series cards use ENP chips and provide native AC and unified user management functions.

** The OSP card supports CheckPoint IPS and F5 ADC load balancer, and can run Windows, SUSE, and VMware operating systems.

***: Each ACU2 card can manage 2K APs. An S12708 switch can have a maximum of 7 ACU2 cards installed and can manage up to 14K APs. An S12712 switch can have a maximum of 11 ACU2 cards installed and can manage up to 22K APs.

In an enterprise campus network

S12700 series switches are deployed on the core layer of an enterprise campus network. Native ACs provided by the S12700 enable customers to build wireless networks without additional AC hardware, reducing network construction costs. The S12700 is the first core switch that provides T-bit AC capabilities, avoiding the performance bottleneck on independent ACs. The native T-bit AC capabilities help customers migrate their wireless networks to 802.11ac. The S12700 series realizes wired and wireless convergence and delivers consistent experience to wired and wireless users through uniform device, user, and service management.

In a college campus network

S12700 series switches are deployed on the core layer of a college campus network. The unified user management function on the S12700 reduces network construction costs by removing the need to purchase new BRAS hardware. Each S12700 switch supports 64,000 users, allowing a large number of concurrent access users. Its five-level H-QoS feature implements fine granular user and service management. The S12700 series realizes wired and wireless convergence and delivers consistent experience to wired and wireless users through uniform device, user, and service management.

In a bearer network for video conferencing, desktop cloud, and video surveillance applications

The 1.5 GB buffer prevents packet loss upon traffic bursts, delivering high-quality video streams. The S12700 series supports up to 1M MAC address entries and 3M FIB entries, which allow access from a large number of terminals and help evolution to IPv6 and the Internet of Things (IoT). Employing end-to-end hardware reliability technologies and iPCA technology, the S12700 series offers a highly reliable, high-quality, scalable video conferencing and surveillance solution.

On the core/aggregation layer of a MAN

S12700 series switches are used as core or aggregation switches on the Metropolitan Area Network (MAN) of a television broadcasting or education network. The 3M FIB entries provided are sufficient for large-scale routing on the MAN. CSS2 switch fabric hardware clustering technology, originating from clustering technology for high-end core routers, delivers carrier-class reliability on the MAN. Additionally, the S12700 series supports comprehensive L2/L3 MPLS VPN features, providing a highly reliable, secure, and scalable metropolitan bearer network solution.

In an enterprise data center

S12700 series switches are deployed on the core or aggregation layer of an enterprise data center network. The S12700 series has high-density line cards, such as 8 x 100 GE and 48 x 10 GE cards, meeting the requirements for large data throughput on data center core/aggregation nodes. Using CSS2 switch fabric hardware clustering technology, the S12700 series provides up to 1.92 Tbit/s cluster bandwidth and shortens the inter-chassis forwarding latency to 21 μs. This technology helps customers build a high performance, high reliability, and low latency data center network.

Huawei Enterprise Network Sx7 Series Switches Family

S12700 Series Agile Switches: Flagship Products

- Supports Cluster Switch System 2 (CSS2) switch fabric clustering, 1+N backup of Main Control Units in the cluster
- Supports native Access Controller (AC) and Unified User Management
- Supports 1.5 GB buffer, 3 M Forwarding Information Base (FIB) entries, and 1 M Media Access Control (MAC) address entries on the service board
- Hardware-based Ethernet Operations, Administration, and Maintenance (OAM) and Bidirectional Forwarding Detection (BFD)
- Maximum 576 x 10 GE ports, 96 x 40 GE ports, or 96 x 100 GE ports on en equipment

S12708

- Total 14 slots; 8 service slots
- Dual Main Control Units (MCUs) and four independent switch fabric units
- Switching capacity: 12.32 Tbit/s/27.04 Tbit/s
- Forwarding performance: 6,240 Mpps/9,120 Mpps

S12712

- Total 18 slots; 12 service slots
- Dual MCUs and four independent switch fabric units
- Switching capacity: 17.44 Tbit/s/37.28 Tbit/s
- Forwarding performance: 9,120 Mpps/12,960 Mpps


S9700 Series Terabit Core Routing Switches

S9703

- Total 5 slots; 3 service slots
- Dual MCUs and M+N backup of power modules
- Switching capacity: 2.88 Tbit/s/5.76 Tbit/s
- Forwarding performance: 2,160 Mpps

S9706

- Total 8 slots; 6 service slots
- Dual MCUs and M+N backup of power modules
- Switching capacity: 6.72 Tbit/s/14.72 Tbit/s
- Forwarding performance: 2,880 Mpps/5,040 Mpps


S6700 Series 10 GE L3 Box Switches

- Intelligent stacking (iStack)
- GE/10 GE auto-sensing
- MPLS L2VPN and L3VPN
- Easy Operation

S6700-24-EI

- 24 x 10 GE Small Form-Factor Pluggable (SFP)+
- Pluggable dual power modules, supporting AC/DC
- One USB port
- Switching capacity: 480 Gbit/s
- Forwarding performance: 358 Mpps

S6700-48-EI

- 48 x 10 GE SFP+
- Pluggable dual power modules, supporting AC/DC
- One USB port
- Switching capacity: 960 Gbit/s
- Forwarding performance: 715 Mpps


S5700 Series Advanced GE L3 Box Switches

S5710-108C-PWR-HI

- 2U high, 48 x GE RJ45, 8 x 10 GE SFP+
- Pluggable dual power modules and PoE+ support
- Four extension slots available for 16 x GE RJ45, 16 x GE SFP, 4 x 10 GE SFP+, or 4 x 40 GE QSFP+ module

S5700-28C-HI

- 24 x GE RJ45
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module



S5700EI Series Enhanced GE Switches

- Abundant routing protocols, such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS)
- Intelligent stacking (iStack)
- Ring network protection protocols SEP and G.8032, implementing protection switchover within 50 ms
- Easy Operation

S5700-28C-EI
S5700-28C-PWR-EI

- 24 x GE RJ45
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module

S5700-52C-EI
S5700-52C-PWR-EI

- 48 x GE RJ45
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module

S5700-28C-EI-24S

- 24 x GE SFP, 4 x GE RJ45 Combo
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module





S5700-LI Series GE Access Switches

S5700-28X-LI-AC
S5700-28X-LI-DC
S5700-28X-PWR-LI-AC

- 24 x GE RJ45, 4 x 10 GE SFP+
- AC or DC power supply
- RPS

S5700-52X-LI-AC
S5700-52X-LI-DC
S5700-52X-PWR-LI-AC

- 48 x GE RJ45, 4 x 10 GE SFP+
- AC or DC power supply
- RPS

S5700-28X-LI-24S-AC
S5700-28X-LI-24S-DC

- 24 x GE SFP, 4 x GE RJ45 Combo, 4 x 10 GE SFP+
- AC or DC power supply
- RPS

S5700-10P-LI-AC
S5700-10P-LI-PWR-AC

- 8 x GE RJ45, 2 x GE SFP
- AC power supply
- RPS

S5700-28P-LI-AC
S5700-28P-LI-DC
S5700-28P-LI-PWR-AC

- 24 x GE RJ45, 4 x GE SFP
- AC or DC power supply
- RPS

S7700 Series Intelligent Routing Switches

S9712

- Total 14 slots; 12 service slots
- Dual MCUs and M+N backup of power modules
- Switching capacity: 8.64 Tbit/s/18.56 Tbit/s
- Forwarding performance: 3,840 Mpps/6,480 Mpps

S7703

- Total 5 slots; 3 service slots
- Dual MCUs, power module backup, and Power over Ethernet (PoE)+ support
- Switching capacity: 1.92 Tbit/s
- Forwarding performance: 576 Mpps/1,440 Mpps

S7706

- Total 8 slots; 6 service slots
- Dual MCUs, power module backup, and PoE+ support
- Switching capacity: 3.84 Tbit/s/5.12 Tbit/s
- Forwarding performance: 1,152 Mpps/2,880 Mpps

S7712

- Total 14 slots; 12 service slots
- Dual MCUs, power module backup, and PoE+ support
- Switching capacity: 3.84 Tbit/s/5.12 Tbit/s
- Forwarding performance: 1,344 Mpps/3,360 Mpps

- CSS switch fabric and service port clustering
- Multi-protocol Label Switching (MPLS) L2VPN and L3VPN
- Hardware-based Ethernet OAM and BFD
- Easy Operation

S5700-28C-HI-24S

- 24 x GE SFP
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module

S5710-28C-EI
S5710-28C-PWR-EI

- 24 x GE RJ45, 4 x GE SFP Combo, 4 x 10 GE SFP+
- Pluggable dual power modules and PoE+ support
- Two extension slots available for 8 x GE RJ45, 8 x GE SFP, or 2 x 10 GE SFP+ module

S5710-52C-EI
S5710-52C-PWR-EI

- 48 x GE RJ45, 4 x 10 GE SFP+
- Pluggable dual power modules and PoE+ support
- Two extension slots available for 8 x GE RJ45, 8 x GE SFP, or 2 x 10 GE SFP+ module

- GE/10 GE auto-sensing
- MPLS L2VPN and L3VPN
- NetStream
- Easy Operation

S5700SI Series Standard GE Switches

S5700-24TP-SI-AC
S5700-24TP-SI-DC
S5700-24TP-PWR-SI

- 24 x GE RJ45, 4 x GE SFP Combo
- One USB port
- AC or DC power supply

S5700-48TP-SI-AC
S5700-48TP-SI-DC
S5700-48TP-PWR-SI

- 48 x GE RJ45, 4 x GE SFP Combo
- One USB port
- AC or DC power supply

S5700-28C-SI
S5700-28C-PWR-SI

- 24 x GE RJ45, 4 x GE SFP Combo
- One USB port
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module

S5700-52C-SI
S5700-52C-PWR-SI

- 48 x GE RJ45
- One USB port
- Pluggable dual power modules
- One extension slot available for 4 x GE SFP, 2 x 10 GE SFP+, or 4 x 10 GE SFP+ module

S5700-26X-SI-12S-AC

- 12 x GE RJ45, 12 x GE SFP, 2 x 10 GE SFP+
- One USB port
- AC power supply
- Redundant Power Supply (RPS)

- Intelligent stacking (iStack)
- Ring network protection protocols SEP and G.8032, implementing protection switchover within 50 ms
- Easy Operation

S5700-52P-LI-AC
S5700-52P-LI-DC
S5700-52P-LI-PWR-AC

- 48 x GE RJ45, 4 x GE SFP
- AC or DC power supply
- RPS

S5700S-28P-LI-AC

- 24 x GE RJ45, 4 x GE SFP
- AC power supply
- RPS

S5700S-52P-LI-AC

- 48 x GE RJ45, 4 x GE SFP
- AC power supply
- RPS

S5700-28P-LI-BAT

- 24 x GE RJ45, 4 x GE SFP
- AC and battery power supply
- Visible battery status management

S5700-28P-LI-24S-BAT

- 24 x GE SFP, 4 x GE RJ45 Combo
- AC and battery power supply
- Visible battery status management

- Innovative AHM energy saving
- Ring network protection protocols SEP and G.8032, implementing protection switchover within 50 ms
- sFlow for visible flow management
- Easy Operation
- Miercom certified

Huawei Enterprise Network Sx7 Series Switches Family

S3700EI Series Enhanced 100 M L3 Switches

S3700-28TP-EI-AC S3700-28TP-EI-DC	S3700-28TP-EI-24S-AC	S3700-28TP-EI-MC-AC	S3700-52P-EI-24S-AC	S3700-52P-EI-48S-AC
• 24 x 100 M RJ45, 4 x GE SFP, 2 x GE RJ45 Combo • AC or DC power supply	• 24 x 100 M SFP, 4 x GE SFP, 2 x GE RJ45 Combo • AC power supply	• 24 x 100 M RJ45, 4 x GE SFP, 2 x GE RJ45 Combo • Two monitor ports • AC power supply	• 24 x 100 M RJ45, 24 x 100M SFP, 4 x GE SFP • AC power supply	• 48 x 100 M SFP, 4 x GE SFP • AC power supply

- Abundant routing protocols, such as OSPF, BGP, IS-IS
- Intelligent stacking (iStack)
- Ring network protection protocol SEP, implementing protection switchover within 50 ms
- Automatic configuration

S3700EI Series Enhanced 100 M L3 Switches

S3700-52P-EI-AC S3700-52P-EI-DC	S3700-28TP-PWR-EI	S3700-52P-PWR-EI
• 48 x 100 M RJ45, 4 x GE SFP • AC or DC power supply	• 24 x 100 M RJ45, 4 x GE SFP, 2 x GE RJ45 Combo • Pluggable dual power modules • PoE+ support	• 48 x 100 M RJ45, 4 x GE SFP • Pluggable dual power modules • PoE+ support

S2700EI Series Enhanced 100 M L2 Switches

S2700-9TP-EI-AC S2700-9TP-EI-DC S2700-9TP-PWR-EI	S2700-18TP-EI-AC	S2700-26TP-EI-AC S2700-26TP-EI-DC
• 8 x 100 M RJ45, 1 x GE RJ45, 1 x GE SFP Combo • AC or DC power supply	• 16 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP Combo • AC power supply	• 24 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP Combo • AC or DC power supply

S2700EI Series Enhanced 100 M L2 Switches

S2700-52P-EI-AC	S2700-26TP-PWR-EI	S2750-20TP-PWR-EI-AC	S2750-28TP-EI-AC S2750-28TP-PWR-EI-AC S2751-28TP-PWR-EI-AC
• 48 x 100 M RJ45, 4 x GE SFP • AC power supply	• 24 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP Combo • Pluggable dual power modules • PoE+ support	• 16 x 100 M RJ45, 4 x GE SFP, 2 x GE RJ45 Combo • PoE+ support • AC power supply	• 24 x 100 M RJ45,4 x GE SFP, 2 x GE RJ45 Combo • AC power supply

- Intelligent stacking (iStack)
- 802.1x, Dynamic Host Configuration Protocol (DHCP) Snooping, Dynamic ARP Inspection (DAI), and MAC Force Forwarding (MFF)
- Embedded 6 KV surge protection
- Easy Operation
- Miercom certified

S1700 Series SMB managed Switches

S1700-10GF-2P S1700-10GF-2P-PWR	S1700-28FR-2T2P-AC	S1700-52FR-2T2P-AC	S1700-28GFR-4P-AC	S1700-52GFR-4P-AC	S1700-28FR-2T2P-PWR
• 8 x GE RJ45, 2 x GE SFP • AC power supply	• 24 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP • AC power supply • Standard rack	• 48 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP • AC power supply • Standard rack	• 24 x GE RJ45, 4 x GE SFP • AC power supply • Standard rack	• 48 x GE RJ45, 4 x GE SFP • AC power supply • Standard rack	• 24 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP • PoE+ support • Standard rack

S3700SI Series Standard 100 M L3 Switches

S3700-28TP-SI-AC S3700-28TP-SI-DC	S3700-52P-SI-AC	S3700-28TP-PWR-SI	S3700-52P-PWR-SI
• 24 x 100 M RJ45, 4 x GE SFP, 2 x GE RJ45 Combo • AC or DC power supply	• 48 x 100 M RJ45, 4 x GE SFP • AC power supply	• 24 x 100 M RJ45, 4 x GE SFP, 2 x GE RJ45 Combo • Pluggable dual power modules • PoE+ support	• 48 x 100 M RJ45, 4 x GE SFP • Pluggable dual power modules • PoE+ support

- Intelligent stacking (iStack)
- Ring network protection protocol SEP, implementing protection switchover within 50 ms
- Embedded 6 KV surge protection
- Automatic configuration

S2700SI Series Standard 100 M L2 Switches

S2700-9TP-SI-AC	S2700-18TP-SI-AC	S2700-26TP-SI-AC	S2710-52P-SI-AC	S2710-52P-PWR-SI
• 8 x 100 M RJ45, 1 x GE RJ45, 1 x GE SFP Combo • AC power supply	• 16 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP Combo • AC power supply	• 24 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP Combo • AC power supply	• 48 x 100 M RJ45, 4 x GE SFP • AC power supply	• 48 x 100 M RJ45, 4 x GE SFP • Pluggable dual power modules • PoE+ support

- Automatic configuration
- Embedded 6 KV surge protection
- Fan-free silent design

S1700 Series SMB Unmanaged Switches

S1700-8-AC	S1700-24-AC	S1700-8G-AC	S1700-24G-AC	S1700-24GR-AC	S1700-52R-2T2P-AC
• 8 x 100 M RJ45 • AC power adapter	• 24 x 100 M RJ45 • AC power supply	• 8 x GE RJ45 • AC power adapter	• 24 x GE RJ45 • AC power supply	• 24 x GE RJ45 • AC power supply • Standard rack	• 48 x 100 M RJ45, 2 x GE RJ45, 2 x GE SFP • AC power supply • Standard rack

- One-key operation: press to reboot; press and hold to restore factory settings
- Fan-free silent design
- Energy Efficient Ethernet (EEE)
- Plug-and-play

S1700-28GFR-4P-PWR	S1700-52GFR-4P-PWR	S1728GWR-4P-AC
• 24 x GE RJ45, 4 x GE SFP • PoE+ support • Standard rack	• 48 x GE RJ45, 4 x GE SFP • PoE+ support • Standard rack	• 24 x GE RJ45, 4 x GE SFP • AC power supply • Standard rack

- One-key operation: press to reboot; press and hold to restore factory settings
- 802.1x, ACL, and anti-DDOS features
- Integrated user authentication, security check, and access authorization functions
- Port sleep mode, in accordance with EEE
- Miercom certified

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

www.huawei.com