TEST REPORT
Tolly.

#218122
July 2018
Commissioned by
Huawei Technologies Co., Ltd

Huawei S6720-HI Series Agile 10GbE Switches

Feature Validation and Capacity Evaluation

Executive Summary

Huawei S6720-HI series 10 GbE switches are Huawei-developed fixed agile switches with 10GbE downlink and 40GbE/100GbE uplink ports, that are applicable to enterprise campus, carrier, university, and government networks.

The S6720-HI delivers abundant agility features and uses a fully programmable architecture to implement software-defined functions and on-demand service changes. With services and network convergence as the core, the S6720-HI supports native AC function to manage APs. In addition, the switch provides free mobility features, to ensure consistent user experience, and features Super Virtual Fabric (SVF) to virtualize the entire network into one device.

Tolly engineers verified Huawei's S6720-HI series agile switches in multiple areas including the cloud management, VXLAN, big data security collaboration, secure boot, Open Programmability System (OPS), Super Virtual Fabric (SVF), etc.

The Bottom Line

Huawei S6720-HI Series Agile 10GbE Switches:

1 Support cloud management with the Huawei Agile Controller for configuration, monitoring and inspection

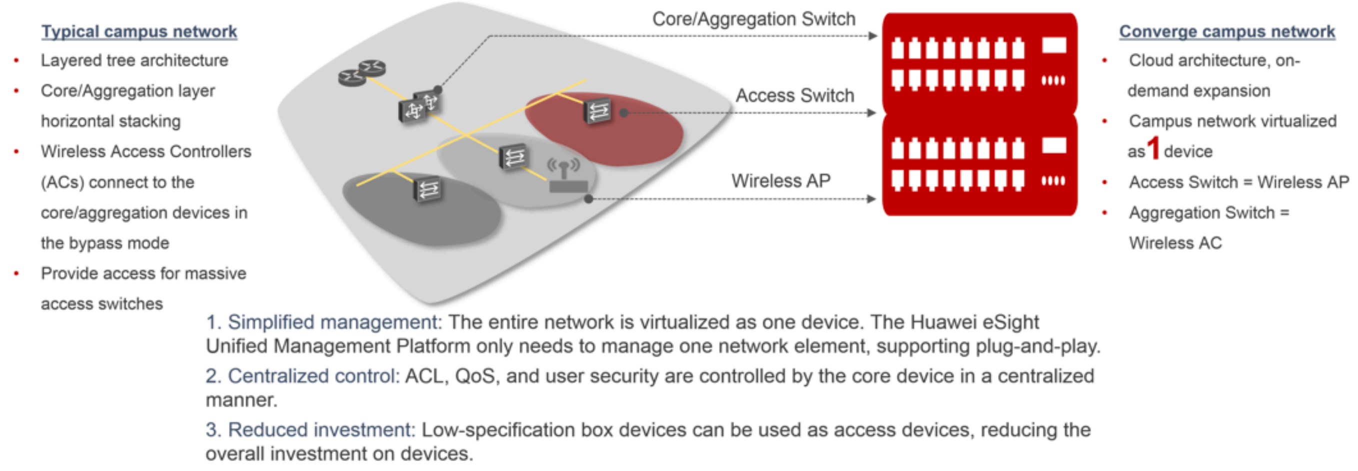
2 Support VXLAN with centralized or distributed gateway deployment modes, dynamic VXLAN tunnel establishment using BGP-EVPN, and NETCONF/YANG based cloud configuration

3 Support big data security collaboration with the NetStream feature to collect network information, the Huawei Cybersecurity Intelligence System (CIS) to run threat analysis, the Agile Controller to deploy policies and the switch to execute

4 Support secure boot with multiple validation features to ensure that the switch can only boot from a legit firmware

5 Support the Open Programmability System (OPS) to run Python scripts for customized O&M functions

Huawei Super Virtual Fabric (SVF) Architecture



Typical campus network
- Layered tree architecture
- Core/Aggregation layer horizontal stacking
- Wireless Access Controllers (ACs) connect to the core/aggregation devices in the bypass mode
- Provide access for massive access switches

Converge campus network
- Cloud architecture, on-demand expansion
- Campus network virtualized as 1 device
- Access Switch = Wireless AP
- Aggregation Switch = Wireless AC

1. Simplified management: The entire network is virtualized as one device. The Huawei eSight Unified Management Platform only needs to manage one network element, supporting plug-and-play.
2. Centralized control: ACL, QoS, and user security are controlled by the core device in a centralized manner.
3. Reduced investment: Low-specification box devices can be used as access devices, reducing the overall investment on devices.

Source: Tolly, April 2018

Figure 1

Test Results

Cloud Management

The Huawei cloud management platform allows users to configure, monitor, and inspect switches from the cloud, reducing on-site deployment and O&M labor costs and decrease network OPEX. Huawei switches support both cloud management using the Huawei Agile Controller and on-premise management modes. These two management modes can be flexibly switched as required to achieve smooth evolution while maximizing return on investment (ROI).

Tolly engineers verified that the S6720-HI switch could be configured using the NETCONF protocol in the cloud management mode. For example, Tolly engineers was able to configure VXLAN with EVPN using multiple S6720-HI switches in the Huawei Agile Controller.

VXLAN

Virtual Extensible LAN (VXLAN) is one major overlay network technology. VXLAN is used to construct a Unified Virtual Fabric (UVF). As such, multiple service networks or tenant networks can be deployed on the same physical network. Also, service and tenant networks are isolated from each other. This capability truly achieves 'one network for multiple purposes'. The benefits include enabling data transmission of different services or customers, reducing the network construction costs, and improving network resource utilization. The S6720-HI series switches are VXLAN-capable and allow centralized and distributed VXLAN gateway deployment modes. These switches also support the BGP-EVPN protocol for dynamic VXLAN tunnel establishment and can be configured using NETCONF/YANG.

Huawei Technologies, Co., Ltd

S6720-HI Series Agile Switches

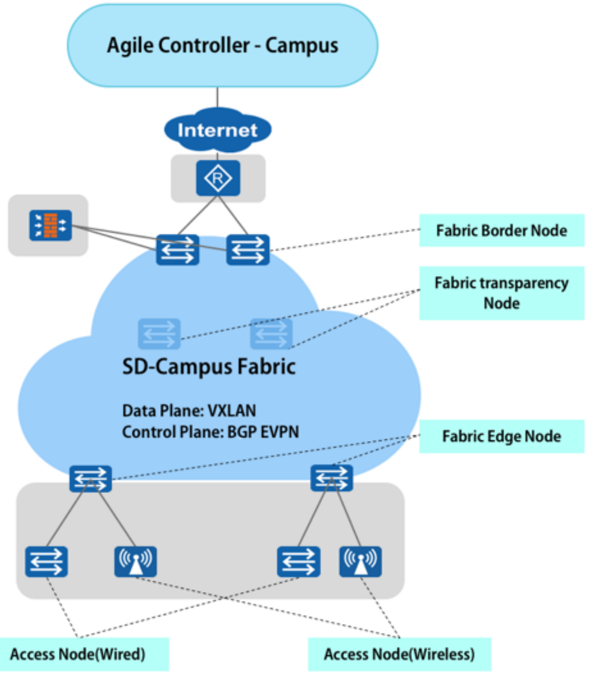
Feature Validation and Capacity Evaluation

Tolly Certified

Tested April 2018

The overlay network technologies can provide Layer 2 connectivity for tunnel endpoints (VTEP in VXLAN) over a physical Layer 3 underlay network. It can expand the Layer 2 network and overcome the limitation of VLAN numbers by adding a new Layer 2 network segment header (VNI for VXLAN).

VXLAN & BGP EVPN Technologies Used in Huawei's SD-Campus Fabric



Benefits:

- **Simple virtual network construction**
  - Supports both centralized and distributed gateway networking.
  - VXLAN only required at the aggregation layer and zero reconstruction of access devices
  - Traversing the complex Layer 3 network
- **Fully automatic virtual network construction**
  - Automatic tunnel establishment based on the BGP-EVPN control plane

Source: Tolly, April 2018

Figure 2

Centralized or Distributed VXLAN L3 Gateways

To allow hosts/VMs using VXLAN to communicate with other non-VXLAN hosts as well as provide connectivity for hosts/VMs in the same or different network segment of the VXLAN overlay network, a gateway is needed.

Tolly engineers verified that the Huawei S6720-HI switch could act as a centralized or a distributed VXLAN L3 gateway.

In either mode, Tolly engineers verified connectivity between endpoints in the same network segment, in different segments, and between VXLAN and non-VXLAN environment.

VXLAN with the BGP-EVPN Control Plane

The initial VXLAN standard relies on data plane flood-and-learn behavior for remote end-host learning (MAC and ARP). This flooding mechanism limits the scalability of the VXLAN overlay network.

Ethernet VPN (EVPN) introduces the control plane to VXLAN.

First, local L2 VNI and L2 VTEP information can be advertised. With EVPN, L2 VXLAN tunnels can be created dynamically. This solution greatly reduces manual configuration and simplifies network deployment.

Second, EVPN advertises host MAC addresses and ARP records, reducing flood traffic on the VXLAN network.

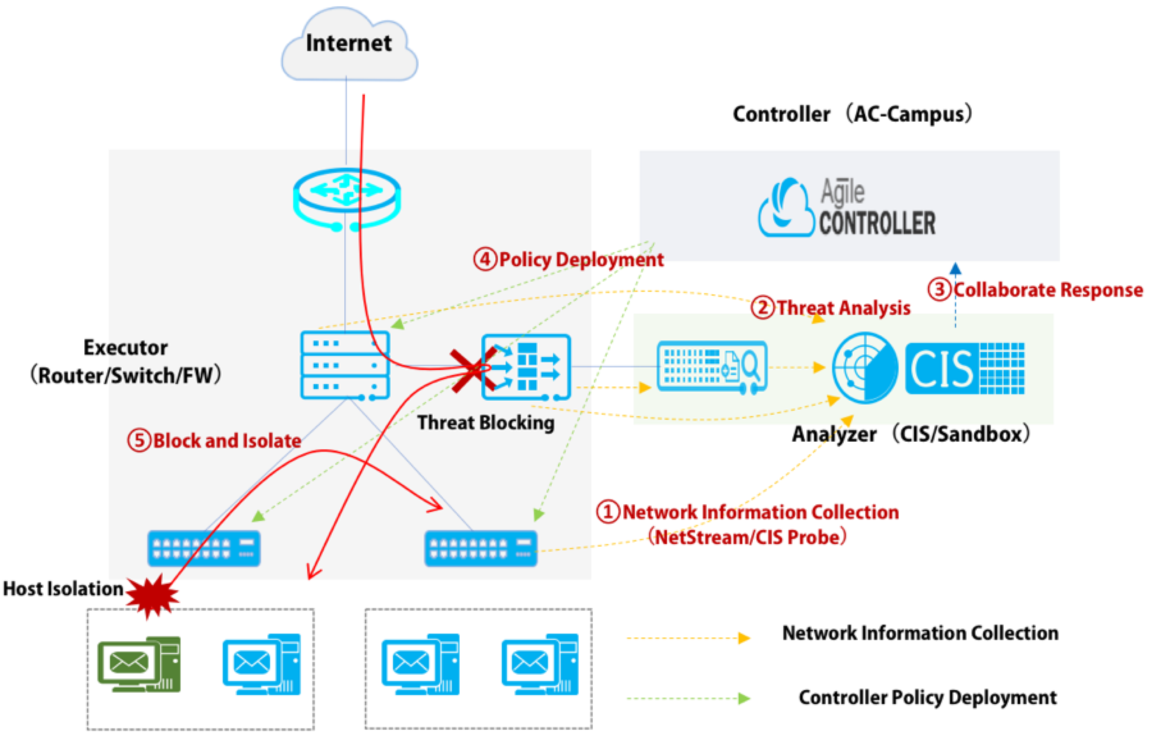
Third, EVPN advertises host IP routes, enabling hosts on different subnets to communicate with each other.

Tolly engineers verified that the S6720-HI switch supported VXLAN with BGP-EVPN.

Big Data Security Collaboration

Huawei agile switches use the NetStream features to collect campus network data and then report such data to the Huawei Cybersecurity Intelligence System (CIS). The purposes of doing so are to detect network security threats, display the security posture across the entire network, and enable automatic or manual response to security threats. The CIS delivers the security policies to the Huawei Agile Controller. The Agile Controller then delivers such policies to agile switches that

Huawei Big Data Security Collaboration



Source: Tolly, April 2018

Figure 3

will handle security events accordingly. All these ensure campus network security. See Figure 3 for the solution.

Tolly engineers verified that the S6720-HI switch interoperated with the Huawei CIS and Agile Controller properly on this.

Secure Boot

Secure boot is the cornerstone of secure system and secure storage. It ensures that the program to be run at each next stage is a trusted one that has not been modified. Huawei uses the secure CPU, eFuse, and other security measures to ensure the Secure Boot system. Starting from the hardware trust anchor, Huawei validates each step in the boot process. The system cannot boot if any boot step fails the validation process. Tolly engineers verified that any modified or forged digital signature image file cannot boot the system. The S6720-HI switch reported a CRC error or signature error based on the modification type.

Super Virtual Fabric

Enterprise campus networks are built step-by-step and have numerous access nodes, multiple layers, and complex topologies. The wide deployment of wireless networks makes enterprise campus networks more difficult to manage.

To address these problems, Huawei developed the Super Virtual Fabric (SVF) technology. SVF virtualizes different network layers' devices including wired and wireless ones into a single network element. The entire network is a large virtual switch to simplify network deployment and management.

Huawei SVF virtualizes core/aggregation layer devices into the virtual switch's Main Processing Unit (MPU), access switches into the line cards, and wireless APs into the ports.

Tolly engineers verified that the S6720-HI switch could act as the SVF parent switch. See Figure 1 for detail.

Native Wireless Access Controller (AC)

Wired and Wireless Convergence

Tolly engineers verified that one S6720-HI switch could manage 1K (1,024) APs and provide connectivity between the wired and wireless networks to achieve wired and wireless network convergence.

OPS

Open Programmability System (OPS) is an open programmable system based on the Python language. IT administrators can program the O&M functions of a Huawei switch through Python scripts to quickly innovate customized functions and implement intelligent O&M.

Tolly engineers verified that the S6720-HI switch supported OPS. One Python scrip was loaded and run on the S6720-HI switch to provide new warnings.

SDN

NETCONF

The Network Configuration protocol (NETCONF) is a network management protocol defined by IETF to install, manipulate, and delete the configuration of network devices. The S6720-HI switch was able to be managed by the NETCONF protocol.

Capacity

Eth-Trunk (LACP Group)

Each Eth-Trunk port (link aggregation port) of the S6720-HI switch supported 32 physical ports.

MAC Table

The S6720-HI switch supported 64K entries in the MAC table.

Routing Table

The S6720-HI switch's routing table supported 64K IPv4 routes and 22K IPv6 routes.

FIB

The S6720-HI switch's Forwarding Information Base (FIB) supported 64K IPv4 and 22K IPv6 FIB entries. Traffic matching the 64K IPv4 and 22K IPv6 FIB entries was forwarded without loss.

ARP Table

The S6720-HI switch supported 64K entries in the ARP table.

VLAN

The S6720-HI switch supported 4,094 VLANs.

Access Control Lists (ACLs)

The S6720-HI switch supported 6K ACL rules. All 6K ACL rules worked properly.

NetStream

The NetStream feature on the S6720-HI switch supported collecting statistics for 1M flows (e.g. each flow has one unique source IP).

Huawei S6720-HI Series Agile 10GbE Switches

Tolly Verified Features and Capacity - Part 1

Cloud Management		✔	ARP Table: 64K entries
✔	Managed by the Agile Controller in the Cloud Management Mode Configuration, monitoring and inspection based on NETCONF/YANG	✔	VLAN: 4,094 VLANs
VXLAN		✔	ACL: 6K ACL rules
✔	Centralized or distributed L3 gateways	✔	NetStream: 1M flows
✔	VXLAN with BGP-EVPN Dynamic VXLAN Tunnel Establishment	**VLAN**	
✔	VXLAN can be configured by the Huawei Agile Controller	✔	VLAN Central Management Protocol (VCMP)
Big Data Security Collaboration		✔	Policy VLAN
✔	Interoperate with the Huawei Cybersecurity Intelligence System (CIS) and Huawei Agile Controller for Campus Network Security The NetStream feature collects network data and report to the Huawei CIS. Huawei CIS run analytics to detect security threats, display the security posture across the entire network, and enable automated or manual response. The CIS delivers security policies to the Agile Controller. The Agile Controller delivers policies to agile switches.	**Security**	
Secure Boot		✔	CPU Defend Policy - CPCAR Device level rate limit for traffic of certain protocols (e.g. ICMP, ARP, etc.) to protect the CPU
✔	Secure Boot CRC check, signature check and other methods to ensure the switch boots from a legit image	✔	CPU Defend Policy - Blacklist Device level blacklist to block known attackers
Native Wireless Access Controller (AC)		✔	Attack Source Traceback Interface level feature. Identify the attacker and respond with certain actions (interface error down, alarm, etc.)
✔	Wired and Wireless Convergence Manage 1,024 wireless access points (APs) and provide connectivity between wired and wireless networks	✔	Attack Source Traceback Whitelist Disable attack source traceback for certain users using the whitelist
Open Programmability System (OPS)		✔	MAC-Forced Forwarding (MFF) Layer 2 isolation. All Layer 2 communications have to go through the gateway
✔	Open Programmability System (OPS) Install and Run Python scripts on the switch to automate certain actions	✔	DHCPv4 Snooping
SDN		✔	DHCPv6 Snooping
✔	NETCONF	✔	ND Snooping
Capacity		✔	IP Source Guard IP traffic has to match the DHCP snooping user-bind table (e.g. IP, MAC, VLAN, interface etc.) to be forwarded
✔	32 Ports per Link Aggregation Group	✔	Dynamic ARP Inspection (DAI) ARP packets have to match the DHCP snooping user-bind table (e.g. IP, MAC, VLAN, interface etc.) to be forwarded
✔	MAC table capacity: 64K MAC addresses	✔	Source Address Validation Improvements (SAVI)
✔	IPv4 Routing Table: 64K IPv4 routes IPv6 Routing Table: 22K IPv6 routes	✔	PPPoE+
✔	FIBv4 capacity: 64K IPv4 routes FIBv6 Capacity: 22K IPv6 routes		

Source: Tolly, April 2018

Table 1

Huawei S6720-HI Series Agile 10GbE Switches

Tolly Verified Features and Capacity - Part 2

User Access Authentication		VPN	
✔	MAC Authentication	✔	Multi-VPN-Instance CE (MCE)
✔	Web Portal Authentication	IPsec	
✔	802.1x Authentication	✔	IPsec for OSPFv3
✔	Free Mobility Allow a user to obtain the same network access policy regardless of user's location	Device Management	
High Availability Ring Protocols		✔	SVF Parent Switch
✔	Ethernet Ring Protection Switching (ERPS)	✔	Easy Operation - Root Switch Zero Touch Provisioning (ZTP) with Huawei eSIght Unified Management Platform
✔	SEP Ring Protection	✔	Patching
✔	Rapid Ring Protection Protocol (RRPP)	iPCA	
✔	STP/RSTP/MSTP	✔	Packet Conservation Algorithm for Internet (iPCA)
Routing Protocols		ACL	
✔	RIP, OSPF, IS-IS, BGP	✔	ACL Atomic Update In the process of adding or deleting a rule to an ACL, other rules in the ACL are always effective
✔	RIPng, OSPFv3, IS-ISv6, BGP4+		

Source: Tolly, April 2018

Table 2

VLAN

VCMP

The S6720-HI switch supported Huawei VLAN Central Management Protocol (VCMP) to synchronize VLAN information across devices.

Policy VLAN

The S6720-HI switch supported policy VLAN based on MAC address, IP subnet, etc.

Security

Certain types of protocol packets including ARP requests, ICMP, DHCP Discover, etc. are sent to switch's CPU for processing. It's critical that the switch provides certain attack defense features to prevent the CPU from overloading.

CPU Attack Defense

Two functions of CPU Attack Defense were verified on the S6720-HI switch by Tolly engineers.

Blacklist - Administrators can create a blacklist by defining an ACL. Then the switch discard the packets matching the ACL rules.

CPCAR - Control Plane Committed Access Rate (CPCAR) limits the rate of protocol packets sent to the control plane and schedules the packets to protect the control plane. The switch identifies service packets based on ACLs and applies the default CAR value to protocol packets so that a limited number of protocol packets are sent to the control plane.

Attack Source Tracing

Three functions of Attack Source Tracing were verified on the S6720-HI switch by Tolly engineers.

Whitelist - The switch does not trace the source of users in the whitelist, ensuring that valid packets from users in the whitelist can be sent to the CPU for processing.

Attack source tracing - Administrators can set the threshold and sampling ratio for attack source tracing. When the number of protocol packets sent from an attack source in a specified period exceeds the threshold, the switch traces and logs the attack source to notify the administrator.

Attack source punishment - Administrator can configure attack source punishment to discard or shut down the interface that received attack packets.

MFF

MAC-forced Forwarding (MFF) isolates user devices in a broadcast domain at Layer 2. It takes advantage of Ethernet broadcast domains and conserves IP addresses and VLANs. MFF ensures that all traffic, including traffic in the same VLAN, is sent to the gateway, so that the gateway can monitor data traffic and prevent malicious attacks between users. The S6720-HI switch supported MFF.

DHCP Snooping (v4/v6)

The S6720-HI switch supported the DHCP snooping feature to make sure that only the DHCP server connected to the trusted ports can distribute IP addresses. It also created the DHCP binding table to record the mapping of each client's IP address, MAC addresses, VLAN and port.

ND Snooping

Neighbor Discovery (ND) snooping is a security feature of IPv6 ND and applies to Layer 2 networks. It creates the ND snooping binding table to record the mapping of source IPv6 addresses, MAC addresses, VLANs, and inbound ports of Neighbor Solicitation (NS) packets from IPv6 clients. Tolly engineers verified that the S6720-HI switch supported ND snooping.

IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP user-bind table or manually configured IP source bindings.

After the IP or MAC address of a client was manually changed to not match the DHCP user-bind table, Tolly engineers verified that the client could not access the network through the S6720-HI switch.

DAI

The S6720-HI supported Dynamic ARP Inspection (DAI). ARP packets have to match the DHCP user-bind table (static or created by DHCP snooping) on IP, MAC, VLAN and interface to be forwarded.

SAVI

With the Source Address Validation Improvements (SAVI) feature, the S6720-HI switch was able to check the validity of the source addresses in the Neighbor Discovery (ND) packets, DHCPv6 packets, and IPv6 data packets. The S6720-HI was able to filter out invalid packets based on the bindings between IP addresses and ports. The bindings are generated by ND snooping and DHCPv6 snooping. To check the validity of the source addresses in IPv6 data packets, the IP source guard feature was enabled.

PPPoE+ (PPPoE IA)

PPPoE+, also called PPPoE Intermediate Agent is deployed on the switch that is located between the PPPoE client and the PPPoE server. It binds the user authentication information with the interface information to provide security for PPPoE access.

Tolly engineers verified that the S6720-HI switch supported PPPoE+.

User Access Authentication

Portal/802.1x/MAC Authentication

The S6720-HI switch supported portal authentication, 802.1x authentication, as well as MAC authentication.

Free Mobility

The free mobility solution allows a user to obtain the same network access policy regardless of user's location (within one VPN instance) and IP address changes in an agile network.

With the Huawei Agile Controller, administrators can specify users into different UCL groups and assign network access policies based on destination, VPN instance, and applicable devices.

The S6720-HI supported Free Mobility.

High Availability

ERPS

The S6720-HI switch supported ITU-T G. 8032 Ethernet Ring Protection Switching (ERPS) with 19ms traffic failover.

Huawei SEP Ring

Smart Ethernet Protection (SEP) is Huawei's technology for ring topology high availability. The S6720-HI switch supported SEP with 5.7ms traffic failover.

RRPP

The S6720-HI supported the Rapid Ring Protection Protocol (RRPP) with 16ms traffic failover.

STP/RSTP/MSTP

The S6720-HI supported spanning tree protocols STP, RSTP and MSTP.

Routing Protocols

Routing Protocols

IPv4 Routing Protocols

The S6720-HI supported RIP, OSPF, IS-IS and BGP routing protocols.

IPv6 Routing Protocols

The S6720-HI supported RIPng, OSPFv3, IS-ISv6 and BGP4+ IPv6 routing protocols.

VPN

MCE

The S6720-HI switch supported Multi-VPN-Instance CE (MCE). It acted as the CE device for multiple MPLS VPNs.

IPsec

IPsec for OSPFv3

The S6720-HI switch supported IPsec for OSPFv3 to authenticate the OSPFv3 protocol.

Device Management

Zero Touch Provisioning

Tolly engineers verified that the Huawei eSight Unified Management Platform supported the Zero Touch Provisioning (ZTP) feature. Administrators can plan the network topology using eSight's graphic Web interface and specify the configuration for each remote device. A root switch which is managed by eSight can then automatically deploy planned configurations to the remote devices when the out-of-box remote devices connects to the network. The S6720-HI switch supported working as the root device.

Patching

The S6720-HI switch supported patching to the firmware.

iPCA

The S6720-HI adopts Huawei's proprietary Packet Conservation Algorithm for Internet (iPCA). Unlike traditional detection technologies, such as Network Quality Analyzer (NQA) and Y.1731 that use simulated or inserted streams, iPCA implements the evolution from estimated to accurate Operations and Maintenance (O&M). NQA technology uses simulated streams to detect network quality, and the Y.1731 technology uses inserted streams. Both methods actually detect link quality by simulating service flows. Therefore, these detection methods cannot reflect the actual link quality or accurately locate fault sources. From Huawei's field experience, latency, jitter, and packet loss accuracy of traditional methods is only about 30 percent. Since traditional methods locate faults by reducing fault impact ranges, the fault location is less precise and the fault isolation process can take weeks or longer.

iPCA is an in-line detection technology that uses programmable service flows to detect network quality, dye the packets with no overhead, count real service flows, and detect service flow link quality anytime and anywhere. According to Huawei, the latency, jitter, and packet loss detection accuracy of iPCA can reach 99 percent. Each Ethernet Network Processor (ENP) has two built-in detection points that cover all forwarding paths on links, cards, and processors. Faults are reported based on fine granularity. If a network problem that affects user experience occurs, iPCA can locate the link, card, or processor where the problem occurs within seconds.

Tolly engineers verified that the S6720-HI switch supported iPCA to detect the device level, link level and network level packet loss accurately.

ACL

ACL Atomic Update

Traditionally, when administrators add or delete a rule in an ACL, the switch needs to update the whole ACL for that rule. During the update process, other existing rules in the ACL will not be effective. This creates security issues.

The S6720-HI switch supports ACL atomic update. When Tolly engineers added or deleted a rule to/from one existing ACL, all other existing rules in that ACL remained effective always.

Huawei S6720-HI Series Agile 10GbE Switches Test Bed

S6720-30L-HI-24S

S6720-50L-HI-48S

Spirent TestCenter

Source: Tolly, April 2018

Figure 4

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 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

The Tolly Group gratefully acknowledges the providers of test equipment/software used in this project.

Vendor	Product	Web
Spirent	**TestCenter**	TESTED WITH SPIRENT http://www.spirent.com

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.