TEST REPORT

Tolly.

#219156

December 2019

Commissioned by
Huawei Technologies Co., Ltd.

Huawei CloudEngine S5735-L Series Switches

Performance Evaluation and Feature Validation

Executive Summary

Huawei CloudEngine S5735-L series switches are simplified gigabit switches with GbE access ports and 10GbE uplink ports. They are ideal to be deployed in the access layer of campus networks.

Tolly engineers evaluated Huawei CloudEngine S5735-L series switches' performance and validated their features. Built upon Huawei's high performance Versatile Routing Platform (VRP) software, CloudEngine S5735-L series switches support flexible Ethernet networking, various security features, and basic IPv4 / IPv6 Layer 3 routing protocols.

The Bottom Line

Huawei CloudEngine S5735-L Series Switches:

1 Support Huawei's Super Virtual Fabric (SVF) technology, which virtualizes core/aggregation devices (parent) and access devices (clients) into one logical device for easier management. SVF clients can include two layers of access switches (ASes) and one layer of WLAN APs, with ASes supporting stacked devices

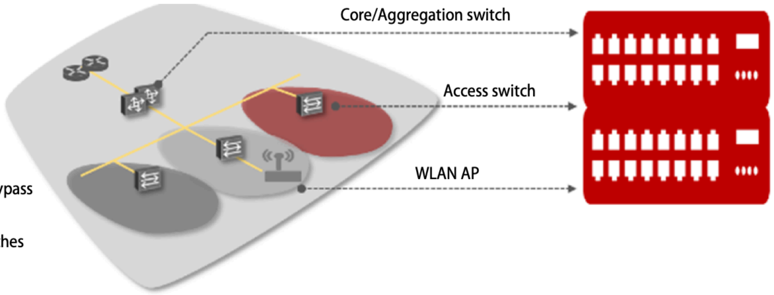
2 Support common Layer 2 protocols and basic Layer 3 routing protocols

3 Support numerous security features including dynamic ARP inspection, IP source guard, PPPoE+, secure boot, and more

Huawei Super Virtual Fabric (SVF)

Typical Campus Network

- Layered tree architecture
- Horizontal stacking of core/aggregation devices
- WLAN ACs connect to core/aggregation devices in bypass mode
- High quantities of access switches



Converged Campus Network

- Cloud architecture, on-demand expansion
- Campus network virtualized into **one** device
- Access switch = WLAN AP
- Aggregation switch = WLAN AC

1. **Simplified Management**: The entire network is virtualized into one device. Huawei eSight, a unified network management platform, only needs to manage one network element, supporting plug-and-play.
2. **Centralized Control**: ACL, QoS, and user security policies are centrally controlled by the core device.
3. **Reduced Investment**: Low-specification fixed switches can be used as access devices, reducing the overall investment on devices.

Source: Tolly, November 2019

Figure 1

Test Results

Tolly engineers tested functions and performance of Huawei CloudEngine S5735-L series switches (hereinafter referred to as the S5735-L switch). Test results apply to all Huawei CloudEngine S5735-L models as listed in Figure 2. For summary of the test cases, refer to Table 2 and Table 3 on pages 6 and 7. Test results are as follows.

Port Capability

Port Performance

The 10/100/1000BASE-T ports and 10GbE SFP+ optical ports on the S5735-L switch support line-rate forwarding of traffic with different frame sizes, as described in Table 1.

Device Capacity

MAC Table Capacity

The S5735-L switch supports 16K (16,384) MAC addresses in its MAC table. Tolly engineers verified that the switch forwarded traffic matching all entries in the MAC table, without frame loss or broadcasts occurring.

ARP Table Capacity

The S5735-L switch supports 4K entries in its ARP table. Tolly engineers verified that the switch forwarded traffic matching all entries in its ARP table, without any packet loss.

Routing Table/FIB Capacity

The S5735-L switch supports 4,096 IPv4 routes in both its IPv4 routing table and FIBv4 table. Tolly engineers verified that the switch forwarded traffic matching all routing entries in the FIBv4 table, without any packet loss.

The S5735-L switch supports 1,023 IPv6 routes in both its IPv6 routing table and FIBv6 table. Tolly engineers verified that the switch forwarded traffic matching all routing entries in the FIBv6 table, without any packet loss.

VLAN Capacity

The S5735-L switch supports 4,094 VLANs.

Huawei Technologies Co., Ltd.

CloudEngine S5735-L Series Switches

Performance Evaluation and Feature Validation

Tested November 2019

ACL Capacity

The S5735-L switch supports 2,432 ACL rules. Tolly engineers verified that all ACL rules worked properly to match traffic and perform configured actions (e.g. deny).

Huawei CloudEngine S5735-L Series Switch Performance (% of Line-rate)

(as reported by Spirent TestCenter)

Frame Size (Bytes)	64	128	256	512	1024	1280	1518
GbE Ports	100%	100%	100%	100%	100%	100%	100%
10GbE Ports	100%	100%	100%	100%	100%	100%	100%

Notes: 100% line-rate bidirectional traffic between two ports ("GbE to GbE" or "10GbE to 10GbE") was used with zero frame loss. The CloudEngine S5735-L24P4X-A model was used as the device under test.

Source: Tolly, November 2019

Table 1

Loop-free/Ring Protocols

STP/RSTP/MSTP

The S5735-L switch supports the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).

ERPS

The S5735-L switch supports the Ethernet Ring Protection Switching (ERPS) protocol with less than 50ms failover time.

SEP

The S5735-L switch supports the Smart Ethernet Protection (SEP) protocol with less than 50ms failover time.

RRPP

The S5735-L switch supports the Rapid Ring Protection Protocol (RRPP) with less than 50ms failover time and less than 7ms failback time.

Routing Protocols

The S5735-L switch supports IPv4 routing protocols such as RIP and OSPF, as well as IPv6 routing protocols such as RIPng and OSPFv3.

Security

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

CPU Attack Defense

Two functions of CPU Attack Defense were verified on the S5735-L switch by Tolly engineers.

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

CPCAR - Control Plane Committed Access Rate (CPCAR) limits the rate of protocol packets sent to the control plane. The switch can limit the traffic rate based on either the protocol type or ACL.

Attack Source Tracing

Three functions of Attack Source Tracing were verified on the S5735-L switch by Tolly engineers.

Whitelist - The switch does not trace the source of users in the whitelist, ensuring that valid protocol 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 and perform attack source punishment.

Attack source punishment - Administrators can configure attack source punishment to discard or shut down the interface when an attack source is traced.

MFF

MAC-forced Forwarding (MFF) isolates user devices in a broadcast domain at Layer 2. 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 S5735-L switch supports MFF.

IPSG

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 (static or created by DHCP snooping).

After the IP or MAC address of a host was manually changed to not match the DHCP user-bind table, Tolly engineers verified that the host's IP traffic was all discarded by the S5735-L switch.

DAI

The S5735-L switch supports 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.

DHCPv6 Snooping

The S5735-L switch supports the DHCPv6 snooping feature to make sure that only the DHCPv6 server connected to the trusted ports can distribute IPv6 addresses. It also creates the DHCP user-bind table to record the mapping of each client's IPv6 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 user-bind table to record the mapping of source IPv6 addresses, MAC addresses, VLANs, and inbound ports of Neighbor Solicitation (NS) packets from IPv6 hosts. Tolly engineers verified that the S5735-L switch supported ND snooping.

SAVI

With the Source Address Validation Improvements (SAVI) feature, the S5735-L switch is able to check the validity of the source addresses in the Neighbor Discovery (ND) packets, DHCPv6 packets, and IPv6 data packets. The S5735-L switch is able to filter out invalid packets based on the user-bind table. The user-bind table is generated by ND snooping and DHCPv6 snooping. To check the validity of the source addresses in IPv6 data packets, the IP source guard feature needs to be enabled.

PPPoE+

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 S5735-L switch supported PPPoE+.

Secure Boot

Secure boot is the cornerstone of a secure system and secure storage. It ensures that the program to be run at each boot stage is a trusted one that has not been modified. Huawei uses the secure CPU, eFuse, and other security measures to ensure the boot security of the 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 a modified or forged digital signature image file cannot boot the system. The S5735-L switch reported a CRC error or signature error based on the modification type.

Authentication

802.1X/MAC/Web Portal Authentication

The S5735-L switch can work as the authentication policy enforcement point to implement 802.1X authentication, MAC authentication, and web portal authentication for users. The S5735-L switch can support up to 1,024 concurrent online users.

Device Management

Zero Touch Provisioning (ZTP)

The S5735-L switch can work with Huawei eSight Unified Management System, to implement zero touch provisioning (ZTP).

Super Virtual Fabric (SVF)

On a traditional campus network, a large number of access devices are widely distributed and have similar configurations. If these devices are configured and managed via traditional methods, a large amount of work is repeated. Huawei's SVF technology virtualizes core/aggregation devices and access devices (including access switches for wired access and WLAN APs for wireless access) into one logical device. The SVF parent (core/aggregation device) manages and configures SVF clients (access devices), simplifying network management and configuration.

An SVF system's clients support two layers of Access Switches (ASes) and one layer of WLAN APs, with ASes supporting stacked devices.

Tolly engineers verified that the S5735-L switch was able to function as the AS node in an SVF system.

Intelligent Upgrade

The S5735-L switch can be connected to Huawei Online Upgrade Platform (HOUP) to implement intelligent upgrade.

PoE

CloudEngine S5735-L series PoE models (e.g. CloudEngine S5735-L24P4X-A and other P models) support acting as the PoE power sourcing equipment (PS) to provide power to powered devices (PDs), such as WLAN APs.

Perpetual PoE

PoE-capable S5735-L series switches support perpetual PoE. During soft reboot by command or firmware update, the PoE ports of the switch continuously supply power to powered devices (PDs).

Fast PoE

After the S5735-L switch is powered on, the PoE ports on it start to provide PoE power to powered devices (PDs) within 4 seconds.

802.3af and 802.3at

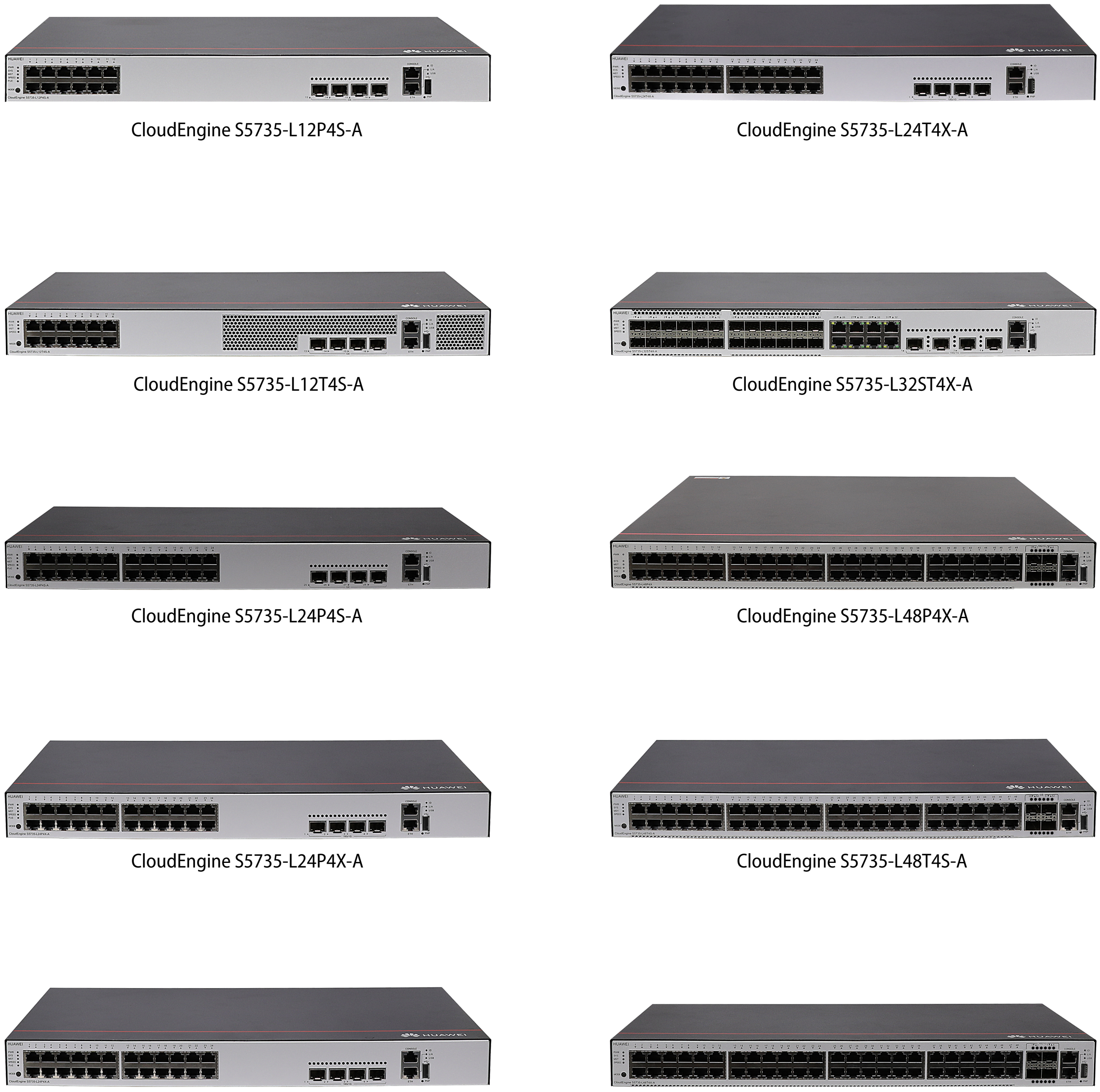
PoE-capable S5735-L series switches support 802.3af (PoE) and 802.3at (PoE+) standards.

Test Methodology

Capacity

In the capacity test, each item was tested independently.

Huawei CloudEngine S5735-L Series Switches



CloudEngine S5735-L12P4S-A

CloudEngine S5735-L24T4X-A

CloudEngine S5735-L12T4S-A

CloudEngine S5735-L32ST4X-A

CloudEngine S5735-L24P4S-A

CloudEngine S5735-L48P4X-A

CloudEngine S5735-L24P4X-A

CloudEngine S5735-L48T4S-A

CloudEngine S5735-L24T4S-A

CloudEngine S5735-L48T4X-A

Source: Tolly, November 2019

Figure 2

Huawei CloudEngine S5735-L Series Switches

Tolly Verified Features - Part 1 of 2

Interface Capability	
✔	GbE Ports Port-to-port Line-rate Forwarding (64- to 1518-Byte RFC2544 standard frame sizes)
✔	10GbE Ports Port-to-port Line-rate Forwarding (64- to 1518-Byte RFC2544 standard frame sizes)
Device Capacity	
✔	MAC table: 16K MAC addresses
✔	ARP table: 4K entries
✔	Routing table: 4,096 IPv4 routes 1,023 IPv6 routes
✔	FIB: 4,096 IPv4 forwarding entries 1,023 IPv6 forwarding entries
✔	VLAN: 4,094 VLANs
✔	ACL: 2,432 ACL rules
Loop-free/Ring Protocol	
✔	STP/RSTP/MSTP
✔	Ethernet Ring Protection Switching (ERPS) with less than 50ms failover convergence time
✔	Smart Ethernet Protection (SEP) with less than 50ms failover convergence time
✔	Rapid Ring Protection Protocol (RRPP) with less than 50ms failover convergence time and 7ms failback convergence time

Routing Protocol	
✔	RIP
✔	OSPF
✔	RIPng
✔	OSPFv3

Source: Tolly, November 2019

Table 2

Huawei CloudEngine S5735-L Series Switches

Tolly Verified Features - Part 2 of 2

	Security		Authentication (as the Network Access Control - NAC Policy Enforcement Point)
✔	CPU defend policy - CPCAR Device level rate limit for traffic of certain protocols (e.g. ICMP, ARP, etc.) to protect the CPU	✔	802.1X authentication
✔	CPU defend policy - blacklist Device level blacklist to block known attackers	✔	MAC authentication
✔	Attack source tracing Interface level feature. Identify the attacker and respond with certain actions (interface error down, alarm, etc.)	✔	Web authentication (portal authentication)
✔	MAC-Forced Forwarding (MFF) Layer 2 isolation. All Layer 2 communications have to go through the gateway	✔	1,024 concurrent authenticated users
✔	Dynamic ARP Inspection (DAI) Prevent man-in-the-middle attacks and theft on authorized users' information. The device validates ARP packets' source IP, source MAC, VLAN ID and interface with the binding table (static or DHCP snooping)		**Device Management**
✔	IP Source Guard (IPSG) Prevent IP address spoofing attacks (unauthorized hosts access and attack the network with forged IP addresses). The device validates IP packets' source IP, source MAC, VLAN ID and interface with the binding table (static or DHCP snooping)	✔	Zero Touch Provisioning (ZTP) with Huawei eSight Unified Management System
✔	DHCPv6 snooping Trusted port for the DHCPv6 server; Binding table creation	✔	Super Virtual Fabric (SVF) Access Switch (AS) role
✔	ND snooping Trusted port for ND; Binding table creation	✔	Intelligent upgrade with the Huawei Online Upgrade Platform (HOUP)
✔	Source Address Validation Improvements (SAVI) Validate DHCPv6, ND and IPv6 packets with the binding table		**PoE (P Models only)**
✔	PPPoE+ (PPPoE Intermediate Agent) Add the PPPoE client-side interface information to the PPPoE packets for the BRAS to distinguish between end hosts	✔	Perpetual PoE PoE ports provide continuous power to powered devices during soft reboot (reboot via command line) or firmware update
✔	Secure boot CRC check, signature check and other methods to ensure the switch boots from a legit image	✔	Fast PoE After the switch is powered on, the PoE ports on it start to provide PoE power to PD devices within 4 seconds
		✔	802.3af and 802.3at (PoE and PoE+)

Source: Tolly, November 2019

Table 3

About Tolly

The Tolly Group companies have been delivering world-class ICT services for 30 years. Tolly is a leading global provider of third-party validation services for vendors of ICT 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	Web
Huawei	CloudEngine S5735-L24P4X-A VRP software, Version 5.170 (S5735 V200R019C00SPC300)	HUAWEI https://e.huawei.com
Spirent	TestCenter	spirent™ Promise. Assured. https://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.