Release Notes for Catalyst 2960-L Series Switches, Cisco IOS Release 15.2(7)Ex

First Published: April 15, 2019

Last Updated: March 29, 2024

This release note describes the features and caveats for the Cisco IOS Release 15.2(7)Ex software on the Catalyst 2960-L family of switches.

Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of the switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Upgrading the Switch Software" section on page 3.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Software Image" section on page 4.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://www.cisco.com/download/navigator.html

Contents

Cisco Systems, Inc.
www.cisco.com

- Related Documentation, page 14

Introduction

The Catalyst 2960-L switches are Ethernet switches to which you can connect devices such as Cisco IP Phones, Cisco Wireless Access Points, workstations, and other network devices such as servers, routers, and other switches.

Supported Hardware

Switch Models

Table 1 Catalyst 2960-L Switch Models

Switch Model	Cisco IOS Image	Description
WS-C2960L-8TS-LL	LAN Lite	Cisco Catalyst 2960-L switch with 8 10/100/1000 Ethernet ports and 2 SFP module slots
WS-C2960L-8PS-LL	LAN Lite	Cisco Catalyst 2960-L PoE switch with 8 10/100/1000 Ethernet ports and 2 SFP module slots
WS-C2960L-16TS-LL	LAN Lite	Cisco Catalyst 2960-L switch with 16 10/100/1000 Ethernet ports and 2 SFP module slots
WS-C2960L-16PS-LL	LAN Lite	Cisco Catalyst 2960-L PoE switch with 16 10/100/1000 Ethernet ports and 2 SFP module slots
WS-C2960L-24TS-LL	LAN Lite	Cisco Catalyst 2960-L switch with 24 10/100/1000 Ethernet ports and 4 SFP module slots
WS-C2960L-24PS-LL	LAN Lite	Cisco Catalyst 2960-L PoE switch with 24 10/100/1000 Ethernet ports and 4 SFP module slots
WS-C2960L-48TS-LL	LAN Lite	Cisco Catalyst 2960-L switch with 48 10/100/1000 Ethernet ports and 4 SFP module slots
WS-C2960L-48PS-LL	LAN Lite	Cisco Catalyst 2960-L PoE switch with 48 10/100/1000 Ethernet ports and 4 SFP module slots, without fan
WS-C2960L-24TQ-LL	LAN Lite	Cisco Catalyst 2960-L switch with 24 10/100/1000 Ethernet ports and 4 SFP+ module slots
WS-C2960L-24PQ-LL	LAN Lite	Cisco Catalyst 2960-L PoE switch with 24 10/100/1000 Ethernet ports and 4 SFP+ module slots
WS-C2960L-48TQ-LL	LAN Lite	Cisco Catalyst 2960-L switch with 48 10/100/1000 Ethernet ports and 4 SFP+ module slots
WS-C2960L-48PQ-LL	LAN Lite	Cisco Catalyst 2960-L PoE switch with 48 10/100/1000 Ethernet ports and 4 SFP+ module slots, without fan

Optics Modules

The Catalyst 2960-L switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest SFP+ and SFP module compatibility information:

http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/GE_Tx_Matrix.html

Device Manager System Requirements

The following table lists the system requirements for a PC running Cisco Configuration Professional for Catalyst, including Web browser versions.

Table 2 System Requirements

System Component	Requirement
Operating System	Any of the following: • Mac OS 10.9.5 • Microsoft Windows Version 7
Browser	Cisco CPC can be used with the following browsers: • Google Chrome 52 and later • Mozilla Firefox 48 and later • Apple Safari 9 and later • Internet Explorer 11 and later
Screen Resolution	1280 X 800 pixels or higher

Upgrading the Switch Software

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release number. The files necessary for web management are contained in a subdirectory. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Software Image

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image and a specific software license.

Table 3 Software Image for Cisco Catalyst 2960-L

Image	Filename	Description
Universal image	c2960l-universalk9-mz.152-7.E.bin	LAN Lite image
Universal image	c2960l-universalk9-mz.152-7.E.tar	LAN Lite cryptographic image with Device Manager.

Web UI

If the Web UI does not load or work properly after the software upgrade, perform the following steps:

Step 1 Specify the authentication method for HTTP server users as local.

```
Device(config)# ip http authentication local
```

Step 2 Configure the username and password with privilege 15.

```
Device(config)# username user privilege 15 password password
```

Step 3 Clear the browser cache and relaunch the Web UI.

Step 4 Login by entering the privilege 15 username and password.

Features of the Switch

The Catalyst 2960-L switch supports the LAN Lite+ feature set. This provides standard Layer 2 security and quality of service (QoS) features, and up to 256 active VLANs. The switch models have reduced functionality and scalability with entry level features in Layer 2.

Specific differences between the two feature sets are described in the following sections.

- Ease of Operations, page 4
- Network Security, page 5
- Deployment and Control Features, page 6

Ease of Operations

- Cisco Catalyst Smart Operations is a comprehensive set of features that simplify LAN deployment, configuration, and troubleshooting. Catalyst Smart Operations enable zero touch installation and replacement of switches and fast upgrade, as well as ease of troubleshooting with reduced operational cost. Catalyst Smart Operations is a set of features that includes Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:
  - Cisco Auto Smartports provide automatic configuration as devices connect to the switch port, allowing auto detection and plug and play of the device onto the network.

  - Cisco Smart Configuration provides a single point of management for a group of switches and in addition adds the ability to archive and back up configuration files to a file server or switch allowing seamless zero touch switch replacement.
  - Cisco Smart Troubleshooting is an extensive array of debug diagnostic commands and system health checks within the switch, including Generic Online Diagnostics (GOLD) and Onboard Failure Logging (OBFL).
  - Auto Configuration determines the level of network access provided to an endpoint based on the type of the endpoint device.
- Cisco Prime Infrastructure is a set of tools that enables you to automate much of the management of your Cisco network. It is supported with device pack1 (2.1) 4.
- Interface templates provide a mechanism to configure multiple commands at the same time and associate it with a target (such as an interface). An interface template is a container of configurations or policies that can be applied to specific ports.

Network Security

The Cisco Catalyst 2960-L Series Switches provide a range of security features to limit access to the network and mitigate threats.

- In Cisco IOS Release 15.2(7)E3 and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.
- Port security secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers.
- Dynamic ARP inspection (DAI) to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.
- Flexible authentication that supports multiple authentication mechanisms including 802.1X, MAC Authentication Bypass and web authentication using a single, consistent configuration.
- Open mode that creates a user friendly environment for 802.1X operations.
- Comprehensive RADIUS Change of Authorization capability for asynchronous policy management.
- Cisco standard and extended IP security router ACLs define security policies on routed interfaces for control-plane and data-plane traffic. IPv6 ACLs can be applied to filter IPv6 traffic.
- Port-based ACLs for Layer 2 interfaces allow security policies to be applied on individual switch ports.
- Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3.
- (SNMPv3) provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH Protocol, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.
- Bidirectional data support on the Switched Port Analyzer (SPAN) port allows Cisco Intrusion Detection.
- TACACS+ and RADIUS authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
- MAC address notification allows administrators to be notified of users added to or removed from the network.

- Multilevel security on console access prevents unauthorized users from altering the switch configuration.
- Bridge protocol data unit (BPDU) Guard shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- IGMP filtering provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port.
- 802.1x monitor mode allows companies to enable authentication across the wired infrastructure in an audit mode without affecting wired users or devices. It helps IT administrators smoothly manage 802.1x transitions by allowing access and logging system messages when a device requires reconfiguration or is missing an 802.1x supplicant.

Deployment and Control Features

- Dynamic Host Configuration Protocol (DHCP) Auto-configuration of multiple switches through a boot server eases switch deployment.
- Auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
- Dynamic Trunking Protocol (DTP) facilitates dynamic trunk configuration across all switch ports.
- Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel groups and Gigabit groups.
- Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad.
- Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links caused by incorrect wiring. Also, port faults can be detected and disabled on the interfaces.
- Internet Group Management Protocol (IGMP) v1, v2, v3 Snooping for IPv4. MLD v1 and v2 Snooping provide fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors.
- Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.
- The Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis.
- Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from source to destination.
- Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location.
- Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches.
- Storm control for unicast, broadcast and multicast traffic to prevent disruption in the network due to packet flooding on the LAN.
- IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) provide rapid spanning-tree convergence independent of spanning-tree timers and also offers the benefit of Layer 2 load balancing and distributed processing.
- Switch-port auto-recovery (error-disable) automatically attempts to reactivate a link that is disabled because of a network error.

Limitations and Restrictions

- There is limit of 384 ACEs for MAC/IPv4 and 256 ACEs for IPv6. For some scenarios, one ACE entry can lead to 2 TCAM entries. For IPv6, 512 TCAM entries are used per ASIC.
- Extension header match options for IPv6 PACLs are not supported on the switch. Also, PACLs not supported in the out direction.
- Storm control for multicast with PPS and % may not work.

Software Compatibility Matrix

ISE	CPC
2.3	1.4

New Software Features

Features Introduced in Cisco IOS Release 15.2(7)10

None.

Features Introduced in Cisco IOS Release 15.2(7)E9

None.

Features Introduced in Cisco IOS Release 15.2(7)E8

None.

Features Introduced in Cisco IOS Release 15.2(7)E7

Data Sanitization: Supports the use of the National Institute of Standards and Technology (NIST) purge method that renders data unrecoverable through simple, non-invasive data recovery techniques or through state-of-the-art laboratory techniques.

For more information, see the Data Sanitization chapter of the System Management Configuration Guide.

Features Introduced in Cisco IOS Release 15.2(7)E6

None

Features Introduced in Cisco IOS Release 15.2(7)E5

None.

Features Introduced in Cisco IOS Release 15.2(7)E4

None

Features Introduced in Cisco IOS Release 15.2(7)E3

None.

Features Introduced in Cisco IOS Release 15.2(7)E2

None.

Features Introduced in Cisco IOS Release 15.2(7)E1

None

Features Introduced in Cisco IOS Release 15.2(7)E0a

- IPv6 RA Guard: Supports allowing the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device platform.
- Dual Active Detection Using Enhanced PAgP: If the switch is connected to a Virtual Switch System (VSS) using a PAgP EtherChannel, it automatically serves as a VSS client, using enhanced PAgP on this EtherChannel for dual-active detection.
- Sampled flow (sFlow): This feature allows you to monitor real-time traffic in data networks containing switches and routers. It uses the sampling mechanism in the sFlow agent software on switches to monitor traffic and Last Updated: March 29, 2024to forward the sample data to the central data collector.
- IP Source Guard support for EtherChannels: You can now configure IP source guard on EtherChannel interfaces.
- SFTP: The device supports SSH File Transfer Protocol (SFTP). The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device. Therefore, any SFTP server user with the appropriate permission can copy files to and from the device.

Service and Support

Information About Caveats

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/en/US/support/index.html

Click **Product Support** > **Switches**. Choose your product and click **Troubleshooting** to find information on the problem you are experiencing.

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats

None

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.2(7)E10

Table 4 Caveats Resolved in Cisco IOS Release 15.2(7)E10

Bug ID	Headline
CSCwh96519	For PoE used and remaining power on 3560, the SNMP walk result is showing inaccurate data
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerability

Caveats Resolved in Cisco IOS Release 15.2(7)E9

None

Caveats Resolved in Cisco IOS Release 15.2(7)E8

Table 5 Caveats Resolved in Cisco IOS Release 15.2(7)E8

Bug ID	Headline
CSCwb76885	Cat2960-L stops providing power on random ports after IOS upgrade.

Caveats Resolved in Cisco IOS Release 15.2(7)E7

Table 6 Caveats Resolved in Cisco IOS Release 15.2(7)E7

Bug ID	Headline
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvx63027	Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability.
CSCwa96810	Cisco IOS and IOS XE Software Common Industrial Protocol Request Denial of Service Vulnerability.

Caveats Resolved in Cisco IOS Release 15.2(7)E6

Table 7 Caveats Resolved in Cisco IOS Release 15.2(7)E6

Bug ID	Headline
CSCwa19652	Reachability issue after IOS upgrade to the version 15.2(7)E4.
CSCvx37171	ARP broadcast packet duplicated on egress C1000/C2960l.
CSCvx23984	Cat2960 crash after DACL is pushed from ISE to the switch.
CSCwa47201	Switch failure while handling Ethernet Configuration Testing Protocol (ECTP)

Caveats Resolved in Cisco IOS Release 15.2(7)E5

Table 8 Caveats Resolved in Cisco IOS Release 15.2(7)E5

Bug ID	Headline
CSCvx75762	C2960L does not transfer VRRP packets.
CSCvx77198	Spanning-tree port shows 'Role:ROOT status:BLK' on Cat1000 after shutting the port on Cat2960L.
CSCvy73453	C2960L Loopback interface is unreachable after copying file from FTP server.
CSCvy92366	Wrong Operational Bandwidth on 2960L.
CSCvx76066	Switch crashes due to "HTTP Core".
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability.

Caveats Resolved in Cisco IOS Release 15.2(7)E4

Table 9 Caveats Resolved in Cisco IOS Release 15.2(7)E4

Bug ID	Headline
CSCvv93417	Stack Member Switch fails wired dot1x; MasterSwitch passes dot1x using the same configs.
CSCvv45359	no ip source-route\" command is not supported on 2960L 15.2(7)E2 but is on 2960X.
CSCvv75698	Switch gets hung with traces and error logs.
CSCvw22338	After version up switch detected as IEEE PD when connecting to Non-PD device.
CSCvw79337	Switch archive download-sw failed.

Table 9 Caveats Resolved in Cisco IOS Release 15.2(7)E4

Bug ID	Headline
CSCvu52584	g0/26 port mac address abnormal.
CSCvv86851	TACACS not working if TACACS group server has "server-private <ip> key <passw>" in 15.2(7)E3/3.11.3E.

Caveats Resolved in Cisco IOS Release 15.2(7)E3

Table 10 Caveats Resolved in Cisco IOS Release 15.2(7)E3

Bug ID	Headline
CSCvs83982	Pings to Phones Through 2960L Are Unresponsive When Configured as an Access Port.
CSCvs95884	C2960L:15.2(7)E1 - DHCP snooping blocks request from DHCP assigned address to pxe boot server.
CSCvt21796	Traffic blackhole due to wrongly programmed trunk port.
CSCvu69734	Broadcast packet duplicated when through C2960L.
CSCvu10399	Cisco IOS and IOS XE Software Information Disclosure Vulnerability.
CSCvv00134	VTY telnet disable, enable ssh based on platform request.

Caveats Resolved in Cisco IOS Release 15.2(7)E2

Table 11 Caveats Resolved in Cisco IOS Release 15.2(7)E2

Bug ID	Headline
CSCvt19077	AAA configurations are missing after reload.
CSCvq91578	IPDT doesn't trigger the inactivity timer.
CSCvs43220	After failover, C2960L Standby Switch cannot ping the virtual IP address.
CSCvr01634	2960L spanning-tree doesn't block BPDU of bridge group when bridge group is enabled on neighbor device.
CSCvr12424	WS-C2960L-48TS | 15.2(7)E0a | Switch duplicates DHCP Packets.
CSCvs46744	Frame with special DesMac are not pass through.
CSCvs83982	Pings to Phones Through 2960L Are Unresponsive When Configured as an Access Port.

Caveats Resolved in Cisco IOS Release 15.2(7)E1

Table 12 Caveats Resolved in Cisco IOS Release 15.2(7)E1

Bug ID	Headline
CSCvk21769	C2960L packet loss on 10M/Full port.
CSCvn60573	2960L doesn't fwd mcast traffic when igmp snooping querier is enabled.
CSCvo86028	C2960L IP Device Tracking deleting voice device IP and removes DACL from port.
CSCvp20868	2960L archive download-sw failed from 15.2(7)E to other version.
CSCvr23528	When second clients downloads a DACL it is not able to ping to switch or any device.
CSCvo07272	Only G0/2 failed to pass traffic on C2960L if MAB is enabled.
CSCvo09529	On 2960L 15.2(6)E2, QoS remarking is not working.
CSCvp13111	'ip igmp snooping' under vlan missing after 2960L reload.
CSCvq69541	C2960L not able to learn SVI MAC address of Peer C2960L switch.
CSCvq72699	Multicast is not forwarded on 2960L <PAgP>.
CSCvq76129	2960L no ICMP response (timeout) when traceroute.
CSCvr01634	2960L spanning-tree doesn't block bpdu of bridge group when bridge group enabled on neighbor device.
CSCvr17772	C2960L - DHCP snooping blocks request from DHCP assigned address to pxe boot server.

Caveats Resolved in Cisco IOS Release 15.2(7)E0a

Table 13 Caveats Resolved in Cisco IOS Release 15.2(7)E0a

Bug ID	Headline
CSCvj84079	2960L ping/telnet issue due to i/o memory leak.
CSCvm71022	Loop on 2960L.
CSCvm87588	2960L drops inner vlan tag whenever double tagged packet is received.
CSCvn37402	2960L hung up suddenly without any syslog output.
CSCvj86378	REP: SVI MAC address flap between the interfaces when the REP is operational.
CSCvk60589	2960L BLK port learn BPDU mac address when using rstp pvst.
CSCvm15295	Snooping table not updated when DHCP snooping is enabled with DHCP relay.
CSCvm21043	cErrDisableIfStatusCause and TimeToRecover could not be get when loopdetect error detected.

Table 13 Caveats Resolved in Cisco IOS Release 15.2(7)E0a

Bug ID	Headline
CSCvm53867	Switch hang up after execute [snmp-server community]&[snmp mib flash cache].
CSCvm93182	High CPU every 10 min by process SFF8472 with 4 SFP.
CSCvn65197	Switch crashes after applying Auto SmartPort Macro configuration on the device.
CSCvn73382	2960-plus QoS \"police rate-bps burst-byte exceed-action drop\" police. Not working as expected.
CSCvo09529	On 2960L 15.2(6)E2, QoS remarking is not working.
CSCvg23885	When a port is errdisabled, the port LED is off.

Related Documentation

- Catalyst 2960-L switch documentation at these URLs:

  http://www.cisco.com/go/2960l
- Cisco SFP and SFP+ modules documentation, including compatibility matrices at this URL:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents at this URL:

  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.