Release Notes for Catalyst 2960-L Series Switches, Cisco IOS Release 15.2(6)E and Later

First Published: Aug 08, 2017

This release note describes the features and caveats for the Cisco IOS Release 15.2(6)E 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 4.
- 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

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

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

Cluster Compatibility

You cannot create and manage switch clusters through Device Manager. To create and manage switch clusters, use the command-line interface (CLI).

When you create a switch cluster or add a switch to a cluster, follow these guidelines:

- We recommend that you configure the highest-end switch in your cluster as the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 2960-L switch, all standby command switches must be Catalyst 2960-L switches.

For additional information about clustering, see the Cisco-enhanced EtherSwitch service module documentation, the software configuration guide, and the command reference.

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.152-6.E.bin	LAN Lite image
Universal image	c2960l-universalk9-mz.152-6.E.tar	LAN Lite cryptographic image with Device Manager.

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 64 active VLANs. The switch models have reduced functionality and scalability with entry level features in Layer 2, and support virtual stacking.

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

- Ease of Operations, page 5
- Network Security, page 5
- Deployment and Control Features, page 6
- Quality of Service, page 7

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 Smart Install, Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:
  - Cisco Smart Install is a transparent plug-and-play technology that can configure the Cisco IOS software image and switch configuration without user intervention. Smart Install uses dynamic IP address allocation and the assistance of other switches to facilitate installation.
  - 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.

- 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.

Quality of Service

- Up to 4 egress queues per port and strict priority queuing, and finer flow segregation using 2 threshold markers for non-strict-priority queues.
- Shared Round Robin (SRR) scheduling to ensure differential prioritization of packet flows.
- Strict priority queuing to ensure that the highest-priority packets are serviced ahead of all other traffic.
- Class maps and policy maps are not supported.

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.

New Software Features

- Features Introduced in Cisco IOS Release 15.2(6)E, page 7

Features Introduced in Cisco IOS Release 15.2(6)E

- Loop Detection: A new method to detect network loops in the absence of Spanning Tree Protocol (STP) is introduced. When an edge switch is connected to an unmanaged switch that does not understand STP or it is part of a network topology where STP is not usable, the loop-detect sub-system sends a frame to the interface, at configured intervals, and detects loops.
- Routing Information Protocol: (LANLite) - RIP is a commonly used routing protocol in small to medium TCP/IP networks. It is supported in both IPv4 and IPv6 network environments.

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

Bug ID	Headline
CSCvf24420	Scale: Failed route reprogramming into tcam hold till the routes expires from CEF RIP
CSCvf42634	Haywards 1G/10G: Jumbo Frames + CRC errors and Runt Frames + CRC errors not incrementing errors

Resolved Caveats

- Caveats Resolved in Cisco IOS Release 15.2(6)E, page 9

Caveats Resolved in Cisco IOS Release 15.2(6)E

Bug ID	Headline
CSCvd36820	Smart Install client feature should auto-disable when not in use
CSCvd37517	CDP will keep sending untagged frames after certain switchport interface configuration order
CSCvd88900	Ping from 2960L failed after Flex-link switchover on peer side
CSCve73535	storm-control can not work when ARP broadcast storm was generated
CSCvd67643	when config dhcpsnooping and didn't include the vlan 1the channel interface has loop
CSCvd66726	2960L: Power not granted again after some period of time under PD is OFF status
CSCvd97247	C2960L: PoE+ negotiation by CDP doesn't work
CSCvd68472	CPU on 2960X pegged at 100% after configuring 'privilege configure level 7 switch'
CSCve09686	C2960L start to count IPG in shaping after seting bandwidth limit
CSCve97401	2960L Ping failed due to MAC aged out at about every 30s if configured port security
CSCve54486	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port
CSCvd88213	Crash while polling cafSessionEntry
CSCva74457	Sticky Interface template not working per requirement
CSCvd13306	"no default-information originate" doesnt work unless "default-information originate" is added first
CSCvb64727	"no ntp allow mode control" does not seem to be working

Bug ID	Headline
CSCva38391	CVE-2016-1550: NTP security against buffer comparison timing attacks
CSCve60467	snmp crash if we remove one of the informs host CLI when traps are pending for that host

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

Obtain Documentation and Submit 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.