



# Release Notes for Catalyst 2960-L Series Switches, Cisco IOS Release 15.2(5)E and Later

---

**First Published: November 28, 2016**

**Last Updated: May 03, 2017**

This release note describes the features and caveats for the Cisco IOS Release 15.2(5)E and later 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

- [Introduction](#), page 2
- [Supported Hardware](#), page 2
- [Device Manager System Requirements](#), page 3
- [Upgrading the Switch Software](#), page 4
- [Features of the Switch](#), page 4
- [Limitations and Restrictions](#), page 7
- [New Software Features](#), page 7
- [Service and Support](#), page 8
- [Caveats](#), page 8



- [Related Documentation, page 10](#)

## 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](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: <ul style="list-style-type: none"> <li>• Mac OS 10.9.5</li> <li>• Microsoft Windows Version 7</li> </ul>
Browser	Cisco CPC can be used with the following browsers: <ul style="list-style-type: none"> <li>• Google Chrome 52 and later</li> <li>• Mozilla Firefox 48 and later</li> <li>• Apple Safari 9 and later</li> <li>• Internet Explorer 11 and later</li> </ul>
Screen Resolution	1280 X 800 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	c29601-universalk9-mz.152-5.E.bin	LAN Lite+ image
Universal image	c29601-universalk9-mz.152-5.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

- MLS QoS provides the ability to configure granular policies and classes on every interface. These policies include policers, markers, and classifiers.
- Up to 4 egress queues per port and strict priority queuing, and finer flow segregation using 2 threshold markers for non-strict-priority queues.
- Weighted Round Robin (WRR) 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.

## Limitations and Restrictions

- The switch does not support routing protocols.
- Effective with Cisco IOS Release 15.2(6)E2, Smart Install feature is not available in Cisco IOS software.
- 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\(5\)E2, page 7](#)
- [Features Introduced in Cisco IOS Release 15.2\(5\)E1, page 8](#)

## Features Introduced in Cisco IOS Release 15.2(5)E2

- Persistent PoE provides uninterrupted power to connected devices even when the switch is booting. See the [Configuring Persistent PoE](#) section in the software configuration guide.
- Support for switch configuration via Bluetooth. See the [Accessing the CLI through Bluetooth](#) section in the software configuration guide.

- Support for GLC-TE transceiver (1 Gigabit SFP).
- Static unicast routing that allow packets moving between a source and a destination to take a user-defined path. See the [Configuring IP Unicast Routing](#) chapter in the software configuration guide.
- Cluster command-switch redundancy. See the [HSRP and Standby Cluster Command Switches](#) section in the software configuration guide.

## Features Introduced in Cisco IOS Release 15.2(5)E1

- Central Web Authentication

# 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](#), page 9
- [Open Caveats](#), page 9
- [Resolved Caveats](#), page 9
- [Related Documentation](#), page 10



## 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
CSCva14843	2960L - Uplink LED doesn't blink with traffic rate
CSCva24214	2960L - Junk characters on reload of switch with Baud other than 115200
CSCva36610	2960L - Downlink LED blink does not reflect the traffic rate
CSCva62862	2960L: Uplink LED doesnt glow amber color for STP blk or for errors
CSCvb37700	Add confirmation check window on submitting day0 configs
CSCvc10240	IOS Crash seen at HAYSEL SISF Process on unconfiguring RA guard policy

## Resolved Caveats

- [Caveats Resolved in Cisco IOS Release 15.2\(5\)E2, page 9](#)
- [Caveats Resolved in Cisco IOS Release 15.2\(5\)E1, page 10](#)
- [Caveats Resolved in Cisco IOS Release 15.2\(5c\)E, page 10](#)
- [Caveats Resolved in Cisco IOS Release 15.2\(5b\)E, page 10](#)

## Caveats Resolved in Cisco IOS Release 15.2(5)E2

No resolved bugs.

## Caveats Resolved in Cisco IOS Release 15.2(5)E1

Bug ID	Headline
CSCuu13476	Cisco IOS & IOS XE Software OpenSSH TCP Denial of Service Vulnerability
CSCux05246	snmpwalk and snmpget have incorrect behavior on IP SLA
CSCuz72344	ip ssh version 2 missing after the reload
CSCva35194	PTF card is crashed while provisioning when all vty sessions exhausted
CSCva37519	stale flowmgr entry during ipv6 tacacs transaction leads to crash
CSCva41556	UI: Unable to apply VLAN configuration changes
CSCvb05793	traffic drop observed upto 2 mins on active Sup pull with ECMP
CSCvb16274	PPTP Start-Control-Connection-Reply packet leaks router memory contents

## Caveats Resolved in Cisco IOS Release 15.2(5c)E

Bug ID	Headline
CSCvb58514	Need to remove FAN control from IOS
CSCvb58527	Temperature values not stable in "show env all"

## Caveats Resolved in Cisco IOS Release 15.2(5b)E

Bug ID	Headline
CSCvb32014	RTC clock setting with IOS and DIAGs out of sync

## 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](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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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.

© 2017 Cisco Systems, Inc. All rights reserved

