Release Notes for Catalyst 2960-X Series Switch, Cisco IOS Release 15.0(2)EX and Later

First Published: June 22, 2013
September 17, 2013
OL-29242-02

This release note describes the features and caveats for the Cisco IOS Release 15.0(2)EX and later software on the Catalyst 2960-X 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 5.

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Catalyst 2960-X 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. Some models of the switches support stacking through the Cisco FlexStack-Plus technology. Unless otherwise noted, the term *switch* refers to both a standalone switch and to a switch stack.

What's New in Release Cisco IOS Release 15.0(2)EX3

- Hibernation—This feature places the switch in ultra low power mode. You can use Cisco EngergyWise management software to schedule the switch to be placed hibernation mode during periods of non-operation, for example, at night and during the weekend.
- Support for switch model Catalyst 2960X-24PSQ-L.

Supported Hardware

Switch Models

Table 1 Catalyst 2960-X Switch Models

Switch Model	Cisco IOS Image	Description
Catalyst 2960X-48FPD-L	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 Power over Ethernet Plus (PoE+) ports (PoE budget of 740 W) and two small form-factor pluggable (SFP)+[1] module slots.
Catalyst 2960X-48LPD-L	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 PoE+ ports (PoE budget of 370 W) and two SFP+ module slots.
Catalyst 2960X-24PD-L	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 PoE+ ports (PoE budget of 370 W) and two SFP+ module slots.
Catalyst 2960X-48TD-L	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 Ethernet ports and two SFP+ module slots.
Catalyst 2960X-24TD-L	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 Ethernet ports and two SFP+ module slots.

Table 1 Catalyst 2960-X Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 2960X-48FPS-L	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 PoE+ (PoE budget of 740 W) and four SFP[2] module slots.
Catalyst 2960X-48LPS-L	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 PoE+ ports (PoE budget of 370 W) and four SFP module slots.
Catalyst 2960X-24PS-L	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 PoE+ ports (PoE budget of 370 W) and four SFP module slots.
Catalyst 2960X-24PSQ-L	LAN Base	Cisco Catalyst 2960-X Non-Stackable, fanless, 24 10/100/1000 Ethernet ports, including 8 POE ports (PoE budget of 110 W), two copper module slots, and two SFP module slots.
Catalyst 2960X-48TS-L	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 Ethernet ports and four SFP module slots.
Catalyst 2960X-24TS-L	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 Ethernet ports and four SFP module slots.
Catalyst 2960X-48TS-LL	LAN Lite	Cisco Catalyst 2960-X 48 10/100/1000 Ethernet ports and two SFP module slots.
Catalyst 2960X-24TS-LL	LAN Lite	Cisco Catalyst 2960-X 24 10/100/1000 Ethernet ports and two SFP module slots.

1. SFP+ = 10-Gigabit uplink.
2. SFP = 1-Gigabit uplink.

Optics Modules

The Catalyst 2960-X 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/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Device Manager System Requirements

Hardware Requirements

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox 1.5, 2.0 or later with JavaScript enabled.

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.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be 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-X switch, all standby command switches must be Catalyst 2960-X 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

Image	Filename	Description
Universal image	c2960x-universalk9-mz.150-2.EX3.bin	LAN Base and LAN Lite images.
Universal image	c2960x-universalk9-tar.150-2.EX3.tar	LAN Base and LAN Lite cryptographic images with Device Manager.

Features

The Catalyst 2960-X switch supports two different feature sets:

- LAN Lite feature set—Provides standard Layer 2 security, quality of service (QoS), and up to 1024 active VLANs. LAN Lite models have reduced functionality and scalability with entry level features in layer 2 and provide no routing capability. They do not support stacking.
- LAN Base feature set—In addition to the LAN Lite feature set, the LAN Base feature set provides more advanced Layer 2 features, extended scalability, routing capability, and support for stacking with FlexStack-Plus.

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

- Ease of Operations, page 5
- Network Security, page 6
- Deployment and Control Features, page 7
- High Availability, page 8
- Quality of Service, page 8

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).
- NetFlow Lite enables monitoring, capturing, and recording of network traffic for further analysis. NetFlow Lite support is available on the LAN Base image.
- Cisco Prime Infrastructure is a set of tools that enables you to automate much of the management of your Cisco network.

Network Security

The Cisco Catalyst 2960-X 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.
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings.
- 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.
- Unicast Reverse Path Forwarding (RPF) feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.
- Cisco security VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs.
- 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, Kerberos, 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.
- System (IDS) to take action when an intruder is detected.
- 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.
- Spanning Tree Root Guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
- IGMP filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.

Deployment and Control Features

- FlexStack-Plus technology creates a resilient single unified system (a stack) of up to eight switches in a homogeneous stack and up to four switches in a mixed stack. With a stack bandwidth of 80 Gbps, the stack functions as a single switching unit that is managed by the stack master. If the stack master fails, a new stack master is elected, keeping the stack operational. The new stack master is elected based on factors such as stack member priority value or lowest MAC address.
- Dynamic Host Configuration Protocol (DHCP) Auto-configuration of multiple switches through a boot server eases switch deployment.
- Automatic QoS (AutoQoS) simplifies QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect Cisco IP phones, classify traffic, and help enable egress queue configuration.
- 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.
- EtherChannel groups to link to another switch, router, or server. The LAN Base image supports up to 24 EtherChannels. In a mixed stack, up to six EtherChannels are supported.
- 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 fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
- Switching Database Manager (SDM) templates allow the administrator to automatically optimize the TCAM memory allocation to the desired features based on deployment-specific requirements.
- Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.
- 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.
- Remote Switch Port Analyzer (RSPAN) allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.

- 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.

High Availability

- Cross-Stack EtherChannel provides the ability to configure Cisco EtherChannel technology across different members of the stack for high resiliency.
- FlexLink provides link redundancy with convergence time less than 100 ms.
- 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. Stacked units behave as a single spanning-tree node.
- Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances.
- Switch-port auto-recovery (error-disable) automatically attempts to reactivate a link that is disabled because of a network error.
- FlexStack-Plus provides switch redundancy.

Quality of Service

- Cross-stack QoS to enable QoS configuration across the entire stack.
- 802.1p class of service (CoS) and differentiated services code point (DSCP) field classification are provided, using marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number.
- Up to eight egress queues per port and strict priority queuing.
- Shaped 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.
- Flow-based rate limiting and up to 256 aggregate or individual policers per port.

Limitations and Restrictions

- Although you can configure up to 1,024 VLANs in a mixed stack configuration where the Catalyst 2960-S is the stack master, configuring more than 255 VLANs can cause the stack master to unexpectedly reload. (CSCue82689)

Caveats

Open Caveats

- CSCue95288

  The **show platform forward** command does not generate the correct output. There is no functional impact.

- CSCug40311

  During POST operations, the LEDs on the front panel do not glow amber.

  There is no workaround.

- CSCuh24740

  When two USB flash devices are inserted into host ports, a traceback is observed. There is no functional impact.

  There is no workaround.

- CSCuh65397

  During the insertion or removal of a power supply, the following message might be displayed on the console:

```
%PLATFORM_ENV-1-FRU_PS_ACCESS: FRU Power Supply is not responding
```

  There is no functional impact. There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)EX3

- CSCud68268

  The Flexible NetFlow options are exported with an ID of zero instead of the IP address of the interface.

  There is no workaround.

- CSCuf87808

  When you use 4-G or 8-G USB memory sticks, the bootloader **dir** command displays a negative value for the number of bytes available. For example:

```
Switch# dir usbflash0:
Directory of usbflash0:/
-297177088 bytes available (4096 bytes used)
```

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)EX1

- CSCuf73324

  The **show platform tcam utilization** command shows that the maximum number of IPv4 multicast routes is 1072 and the maximum number of IPv6 multicast routes is 1072. However, the maximum number of multicast routes that can be configured on the switch is 1072; that is, when a combination of IPv4 and IPv6 multicast routes are configured, the total is limited to 1072.

  There is no workaround.

Documentation Updates

- The *Catalyst 2960-X Switch Hardware Configuration Guide* and the *Catalyst 2960-X Getting Started Guide* erroneously include information about Cisco Network Assistant (CNA). CNA is not supported in this release.
- The *Cisco Smart Install Configuration Guide* includes information about built-in group configuration; however, built-in group configuration is not supported in this release. You can upgrade the Smart Install client using custom group configuration. For more information, see the "Using Custom Groups to Configure Groups Based on Connectivity, MAC Address, Stack Number and Product ID" section of the *Cisco Smart Install Configuration Guide.*

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.

Related Documentation

- Catalyst 2960-X switch documentation at this URL:

  http://www.cisco.com/go/cat2960x_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes 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, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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