



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

First Published: March 7, 2014

Revised: February 19, 2015

This release note describes the features and caveats for the Cisco IOS Release 15.0(2)EX software on the Catalyst 2960-X and the Catalyst 2960-XR 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 6.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Software Image](#)” section on page 7.

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
- [What’s New in Cisco IOS Release 15.0\(2a\)EX5](#), page 2
- [What’s New in Cisco IOS Release 15.0\(2\)EX5](#), page 2
- [What’s New in Cisco IOS Release 15.0\(2\)EX4](#), page 2
- [What’s New in Cisco IOS Release 15.0\(2\)EX3](#), page 2
- [What’s New in Cisco IOS Release 15.0\(2\)EX1](#), page 2
- [What’s New in Cisco IOS Release 15.0\(2\)EX](#), page 3
- [Supported Hardware](#), page 3



- [Device Manager System Requirements, page 5](#)
- [Upgrading the Switch Software, page 6](#)
- [Features, page 7](#)
- [Limitations and Restrictions, page 11](#)
- [Caveats, page 12](#)
- [Documentation Updates, page 16](#)
- [Service and Support, page 16](#)
- [Related Documentation, page 16](#)

Introduction

The Catalyst 2960-X and Catalyst 2960-XR 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 Cisco IOS Release 15.0(2a)EX5

No new features were added.

What's New in Cisco IOS Release 15.0(2)EX5

No new features were added.

What's New in Cisco IOS Release 15.0(2)EX4

No new features were added.

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

Support for the fanless switch model Catalyst 2960X-24PSQ-L.

Hibernation—This feature places the switch in ultra low power mode. You can use Cisco EnergyWise management software to schedule the switch to be placed hibernation mode during periods of non-operation, for example, at night and during the weekend.

What's New in Cisco IOS Release 15.0(2)EX1

First release of the Cisco Catalyst 2960-XR Series Switches support:

- IP Lite Feature Set—In addition to standard LAN Base features, IP Lite provides dynamic routing such as RIP, OSPF routed access, EIGRP stub and other Layer 3 features.
- Optional 8 egress queue support
- ISE Device Sensor

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

First release of the Cisco Catalyst 2960-X Series Switches supporting 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.

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.
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.

Table 1 *Catalyst 2960-X Switch Models (continued)*

Switch Model	Cisco IOS Image	Description
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.

Table 2 *Catalyst 2960-XR Switch Models*

Switch Model	Cisco IOS Image	Description ¹
Catalyst WS-C2960XR-48FPD-I	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 Power over Ethernet Plus (PoE+) ports (PoE budget of 740 W), two small form-factor pluggable (SFP)+ ² module slots, 1025-W power supply.
Catalyst WS-C2960XR-48LPD-I	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 PoE+ ports (PoE budget of 370 W), two SFP+ module slots, 640-W power supply.
Catalyst WS-C2960XR-24PD-I	IP Lite	Cisco Catalyst 2960-XR Stackable 24 10/100/1000 PoE+ ports (PoE budget of 370 W), two SFP+ module slots, 640-W power supply.
Catalyst WS-C2960XR-48TD-I	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 Ethernet ports, two SFP+ module slots, and 250-W power supply.
Catalyst WS-C2960XR-24TD-I	IP Lite	Cisco Catalyst 2960-XR Stackable 24 10/100/1000 Ethernet ports, two SFP+ module slots, and 250-W power supply.
Catalyst WS-C2960XR-48FPS-I	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 PoE+ (PoE budget of 740 W), four SFP ³ module slots, and 1025-W power supply.

Table 2 *Catalyst 2960-XR Switch Models (continued)*

Switch Model	Cisco IOS Image	Description ¹
Catalyst WS-C2960XR-48LPS-I	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 PoE+ ports (PoE budget of 370 W), four SFP module slots, and 640-W power supply.
Catalyst WS-C2960XR-24PS-I	IP Lite	Cisco Catalyst 2960-XR Stackable 24 10/100/1000 PoE+ ports (PoE budget of 370 W), four SFP module slots and 640-W power supply.
Catalyst WS-C2960XR-48TS-I	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 Ethernet ports, four SFP module slots, and 250-W power supply
Catalyst WS-C2960XR-24TS-I	IP Lite	Cisco Catalyst 2960-XR Stackable 24 10/100/1000 Ethernet ports, four SFP module slots, and 250-W power supply.

1. The 250-W power supply is not supported in any PoE switch. The 640-W power supply is not supported in a full PoE switch. If you insert an unsupported power supply, the following error message is displayed: %PLATFORM_ENV-1-FRU_PS_ACCESS: UNKNOWN or UNSUPPORTED Power Supply
2. SFP+ = 10-Gigabit uplink.
3. 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 3 *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 or 7.0, and Firefox up to version 27, 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) or the Network Assistant application.

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 *Getting Started with Cisco Network Assistant, Release Notes for Cisco Network Assistant*, the Cisco-enhanced EtherSwitch service module documentation, the software configuration guide, and the command reference.

CNA Compatibility

For Cisco IOS Release 15.0(2)EX5, CNA support is available on release version 5.8.9 and later.

You can download Cisco Network Assistant from this URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/NetworkAssistant>

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

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 4 *Software Image for Cisco Catalyst 2960-X*

Image	Filename	Description
Universal image	c2960x-universalk9-mz.150-2a.EX5.bin	LAN Base and LAN Lite images.
Universal image	c2960x-universalk9-tar.150-2a.EX5.tar	LAN Base and LAN Lite cryptographic images with Device Manager.

Table 5 *Software Images for Cisco Catalyst 2960-XR*

Image	Filename	Description
Universal image	c2960x-universalk9-mz.150-2a.EX5.bin	IP Lite image.
Universal image	c2960x-universalk9-tar.150-2a.EX5.tar	IP Lite cryptographic image 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 8](#)
- [Network Security, page 8](#)
- [Deployment and Control Features, page 9](#)
- [High Availability, page 10](#)
- [Quality of Service, page 11](#)
- [High Performance Routing \(IP Lite Image\), page 11](#)

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. On the IP Lite image, NetFlow Lite support is available on physical ports configured as either a switch port or a routed port.
- 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.

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 non-subscribers and limits the number of concurrent multicast streams available per port.
- TrustSec uses the Security Group Tag Exchange Protocol (SXP) tags to enable network segmentation through identify based security groups. The SG ACLs enforce network access based on roles enabling companies to scale ACLs across a very large and diverse IT network.
- 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

- 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 up to 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. The IP Lite image supports up to 48 EtherChannels.
- 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

- MLS QoS provides the ability to configure granular policies and classes on every interface. These policies include policers, markers, and classifiers.
- 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.
 - Catalyst 2960-X supports 4 queues with finer flow segregation using three threshold markers for non-strict-priority queues.
 - Catalyst 2960-XR supports 8 queues with finer flow segregation using three threshold markers for non-strict-priority queues.
- 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.

High Performance Routing (IP Lite Image)

- IP unicast routing protocols (Static, Routing Information Protocol Version 1 (RIPv1) and RIPv2) are supported for small-network routing applications.
- Advanced IP unicast routing protocols (OSPF for routed access) are supported for load balancing and constructing scalable LANs. IPv6 routing (OSPFv3) is supported in hardware for maximum performance.
- Equal-cost routing facilitates Layer 3 load balancing and redundancy across the stack.
- Policy-based routing (PBR) allows superior traffic control by providing flow redirection regardless of the routing protocol configured.
- Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) provide dynamic load balancing and failover for routed links.
- Protocol Independent Multicast (PIM) for IP multicast is supported, including PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), PIM sparse-dense mode and Source Specific Multicast (SSM).

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)

- The 250-W power supply is not supported in any PoE switch. The 640-W power supply is not supported in a full PoE switch. If you insert an unsupported power supply, the following error message is displayed:

```
%PLATFORM_ENV-1-FRU_PS_ACCESS: UNKNOWN or UNSUPPORTED Power Supply
```
- The following ACL configurations (**show access-list** command) are displayed only in Cisco IOS releases 15.2(2)E or higher.
 - Extended IP access list CISCO-CWA-URL-REDIRECT-ACL
 - Extended IP access list preauth_ipv4_acl (per-user)
 - IPv6 access list preauth_ipv6_acl (per-user)

Caveats

- [Open Caveats, page 12](#)
- [Caveats Resolved in Cisco IOS Release 15.0\(2a\)EX5, page 13](#)
- [Caveats Resolved in Cisco IOS Release 15.0\(2\)EX5, page 14](#)
- [Caveats Resolved in Cisco IOS Release 15.0\(2\)EX4, page 14](#)
- [Caveats Resolved in Cisco IOS Release 15.0\(2\)EX3, page 15](#)
- [Caveats Resolved in Cisco IOS Release 15.0\(2\)EX1, page 15](#)

Open Caveats

- CSCuc90657
 The **sh inventory** command does not list the 1G SFP.
 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.
- CSCun41300
 Unsetting the stack member numbers and then rebooting the switch stack can cause the stack to crash or cause the stack master election to stop.
 If this occurs, either:
 - Restart the switch stack.
 - Manually assign stack member numbers to all switches in the stack, and then restart the stack.
- CSCuq02930
 The link flaps when no fiber cable is inserted.
 There is no workaround.
- CSCus82139

TDR diagnostics at 10M/100M speed cannot be run on the switch.
There is no workaround. This feature will be supported in a future release.

Caveats Resolved in Cisco IOS Release 15.0(2a)EX5

- CSCug90127

The switch port goes in to the error-disabled state due to port security violations.
The workaround is to run the no switchport command on the interface.

- CSCul78520

When the flex link is configured for the GLC-T interface and the link flaps, the %ENTROPY-0-ENTROPY_ERROR error message is displayed.
There is no workaround.

- CSCum02538

For SFP-10-LRM module installed on Catalyst 6800ia or 2960-X series switches, its version and product ID cannot be read, and the following I2C read failure error message is displayed:
hulc_sfp_iic_intf_read_eeprom sfp _index 0 yeti_iic_read_retry fail
There is no workaround.

- CSCur56395

When GLC-T interfaces or SFPs are plugged into the uplink ports, the member etherchannels go down. The **show idprom** command gives the following error:

```
hulc_sfp_iic_intf_read_eeprom sfp _index 3 yeti_iic_read_retry fail
```

Additionally, device authentication for the stack module fails (with or without ether channel), and the following error is displayed:

```
%ILET-1-DEVICE_AUTHENTICATION_FAIL: The FlexStack Module inserted in this switch may not have been manufactured by Cisco or with Cisco's authorization. If your use of this product is the cause of a support issue, Cisco may deny operation of the product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco's Technical Assistance Center for more information.
```

There is no workaround.



Note During the switch software upgrade, if the error messages continues to be displayed in spite of one or two reboots, a hard reset (unplug the power cord and plug it back in) for the switch stack and RPS may be required once.

- CSCur94280

When GLC-T interfaces are plugged into the uplink ports, the links fail randomly.
The workaround is to use GLC-T SFP in the uplink ports and use 1G fiber SPFs. To recover from the issue, reload the switch.



Note During the switch software upgrade, if the error messages continues to be displayed in spite of one or two reboots, a hard reset (unplug the power cord and plug it back in) for the switch stack and RPS may be required once.

Caveats Resolved in Cisco IOS Release 15.0(2)EX5

- CSCub41348
If all the 4 uplinks of the Catalyst 2960-X switch are connected to a 1G 1000BaseSX SFP module, the CPU is hogged during switch boot and the following message is displayed:

```
hulc_sfp_iic_intf_read_eeprom sfp_index 0 yeti_iic_read_retry fail
```

There is no workaround
- CSCuj46233
On switch model WS-C2960X-24PSQ-L, when the mode button is set to PoE mode (that is, the button is pressed three times), the LED marked SPEED on the front panel glows instead of the LED marked PoE. There is no impact to PoE functionality or to other LED behavior.
- CSCue95288
The **show platform forward** command does not generate the correct output. There is no functional impact.
- CSCul88801
1G or 10G in uplink ports of a Catalyst 2960-X stack may not come up after a reload or OIR of SFP/SFP+.
1G or 10G SFP appear as “unknown” in the output of the **show int status** command.

```
2960X# Show interfaces tel1/0/1 transceiver properties
Diagnostic Monitoring is not implemented.
Name: Tel1/0/1
Administrative Speed: 10000
Administrative Duplex: full
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 10000
Operational Duplex: full
Operational Auto-MDIX: off
Media Type: Not Present<<<<
```

Workarounds:

 - Reload the switch.
 - Downgrade to Cisco IOS Release 15.0(2)EX3.
- CSCum03574
Uplink ports in an EtherChannel on a Catalyst 2960X stack (running Cisco IOS Release 15.0(2)EX4) may go down randomly without error logs.

Workarounds:

 - Reload the Catalyst 2960X stack.
 - Downgrade to Cisco IOS Release 15.0(2)EX3.

Caveats Resolved in Cisco IOS Release 15.0(2)EX4

- CSCtb34814
The following error message is reported just before a crash:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

There may not be any tracebacks given for the crash.

There is no workaround.

- CSCug77751

After a stateful switchover (SSO) on a stack, a member of the stack reloads with an ICC communication failure.

There is no workaround.

- CSCuj70291

When the WS-C2960X-48LPD-L switch model is connected to a Catalyst 4500 switch with WS-X4448-GB-SFP and WS-X4306-GB, the uplink port does not come up. If speed no negotiate is enabled, the link comes up but no traffic passes.

There is no workaround.

- CSCuj74167

Gigabyte link from WS-C2960X-48FPD-L not coming up when using GLC-SX-MM.

There is no workaround.

- CSCsi55685

Kron removes recurring telsh cli after first run.

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 and 2960-XR Switch Hardware Configuration Guide* and the *Catalyst 2960-X and 2960-XR 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 and Catalyst 2960-XR switch documentation at these URLs:
http://www.cisco.com/go/cat2960x_docs
http://www.cisco.com/go/cat2960xr_docs
- 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.

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. 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. (1110R)

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.

© 2015 Cisco Systems, Inc. All rights reserved.

