Release Notes for Catalyst 2960-X and 2960-XR Series Switches, Cisco IOS Release 15.2(3)E and Later

This release note describes the features and caveats for the Cisco IOS Release 15.2(3)E and later 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 5.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Software Image" section on page 6.

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-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 15.2(3)E

Supported Hardware

Switch Models

Table 1   Catalyst 2960-X Switch Models

Switch Model	Cisco IOS Image	Description
Cisco Catalyst 2960X-48FPD-L Switch	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.
Cisco Catalyst 2960X-48LPD-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 PoE+ ports (PoE budget of 370 W) and two SFP+ module slots.
Cisco Catalyst 2960X-24PD-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 PoE+ ports (PoE budget of 370 W) and two SFP+ module slots.
Cisco Catalyst 2960X-48TD-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 Ethernet ports and two SFP+ module slots.
Cisco Catalyst 2960X-24TD-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 Ethernet ports and two SFP+ module slots.
Cisco Catalyst 2960X-48FPS-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 PoE+ (PoE budget of 740 W) and four SFP[2] module slots.
Cisco Catalyst 2960X-48LPS-L Switch	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
Cisco Catalyst 2960X-24PS-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 PoE+ ports (PoE budget of 370 W) and four SFP module slots.
Cisco Catalyst 2960X-24PSQ-L Cool Switch	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.
Cisco Catalyst 2960X-48TS-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 48 10/100/1000 Ethernet ports and four SFP module slots.
Cisco Catalyst 2960X-24TS-L Switch	LAN Base	Cisco Catalyst 2960-X Stackable 24 10/100/1000 Ethernet ports and four SFP module slots.
Cisco Catalyst 2960X-48TS-LL Switch	LAN Lite	Cisco Catalyst 2960-X 48 10/100/1000 Ethernet ports and two SFP module slots.
Cisco Catalyst 2960X-24TS-LL Switch	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]
Cisco Catalyst 2960XR-48FPD-I Switch	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.
Cisco Catalyst 2960XR-48LPD-I Switch	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.
Cisco Catalyst 2960XR-24PD-I Switch	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.
Cisco Catalyst 2960XR-48TD-I Switch	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 Ethernet ports, two SFP+ module slots, and 250-W power supply.
Cisco Catalyst 2960XR-24TD-I	IP Lite	Cisco Catalyst 2960-XR Stackable 24 10/100/1000 Ethernet ports, two SFP+ module slots, and 250-W power supply.
Cisco Catalyst 2960XR-48FPS-I Switch	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 Switch	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.
Cisco Catalyst 2960XR-24PS-I Switch	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.
Cisco Catalyst 2960XR-48TS-I Switch	IP Lite	Cisco Catalyst 2960-XR Stackable 48 10/100/1000 Ethernet ports, four SFP module slots, and 250-W power supply
Cisco Catalyst 2960XR-24TS-I Switch	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, Windows 7, and Windows Server 2003.

- Internet Explorer 6.0, 7.0, Firefox up to version 27.0 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 15.2(2)E, 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/pcgi-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.152-3.E1.bin	LAN Base and LAN Lite images.
Universal image	c2960x-universalk9-tar.152-3.E1.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.152-3.E1.bin	IP Lite image.
Universal image	c2960x-universalk9-tar.152-3.E1.tar	IP Lite cryptographic image with Device Manager.

New Software Features

- Feature Introduced in Cisco IOS Release 15.2(3)E3, page 6
- Features Introduced in Cisco IOS Release 15.2(3)E2, page 7
- Features Introduced in Cisco IOS Release 15.2(3)E1, page 7
- Features Introduced in Cisco IOS Release 15.2(3)E, page 7

Feature Introduced in Cisco IOS Release 15.2(3)E3

What's New	Description
Rapid PVST+	(All licenses) Rapid PVST+ is now the default spanning-tree mode used on all Ethernet port-based VLANs
Enhancement to Smart Install	(All licenses) PnP discovery process via various discovery mechanisms and security methods is supported
Named VLAN	(All licenses) Option to specify a VLAN name for access and voice VLAN.

Features Introduced in Cisco IOS Release 15.2(3)E2

What's New	Description
LACP Rate Fast	Support for the **lacp rate** command, to set the rate at which Link Aggregation Control Packets (LACP) packets are sent to LACP-supported interfaces.

Features Introduced in Cisco IOS Release 15.2(3)E1

What's New	Description
Enhancement to Port Security Configuration	Specify a MAC address that is forbidden by port security on all interfaces.

Features Introduced in Cisco IOS Release 15.2(3)E

What's New	Description
IPv6 First Hop Security support on Etherchannels	The IPv6 FHS policies can be attached to EtherChannel interfaces (Port Channels).
FnF Egress IF Export	New collect field added to flow monitor.
Auto-QoS Compact	This feature hides the auto-QoS-generated commands from the running configuration.
VLAN name extension	Maximum characters allowed for a VLAN name has been increased from 32 to 128.
mDNS Service Discovery Gateway Phase 3	The Service Discovery Gateway feature enables multicast Domain Name System (mDNS) to operate across Layer 3 (L3) boundaries. In this phase, features such as de-congestion of incoming mDNS traffic, redistribution of service withdrawal messages, a filter criterion for learning services available on a specific interface, and the periodic browsing of services on specific interfaces are introduced.
AN Infra	Autonomic networking makes network devices intelligent by introducing self-management concepts that simplify network management for the network operator.

Features of the Switch

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 64 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, and up to 1024 active VLANs

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

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.

- For standalone (non-stacked) setup, up to 8 egress queues per port and strict priority queuing, and finer flow segregation using 3 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
```

- When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may crash. As a workaround, disable the logging discriminator on the device.

- Standalone web-based authentication fails if the switch port is configured without any port ACL. (CSCuu91975)

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
CSCuo55798	Priority Queue Latency increases significantly during congestion
CSCuw10121	Post Fail/Overheat in 2960X while upgrading from 150-2a.EX5 to15.2(3).E2

Caveats Resolved in Cisco IOS Release 15.2(3)E3

Bug ID	Headline
CSCur23262	On removing 8 queue with AQC enabled, will remove the auto qos
CSCut21950	3560 / RBAC / Unable to exclude enable command.
CSCuu16044	3750 - Not Processing LACP PDUs if Native VLAN is not created
CSCuu50798	"%Invalid input detected" display when system booting up on 15.2(3)E1
CSCuu92224	2960X - EPM vlan plugin crash
CSCuu97550	4500X - SNMP dot1dTpFdbPort retuning incorrect value
CSCuv05123	c3560e/v151_sy_throttle platform doesn't store NTP drift values properly
CSCuv32909	3560X crash occurred with %BIT-4-OUTOFRANGE message after doing show run
CSCuv50743	MAC stuck on 'PRE Event Handling' - needs reload for recover
CSCuv53498	"FRU Power Supply is not responding" seen on 2960XR/6800IA
CSCuv88334	mismatch in the rf parameters mode between cli/gui
CSCuw17699	Switch crashes with Data TLB Miss Exception
CSCuw22050	Switch reports Power device detected when non device is connected
CSCuw28638	3650 Rebooting during EAP-TLS authentication
CSCuw39020	access-session vlan-assignment ignore-errors breaks dynamic vlan assign
CSCuw44957	Cat3560X:some fragmented packets drop
CSCuw67734	CFD CSCun37216 entAliasMappingIdentifier broken on 03.07.02E
CSCuw71607	Switch crashed at HLFM aging process
CSCuw71809	There is no warning message when the C3K configures "ip tcp adjust-mss"

Caveats Resolved in Cisco IOS Release 15.2(3)E2

There are no caveats to list here.

Caveats Resolved in Cisco IOS Release 15.2(3)E1

Bug ID	Headline
CSCtg15739	Failed sessions are not removed in multi-auth mode
CSCup27045	Tracebacks are continuously reported, switches inaccessible.
CSCur23413	2960x high cpu and TB seen at ip_adm_sm_delete_proxy_info

Caveats Resolved in Cisco IOS Release 15.2(3)E

Bug ID	Headline
CSCum02538	Version id & Product id blank in "sh int tran fex" o/p for SFP-10-LRM
CSCuo62332	CISCO-BGP-MIBv8.1 - Add support for cbgpPeer2Type in BGP traps/notif
CSCuo66933	Switch sent Failure packet after reboot and caused PC to fail authen
CSCuo67230	2960X is unable to process jumbo frames at CPU
CSCuo73537	Need to remove right-to-use CLI from 2960X
CSCup05881	2960X-usb console connects with mismatched baud rates, occasional crash
CSCup40193	CPU Host-q does randomly does not receive the TCP SYN packets
CSCup52101	EnergyWise Denial of Service vulnerabilty
CSCuq02930	link on WS-C2960X-48LPD-L flaps when using GLC-SX-MM, no fiber cable

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.

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.