Release Notes for Catalyst 2960-X and 2960-XR Series Switches, Cisco IOS Release 15.2(7)Ex

This release note describes the features and caveats for the Cisco IOS Release 15.2(7)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 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://software.cisco.com/download/navigator.html

Contents

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.

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.
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.

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

Switch Model	Cisco IOS Image	Description
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.
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.

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

Switch Model	Cisco IOS Image	Description[1]
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

The following table lists the system requirements for a PC running Cisco Configuration Professional for Catalyst, including Web browser versions.

Table 3　　　　*System Requirements*

System Component	Requirement
Operating System	Any of the following: • Mac OS 10.9.5 • Microsoft Windows Version 7
Browser	Cisco CPC can be used with the following browsers: • Google Chrome 52 and later • Mozilla Firefox 48 and later • Apple Safari 9 and later • Internet Explorer 11 and later
Screen Resolution	1280 X 800 pixels or higher

Cisco Network Assistant Compatibility

For Cisco IOS Release 15.2(7)E, Cisco Network Assistant 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 Images for Cisco Catalyst 2960-X*

Image	Filename	Description
Universal image	c2960x-universalk9-mz.152-7E.bin	LAN Base and LAN Lite images.
Universal image	c2960x-universalk9-tar.152-7E.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	c2960xr-universalk9-mz.152-7E.bin	IP Lite image.
Universal image	c2960xr-universalk9-tar.152-7E.tar	IP Lite cryptographic image with Device Manager.

Guidelines for Upgrade

Before you upgrade to Cisco IOS Release 15.2(7)E3, ensure the following:

- Remove the **tacacs-server** command configurations using the **no** form of the command.
- Configure the TACACS Server using the new **tacacs server** command.
- If the TACACS group server is configured using the server-private CLI, unconfigure the private server and configure a public server using the **server name** *name* command.

Web UI

If the Web UI does not load or work properly after the software upgrade, perform the following steps:

Step 1   Specify the authentication method for HTTP server users as local.

Device(config)# **ip http authentication local**

Step 2   Configure the username and password with privilege 15.

Device(config)# **username** *user* **privilege 15 password** *password*

Step 3   Clear the browser cache and relaunch the Web UI.

Step 4   Login by entering the privilege 15 username and password.

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, page 7

- Network Security, page 7

- Deployment and Control Features, page 9

- High Availability, page 10

- Quality of Service, page 10

- High Performance Routing (IP Lite Image), page 10

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 Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:

  - 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).

- Flexible NetFlow enables monitoring, capturing, and recording of network traffic for further analysis. Flexible NetFlow support is available with Cisco ONE for Access or DNA Essentials license on Catalyst 2960-X and 2960-XR Series Switches.

- 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.

- In Cisco IOS Release 15.2(7)E3 and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.

- 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 identity-based security groups.

- 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 active switch. If the active switch fails, a new active switch is elected, keeping the stack operational. The new active switch 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) provides 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)

- In a stackable switch, if the VRF configuration is changed and this is followed by a master switchover, the VRF stops working. The workaround is to reload the switch stack after the VRF configuration is changed. (CSCtn71151)

- 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)

- TACACS Server legacy command: Do not use the legacy **tacacs-server** command; this command is deprecated. If the software running on your device is Cisco IOS Release 15.2(7)E3 or later, using the legacy command can cause authentication failures. Use the **tacacs server** command.

New Software Features

Features Introduced in Cisco IOS Release 15.2(7)E10

None.

Features Introduced in Cisco IOS Release 15.2(7)E9

None.

Features Introduced in Cisco IOS Release 15.2(7)E8

None.

Features Introduced in Cisco IOS Release 15.2(7)E7

Data Sanitization: Supports the use of the National Institute of Standards and Technology (NIST) purge method that renders data unrecoverable through simple, non-invasive data recovery techniques or through state-of-the-art laboratory techniques.

For more information, see the Data Sanitization chapter of the System Management Configuration Guide.

Features Introduced in Cisco IOS Release 15.2(7)E6

None

Features Introduced in Cisco IOS Release 15.2(7)E5

None

Features Introduced in Cisco IOS Release 15.2(7)E4

None.

Features Introduced in Cisco IOS Release 15.2(7)E3

Support for Type 6 AES Encryption password: Beginning with this release, you can specify a Type 6 encrypted key for a TACACS Server. The new command is **tacacs server key 6** *key-name.*

Note   Before downgrading from Cisco IOS Release 15.2(7)E3 to an earlier release, ensure that Type 6 encryption is removed from the TACACS Server. (Type 6 encryption is not supported in releases earlier than Cisco IOS Release 15.2(7)E3.)

Features Introduced in Cisco IOS Release 15.2(7)E2

None.

Features Introduced in Cisco IOS Release 15.2(7)E1a

None.

Features Introduced in Cisco IOS Release 15.2(7)E1

AEP MAC Move: New command **authentication mac-move deny-uncontrolled** command is introduced to disable MAC move from a secure port to an unsecured port.

Features Introduced in Cisco IOS Release 15.2(7)E0a

- IPv6 *d*ACL: Supports IPv6 downloadable ACLs (*d*ACL) for authentication and authorization into the network for end-point clients or devices. Cisco Identity Services Engine (ISE) pushed the *d*ACL to the switch or controller, which in turn attaches it with the end-point.

- Loop Detection: A new method to detect network loops in the absence of Spanning Tree Protocol (STP) is introduced. When an edge switch is connected to an unmanaged switch that does not understand STP or it is part of a network topology where STP is not usable, the loop-detect sub-system sends a frame to the interface, at configured intervals, and detects loops.

- SFTP: The device supports SSH File Transfer Protocol (SFTP). The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device. Therefore, any SFTP server user with the appropriate permission can copy files to and from the device.

- Private VLAN (PVLAN) support for Multicast Traffic: Multicast traffic is routed or bridged across PVLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

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

None.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.2(7)E10

Table 6   *Caveats Resolved in Cisco IOS Release 15.2(7)E10*

Bug ID	Headline
CSCwh96519	For PoE used and remaining power on 3560, the SNMP walk result is showing inaccurate data
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerability

\Caveats Resolved in Cisco IOS Release 15.2(7)E9

Table 7   *Caveats Resolved in Cisco IOS Release 15.2(7)E9*

Bug ID	Headline
CSCwe56212	Voice VLAN of port configuration is used despite successful MAB
CSCwe93545	Stack of C2960XR able to provide FAN status via CLI but not via SNMP
CSCwf06443	AAA configuration non persisting across reloads for VTY line 0-4 on IOS platform
CSCwf33438	Crash, when psecurity is disabled followed by mac add static mac vlan 600 drop, psecurity enabled

Caveats Resolved in Cisco IOS Release 15.2(7)E8

Table 8   *Caveats Resolved in Cisco IOS Release 15.2(7)E8*

Bug ID	Headline
CSCwd48815	Crash with mac address-table static <MAC address that is flapping> vlan <> drop and mac flapping.

Caveats Resolved in Cisco IOS Release 15.2(7)E7

Table 9   *Caveats Resolved in Cisco IOS Release 15.2(7)E7*

Bug ID	Headline
CSCwb29375	The switch suddenly change the access VLAN on random access interfaces to vlan1.
CSCwc10457	2960x Auto SmartPort Macro not being triggered in version 15.2(7)E6.
CSCwc25988	C2960X EEE Enabled (ASIC) status on stack member shows [no].
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvx63027	Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability.
CSCwa96810	Cisco IOS and IOS XE Software Common Industrial Protocol Request Denial of Service Vulnerability.

Caveats Resolved in Cisco IOS Release 15.2(7)E6

Table 10   *Caveats Resolved in Cisco IOS Release 15.2(7)E6*

Bug ID	Headline
CSCvw57338	Switch memory leak in auth manager process.
CSCwa24812	PnP does not work with PnP startup VLAN and native VLAN configured on the trunk.
CSCwa07503	MAC address of 3rd Party IP phone is not learned on the Voice VLAN.
CSCvy72006	DHCP Release is sent during the on-boarding IE4000 with the IP address in use in Cisco DNA IE4000.

Table 10   *Caveats Resolved in Cisco IOS Release 15.2(7)E6*

Bug ID	Headline
CSCvz20347	Device classifier config appears in the **show running-config** command output after the primary device is powered off.
CSCvz25717	Connectivity loss while changing VLAN configuration under interface with port security configuration.

Caveats Resolved in Cisco IOS Release 15.2(7)E5

Table 11   *Caveats Resolved in Cisco IOS Release 15.2(7)E5*

Bug ID	Headline
CSCvx02979	C9120AX wireless access point identified incorrectly by device classifier on Cisco switches.
CSCvx77146	The 'no power efficient-ethernet' command disappeared from the shutdown port on Cat2960x stack.
CSCvy00869	2960x RPS LED colors in 15.2(7)E1 and 15.2(7)E3,15.2(7)E4 are different.
CSCvy51254	Ports on member switches do not trigger a re-auth after Radius server is marked alive.
CSCvy53541	2960X: Member switch is crashing on booting up in stack when ipv6 MLD snooping is enabled.
CSCvy61119	Radius-accounting packets are sent with an empty TLV6 empty string (device description) for APs.
CSCvz07394	2960X Stack may observe hang/freeze of member switches or complete stack.
CSCvz15759	2960X:10G fiber trunk fails to fwd all VLAN Mcast groups.
CSCvz15816	No SNMP tranceiver values after restart of a stackmember.
CSCvx76066	Switch crashes due to "HTTP Core".
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability.

Caveats Resolved in Cisco IOS Release 15.2(7)E4

Table 12   *Caveats Resolved in Cisco IOS Release 15.2(7)E4*

Bug ID	Headline
CSCvv17507	Switch May Crash at hpm_hwidb_to_gid.
CSCvv94988	Crash on member switch during client authentication using Dynamic VLAN assignment.
CSCvv86851	TACACS not working if TACACS group server has "server-private <ip> key <passw>" in 15.2(7)E3/3.11.3E.
CSCvv93417	Stack Member Switch fails wired dot1x; MasterSwitch passes dot1x using the same configs.
CSCvv72181	Peer side interface down/up once during 2960XR reload.
CSCvs87822	Member switches randomly reloads due to EPM/Auth process.
CSCvv14451	2960X Member Switches Lose Device Classifier, Breaking Auto Smart Ports (ASP).
CSCvv57812	PnP agent / HTTP Client does not try to reconnect to Cisco DNA Center after a connectivity loss.
CSCvx20933	2960X || Misbehavior for TVL6 and TLV127.

Caveats Resolved in Cisco IOS Release 15.2(7)E3

Table 13   *Caveats Resolved in Cisco IOS Release 15.2(7)E3*

Bug ID	Headline
CSCvp22976	2960x: Downlink ports do not come up with 152(7)E image in 2960x boards with Hw rev 12.
CSCvt58384	ARP packets in RSPAN vlan are punted to CPU.
CSCvt16716	IPv6 source guard feature is broken on 15.2(7)Ex.
CSCvt79105	WS-C2960X-24PSQ-L: Link up issues on all data ports (9-24) post upgrade to 15.2(7).
CSCvt88440	SPAN on 2960X stack configured with horizontal stacking is not working as expected.
CSCvt38789	access-map added after reload active switch.
CSCvu10399	Cisco IOS and IOS XE Software Information Disclosure Vulnerability.
CSCvv00134	VTY telnet disable, enable ssh based on platform request.

Caveats Resolved in Cisco IOS Release 15.2(7)E2

Table 14   Caveats Resolved in Cisco IOS Release 15.2(7)E2

Bug ID	Headline
CSCvt19077	AAA configurations are missing after reload.
CSCvq91578	IPDT doesn't trigger the inactivity timer.
CSCvq98433	SNMPv3 In the 2960X stack, Engineboots and Enginetime will not be sync after switchover.
CSCvr75372	C2960XR IRPS led color become amber blinking when plug one PS's cable.

Caveats Resolved in Cisco IOS Release 15.2(7)E1a

Table 15   Caveats Resolved in Cisco IOS Release 15.2(7)E1a

Bug ID	Headline
CSCvi48253	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, can't be created after that time.

Caveats Resolved in Cisco IOS Release 15.2(7)E1

Table 16   Resolved Caveats for Cisco IOS Release 15.2(7)E1

Bug ID	Headline
CSCvp74289	dot1x client connected to member port not getting assigned with DHCP address.
CSCvq95676	switch crashes @ dot1x_switch_port_vp_unauthorized.
CSCvo38551	Applying user-defined interface template on a member port causes switch stack members to reboot.
CSCvm56063	Switch loses mac on dynamic access ports (tracebacks seen related to VMPS/VQP).
CSCvo98614	Unknown Status for Duplex-Status OID (1.3.6.1.2.1.10.7.2.1.19) on C2960 platforms.
CSCvp33840	FHS is allowing ADV and REP packets from fake DHCPv6 server when source udp port is not 547.
CSCvq44967	C2960X PoE Status LED black instead of amber.
CSCvq48101	storm-control config mismatch on channel and member interface.
CSCvh01607	sh power inline <port> detail doesn't show member port lldp power nego information.
CSCvr57005	2960XR Flow-based SPAN(FSPAN) not work when mutilple session configured.

Caveats Resolved in Cisco IOS Release 15.2(7)E0a

Table 17   Resolved Caveats for Cisco IOS Release 15.2(7)E0a

Bug ID	Headline
CSCvp22976	Catalyst 2960x: Downlink ports do not come up with 152(7)E image in 2960x boards with Hw rev 12.
CSCvk25949	Setting interface: spanning-tree portfast through snmp is not working.
CSCvm56063	Switch loses mac on dynamic access ports (tracebacks seen related to VMPS/VQP).
CSCvm87761	Logging persistent doesn't work for 2960 XR running 15.2.2E(7).
CSCvn15198	Native VLAN not going to FWD when template applied.
CSCvn37402	2960L hung up suddenly without any syslog output.
CSCvj04880	End Client not re-authenticated after RADIUS server marked ALIVE.
CSCvn65197	Switch crashes after applying Auto SmartPort Macro configuration on the device.
CSCvn73382	2960-plus QoS \"police rate-bps burst-byte exceed-action drop\" police Not worked expected.

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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