Release Notes for Catalyst 2960-X and 2960-XR Series Switches, Cisco IOS Release 15.2(2)E and Later

First Published: June 27, 2014
Last Published: May 31, 2019

OL-32568-01

This release note describes the features and caveats for the Cisco IOS Release 15.2(2)E 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.

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.

Table 1 Catalyst 2960-X Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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

- Before upgrading to Cisco IOS XE Release 3.6.6E, you need to upgrade the Prime Infrastructure software to Release 3.1.4 with Device Pack(DP) 6.

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.152-2.E2.bin	LAN Base and LAN Lite images.
Universal image	c2960x-universalk9-tar.152-2.E2.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.152-2.E2.bin	IP Lite image.
Universal image	c2960x-universalk9-tar.152-2.E2.tar	IP Lite cryptographic image with Device Manager.

New Software Features

Note Catalyst 2960-X supports LAN Lite and LAN Base images, and Catalyst 2960XR supports only IP Lite image.

Features Introduced in Cisco IOS Release 15.2(2)E10

- No new features were introduced.

Features Introduced in Cisco IOS Release 15.2(2)E8

- No new features were introduced.

Features Introduced in Cisco IOS Release 15.2(2)E7

- No new features were introduced.

Features Introduced in Cisco IOS Release 15.2(2)E6

- No new features were introduced.

Features Introduced in Cisco IOS Release 15.2(2)E5a

- No new features were introduced.

Features Introduced in Cisco IOS Release 15.2(2)E5

- No new features were introduced.

Features Introduced in Cisco IOS Release 15.2(2)E4

- No new features were introduced.

Featured Introduces in Cisco IOS Release 15.2(2)E3

What's New	Description
Policy-Based Routing(PBR) using Object Tracking	(Catalyst 2960-XR | IP Lite) Provides the capability to configure Policy-Based Routing(PBR) to use object tracking to verify the reachability of the next-hop IP address to which to forward packets, using an Internet Control Message Protocol(ICMP) ping as the verification method.

Features Introduced in Cisco IOS Release 15.2(2)E

What's New	Description
Cisco IOS XE Release 3E Documentation Roadmap Cisco IOS Release 15E Documentation Roadmap	Provides quick and easy access to all relevant documentation for specific platforms. Look for *Quick Links to Platform Documentation* on the respective platform documentation pages.
Integrated Documentation Guides	Provides platform and software documentation for two technologies: • IP Multicast Routing Configuration Guide • Cisco Flexible Netflow Configuration Guide
SMI Post-install	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Eliminates the overhead of manual post install configuration on all the switches, in the smart install network.
Auto Security	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Provides a single line CLI, to enable base line security features (Port Security, DHCP snooping, DAI)
EIGRPv6 stub routing & PIMv6 stub routing	(Catalyst 2960-XR | IP Lite) Support for EIGRP IPv6 stub routing and PIM IPv6 stub routing.
IPv6 Static Route support for Object Tracking	(Catalyst 2960-XR | IP Lite) Allows an IPv6 Static Route to be associated with a tracked-object.
Open Plug-N-Play Agent	(Catalyst 2960-X | LAN Lite and LAN Base, and 2960-XR | IP Lite) Switch based agent support for zero touch automated device installation solution called NG-PNP.
HSRP: Global IPv6 Address	(Catalyst 2960-XR | IP Lite) Allows users to configure multiple non-link local addresses as virtual addresses. The Hot Standby Router Protocol (HSRP) ensures host-to-router resilience and failover, in case the path between a host and the first-hop router fails, or the first-hop router itself fails.
Banner Page and Inactivity timeout for HTTP/S connections	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Allows you to create a banner page and set an inactivity timeout for HTTP or HTTP Secure (HTTPS) connections. The banner page allows you to logon to the server when the session is invalid or expired.
Secure CDP	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Allows you to select the type, length, value (TLV) fields that are sent on a particular interface to filter information sent through Cisco Discovery Protocol packets.
FQDN ACL	(Catalyst 2960-X | LAN Base, 2960-XR | IP Lite) Helps to resolve the destination domain name to an IP address, which is provided to the client as a part of the domain name system (DNS) response.
Web Authentication Redirection to Original URL	(Catalyst 2960-X | LAN Base, 2960-XR | IP Lite) Enables networks to redirect guest users to the URL they had originally requested. This feature is enabled by default and requires no configuration.
Auto conf	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Determines the level of network access provided to an endpoint based on the type of the endpoint device. This feature also permits hardbinding between the end device and the interface. Autoconfig falls under the umbrella of Smart Operations solution.

What's New	Description
Interface templates	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Provides a mechanism to configure multiple commands at the same time and associate it with a target such as an interface. An interface template is a container of configurations or policies that can be applied to specific ports.
FIPS/CC Compliance for NMSP	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Enables strong ciphers for new NMSP connections. The existing NMSP connections will use the default cipher.
8 Egress Queue Support	(Catalyst 2960-X | LAN Base) By default 4 egress queues are supported. This feature provides the flexibility to configure 8 egress queues on standalone only.
Support for Cisco SFP+ Active Optical Cables	(Catalyst 2960-X | LAN Base, 2960-XR | IP Lite) Support for Cisco SFP+ Active Optical Cables - Cisco SFP-10G-AOC1M Cisco SFP-10G-AOC2M Cisco SFP-10G-AOC3M, Cisco SFP-10G-AOC5M, Cisco SFP-10G-AOC7M, Cisco SFP-10G-AOC10. For a list of all supported SFP+ modules, see http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html.
Multi-auth per user VLAN assignment	(Catalyst 2960-X | LAN Base, 2960-XR | IP Lite) Support for Multi-auth per user VLAN assignment.
Auto QoS with 8 Egress Queues	(Catalyst 2960-X | LAN Lite and LAN Base, 2960-XR | IP Lite) Auto QoS is supported with 8 egress queues configuration in standalone only.
ISE Device Sensor	(Catalyst 2960-X | LAN Base, 2960-XR | IP Lite) Support for ISE Device Sensor.

Note **Device Classifier** has been disabled by default starting from Release 15.2(2)E. Any features dependent on device classifier should enable it if required.

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. It supports upto 1024 active VLANs.

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

- Ease of Operations, page 10
- Network Security, page 10
- Deployment and Control Features, page 11
- High Availability, page 12
- Quality of Service, page 13
- High Performance Routing (IP Lite Image), page 13

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 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 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 can support the option to configure 8 egress queues on standalone only. By default it supports 4 egress 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 for routed access) 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

- Effective with Cisco IOS Release 15.2(2)E9, Smart Install feature is not available in Cisco IOS software.
- 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 VRF configuration is changed and this is followed by a master switchover, 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
  ```

Note **Device Classifier** has been disabled by default starting from Release 15.2(2)E. Any features dependent on device classifier should enable it if required.

- 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.
- We recommend that you configure the **access-session interface-template sticky timer** *timer-value* command at the global or interface configuration mode, and not within the template.

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
CSCve85181	FNF Flow exporter source interface is not synchronized across switch stack members.

Caveats Resolved in Cisco IOS Release 15.2(2)E10

Bug ID	Headline
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"

Caveats Resolved in Cisco IOS Release 15.2(2)E9

Bug ID	Headline
CSCvk42571	Redirect to external url fails after PC restart/reboot
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"
CSCvo09436	Active supervisor crashing while DFE training on Standby SUP
CSCvp19855	Crash when removing police action from policy-map
CSCvf42171	Multiple Ports on a C2960X / C2960XR Stack stops providing PoE

Bug ID	Headline
CSCvb59372	Double-free of VTY context causes a software-forced crash
CSCvd78456	Span config lost after reboot when using interface ranges
CSCvd79623	Random SNMP OID missing
CSCvd96099	DOT1X %DATACORRUPTION-1-DATAINCONSISTENCY: copy error session_mgr
CSCve53124	Stack blocks ARP req after port flap when Port security enabled with DHCP Snooping
CSCvg79459	Automate-tester does not send probes when the server is dead.
CSCvh69914	after multiple reloads stack stops processing BPDUs and claims to be root
CSCvh89534	DACL applied to the incorrect interface
CSCvj25236	IPDT flapping after upgrade
CSCvj29126	RADIUS client on network fails to solicit PAC key from CTS even though the device has a valid PAC
CSCvf24186	Catalyst 2960X- Switch failed to boot with IOS version 152-2.E5 and 15.2(4)E4

Caveats Resolved in Cisco IOS Release 15.2(2)E8

Bug ID	Headline
CSCux72245	"CISCO-CWA-URL-REDIRECT-ACL" displayed in show run.
CSCva83873	2960-X-:POST: Failed PortMacLoopback- in 2960-X.
CSCvd23231	VTP_INVALID_DATABASE_DATA, TRACEBACK=82A1C4z 2CEEA50z 2CFC2D4z.
CSCve54486	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port.
CSCve37498	Switch sends duplicate accounting message, that causing ISE to generate Misconfigured NAS Alarms.
CSCvf18046	sticky timer stops if connected device moved from one port to other within timer expiry.
CSCvf76512	Option 82 circuit-id-tag restricted by 6 bytes.

Caveats Resolved in Cisco IOS Release 15.2(2)E7

Bug ID	Headline
CSCty18171	SNMP poll of CISCO-PROCESS-MIB may cause high CPU and SNMP poll timeout.
CSCut33013	3750X linkdown occur by reloading 2960X.
CSCuv22571	Memory corruption crash in slaJitterPacketBuild.
CSCuw15256	IOS PKI: Certificate validation fails after reload.
CSCvb47673	SYS-2-MALLOCFAIL- Traceback and Crash observed in 2k stack.
CSCvc84352	IP Phone connectivity loss with dynamically assigned vlan and MDA.
CSCvd01598	Tacacs+ Timeout Retransmission is done 3 times prior marking server down.
CSCvd35291	Removal of "access-session template monitor" creates Drop MAC entries in CAM table.
CSCve04704	Session blocked in Pending Deletion state due to SM Accounting Feature.
CSCve48844	Multicast packet drops due to IGMP snooping-q handler on 2960X.

Caveats Resolved in Cisco IOS Release 15.2(2)E6

Bug ID	Headline
CSCuz30314	Memory leak in DSensor Cache PROTO and epm authz_sess_info.
CSCuq91509	2960X/XR: Hibernation can not be configured for overnight period.
CSCuw72963	Ethernet link issue between C2960X and 3rd party terminal counter.
CSCuz24063	Storm-control configured on port-channel cannot reflect to member link.
CSCuz92903	Unpowered IP Phone may bring switchport up at 10M on non-PoE switch.
CSCva40478	IP DHCP snooping trust on port-channel does not reflect on member link.

Caveats Resolved in Cisco IOS Release 15.2(2)E5a

Bug ID	Headline
CSCuv87976	CLI Knob for handling Leap second add/delete ignore/ handle
CSCvb29204	BenignCertain on IOS and IOS-XE

Caveats Resolved in Cisco IOS Release 15.2(2)E5

Bug ID	Headline
CSCuw91320	(Catalyst 2960-X) Ports 1,9,17,25,33,41 of Catalyst 2960x do not link up with ws-4424-GB-rj45
CSCuy19990	IOS 15.2 802.1x critical vlan feature - reinitialize is not working

Bug ID	Headline
CSCux38041	Broadcast packet does not send when port channel changes to normal port
CSCuy19327	Template gets applied/removed continuously when we connect laptop
CSCuy56741	(Catalyst 2960-X) Vlan information does not reflect under port-channel member physical interface
CSCuv12898	(Catalyst 2960-X) Catalyst 2960x crashes executing list of "show" commands through monitoring tool
CSCuv48097	(Catalyst 2960-X) Catalyst 2960x with 15.2.3e1 intermittently failing to start MAB authentication

Caveats Resolved in Cisco IOS Release 15.2(2)E4

Bug ID	Headline
CSCuj81067	Memory leak in crypto_create_pkcs7_msg
CSCum41167	Importing multipath routes changes next-hop to 0.0.0.0 and traffic fails
CSCuq36627	WAAS Express:Failed to create SSL session. (no available resources)
CSCuq46932	Crash on dhcpd_find_binding_by_hw
CSCur28336	Memory leak and possible crash when using a logging discriminator
CSCur45606	Logging discriminator does not work
CSCuu21448	ISIS Metric with Multiple instances using ciiCircLevelMetric OID
CSCuv23475	CPUHOG and crash on "no network 0.0.0.0" with vnet configuration on intf
CSCuv31135	Disable connected-check in one side only makes route as unreachable
CSCuw52729	Enabling auto qos causes "line vty 0 4" length set to 0
CSCuw73525	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr
CSCut53599	(Catalyst 2960X) C2960X/6800ia RPS is not functioning correctly, reports "RPS is not responding"
CSCuv32827	(Catalyst 2960X) Stack crashes @epm_vlan_group_feature_ctx_delete
CSCuv34333	(Catalyst 2960X) PXE boot does not obtain DHCP Lease when POE is enabled
CSCuv39850	Switch crashes @auth_mgr_show_method_status_list
CSCuv53498	"FRU Power Supply is not responding" seen on 2960XR/6800IA
CSCuw02593	%SFF8472-5-THRESHOLD_VIOLATION on 3750X sfp port even no cable inserted
CSCuw71607	Switch crashed at HLFM aging process
CSCuw79229	(Catalyst 2960X) 2960X with mab : IP Phone call drops when PC goes to sleep or resets
CSCuo93205	Enable SSL Server Identity Check during SSL handshake

Caveats Resolved in Cisco IOS Release 15.2(2)E3

Bug ID	Description
CSCui35423	DHCP bindings are not happening at first try
CSCuj31600	Call Home causes stack member crash
CSCul30895	Syslog messages not generated for BFD neighbor up/down events
CSCul73513	Server-client clock not in sync after leap configuration
CSCum17258	EPM_SESS_ERR: Error in activating feature (EPM ACL PLUG-IN)
CSCum65703	Inconsistency on configuration "privilege" commands as seen in running-config
CSCun14713	Create new accounting session whenever the principal identity changes
CSCup66629	Traceback @psecure_platform_delete_all_addrs on executing neg events
CSCup81878	Line by Line Sync fail while deleting dynamic NTP peer
CSCuq99943	Watchdog Exception for hulc/sisf component
CSCur09175	IPDT is turned on automatically even when dot1x configs are disabled
CSCur11439	Energywise Activitycheck powers off phone during an active call
CSCur58372	"snmp-server enable traps syslog" shows in "show run all" output after removal
CSCur59242	Crash due to tplus_client_stop_timer
CSCur86947	dummy mcast pkt is not sent out when hsrp mac is there in mac-table
CSCus09761	IOS-Phone not placed in critical voice VLAN when AAA server is unreached
CSCus13476	CSR handled only one MACSec interface's authentication
CSCus13924	Device crashes while configuring 'Identity' commands
CSCus47009	Switch does not increment the "Received on untrusted ports" DHCP counter
CSCus79132	Dot1x authentication legacy behaviour broken
CSCus84744	(2960-XR) PBR verify-availability support on C3750x
CSCut05808	UDP(1975) causes Error msg %IPC-2-INVALIDZONE
CSCut10251	Some commands are not in running-config after AUTOINSTALL finishes
CSCut13064	BPDU filter does not work on output port when STP is disabled
CSCut13458	Specific packet will be forwarded when injected into flexlink backup I/F
CSCut13753	ACLs not syncing to the member switches on stack reload or member reload
CSCut16234	High CPU every 10min by process SFF8472
CSCut20271	C3560X response ARP request from management port
CSCut27272	CPUHOG and crash due to Auth Manager process
CSCut52693	(2960-XR) PBR not routing to default route when next-hop is down
CSCut64257	(2960-X) 2960X System clock gains xx hours after second reload
CSCut68786	PoE inline power denied between WS-C3560CPD and AP1600.
CSCut79680	ip default-gateway is not seen in running-config after AUTOINSTALL
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCut90593	(2960-X) 2960X crash during boot up with Error: ASIC/PHY POST failed

Bug ID	Description
CSCuu16044	3750 - Not Processing LACP PDUs if Native VLAN is not created
CSCuu22144	Vlan1 IP apply method inconsistencies across Static / DHCP / TFTP
CSCuu40796	(2960-XR) "FAN is not present" message when system boots up
CSCuu42684	nas-port attribute hardcoded to 60000
CSCuu50392	Auth Manager memory leak with ISE authentication
CSCuu69332	(2960-X) Frame with special DesMac is forwarded by STP block port
CSCuu82134	IBC:VSS-Predator: Active Predator went SMI upgrade but not standby
CSCuu90639	IP address is missing by end of Autoinstall
CSCuu92224	(2960X) 2960X - EPM vlan plugin crash
CSCuu97116	Acct messages should include Class attribute from authentication
CSCuv06451	IOSd crash in eap_auth_terminal_state calling free_internal
CSCuv19258	DACL may not work under IBNS 2.0

Caveats Resolved in Cisco IOS Release 15.2(2)E2

Bug ID	Headline
CSCuo71145	Standby VSS switch crashes when configuring flow exporter
CSCup27045	Tracebacks are continuously reported, switches inaccessible
CSCur05027	(2960X) Loopback error occurs when keepalive packet is looped back to the port
CSCur20444	I/O memory leak due to DHCPv6 packets
CSCur20551	(2960X) Increase OutDiscards counter when one side of stack switch is reloaded
CSCur21080	SMI director does not support WS-C2960CX-8PC-L as client
CSCur48634	HA fails due to Bulk synch failure with encrypted password
CSCur74702	Wrong SMI vstack group selected due to incorrect client MAC matched
CSCur91360	dot1x identity VLAN log messages are missing
CSCur94280	2960x/6800IA: Link may go down randomly with GLC-T in uplink ports
CSCus09761	IOS-Phone not placed in critical voice VLAN when AAA server is unreached
CSCus40606	802.1x Guest Vlan user cannot receive IP address on non-master switches
CSCus75890	Switch does not resync to NTP server after clock set command or reload

Caveats Resolved in Cisco IOS Release 15.2(2)E1

Bug ID	Headline
CSCum47115	EtherType 888e unicast can not pass 2960 with new releases
CSCun80959	Desg port on the RootBridge experienced block forward for 30 sec
CSCun84283	(2960-X) C2960 || Copper connection interfaces || Keepalive set by default

Bug ID	Headline
CSCuo67230	(2960-X) 2960X is unable to process jumbo frames at CPU
CSCup05881	(2960-X) 2960X-usb console connects with mismatched baud rates, occasional crash
CSCup40193	(2960-XR) CPU Host-q does randomly does not receive the TCP SYN packets
CSCup96299	IPv6 Multicast RIB entry refer to wrong distance
CSCuq02930	Link on WS-C2960X-48LPD-L flaps when using GLC-SX-MM, no fiber cable
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCur00722	Hard Reset of the Active Sup cause switch to power cycle

Caveats Resolved in Cisco IOS Release 15.2(2)E

Bug ID	Headline
CSCun41300	8-member stack does not boot up

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

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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