Release Notes for Catalyst 2960-X and 2960-XR Series Switches, Cisco IOS Release 15.2(4)E and Later

First Published: 01 October, 2015
Last Updated: Apr 07, 2020

This release note describes the features and caveats for the Cisco IOS Release 15.2(4)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.

What's New in Cisco IOS Release 15.2(4)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.
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(4)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.152-4.bin	LAN Base and LAN Lite images.
Universal image	c2960x-universalk9-tar.152-4.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.152-4.bin	IP Lite image.
Universal image	c2960x-universalk9-tar.152-4.tar	IP Lite cryptographic image with Device Manager.

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 6
- Network Security, page 7
- Deployment and Control Features, page 8
- High Availability, page 9
- Quality of Service, page 9
- 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 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.
- 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)
- 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)

New Software Features

Features Introduced in Cisco IOS Release 15.2(4)E10

- There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E9

- There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E8

- There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E7

- There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E6

- There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E5

There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E4

There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E3

There are no new features in this release.

Features Introduced in Cisco IOS Release 15.2(4)E2

- EtherChannel Load Deferral: In an Instant Access system, the EtherChannel Load Deferral feature allows ports to be bundled into port channels, but prevents the assignment of group mask values to these ports. This prevents the traffic from being forwarded to new instant access stack members and reduce data loss following a stateful swtichover (SSO).

Features Introduced in Cisco IOS Release 15.2(4)E1

- (LAN Lite, IP Base, LAN Base) 2 Event Classification: This feature helps discover the power requirements of Power over Ethernet (PoE)-powered devices before the LLDP negotiation starts.
- (IP Lite) Bidirectional Forwarding Detection (BFD): BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent devices, including interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. This feature is supported only on Catalyst 2960-XR Series Switches.
- (LAN Lite, IP Base, LAN Base) Fast PoE: After a power outage, when power is restored, PoE to the endpoints on switch ports are restored quickly.
- Limiting Login: The Limiting Login feature helps network administrators to limit the login attempt of users to a network. When a user fails to successfully login to a network within a configurable number of attempts within a configurable time limit, the user can be blocked. This feature is enabled only for local users and not for remote users. You need to configure the **aaa authentication rejected** command in global configuration mode to enable this feature.
- x.509v3 with SSH Authentication: This feature uses public key algorithm (PKI) for server and user authentication, and allows the Secure Shell (SSH) protocol to verify the identity of the owner of a key pair via digital certificates, signed and issued by a Certificate Authority (CA).

Features Introduced in Cisco IOS Release 15.2(4)E

- (LAN Base for Catalyst 2960-X switches; IP Lite for Catalyst 2960-XR switches) Support for Embedded Event Manager (EEM).
- (LAN Base, Catalyst 2960-X switches) PVLAN support.
- (LAN Base, IP Base, IP Services) New enhancements like LACP rate fast, min links, LACP over QinQ (L2PT LACP) are added.
- Named VLAN: Option to specify a VLAN name for access and voice VLAN.

- (LAN Base, IP Base, and Enterprise Services, Catalyst 2960-XR switches) Policy-Based Routing with Object Tracking: Support for new command **set ip next-hop verify-availability** to use Policy-based Routing (PBR) with 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. This feature is supported only on IPv4 PBR and is not supported on IPv6 PBR, and PBR on VSS and VRF.
- (LAN Base and IP Lite) Control Plane Policing (CoPP) feature runs on a predefined set of protocols to control the flow of traffic coming to the CPU based on a defined rate limit on specific protocol packets. The CoPP protects the CPU from denial of service (DoS) attacks and ensures routing stability, reachability, and packet delivery.
- Rapid PVST+ Default: Rapid PVST+ is now the default spanning-tree mode used on all Ethernet port-based VLANs.
- The Auto Identity feature provides a set of built-in policies at the global configuration and interface configuration modes. The Auto Identity feature use the Cisco Common Classification Policy Language (C3PL)-based configuration that significantly reduces the number of commands used to configure both authentication methods and interface-level commands. The Auto Identity feature provides a set of builtin policies that are based on policy maps, class maps, parameter maps, and interface templates.
- Resilient Ethernet Protocol (REP) Enhancements - Option to configure an administrative VLAN for each segment.
- STP Enhancements
  - Bridge Assurance - Protects the network from bridging loops that are caused by that are caused by unidirectional links, or a malfunctioning switch. Bridge Assurance is enabled only on PortFast network ports.
  - Detecting UniDirectional Link Failures - The switch port detects unidirectional link failures by checking the consistency of the port role and state of the BPDUs received. When a conflict is detected, the designated port reverts to a blocking state. This feature does not require any user configuration.
  - PVST+ Simulation - This is now user-configurable. You can now enable or disable this per port, or globally. PVST+ simulation is enabled by default. It allows seamless interoperability between MST and Rapid PVST+. .

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
CSCva26201	3750X is not sending correct DSCP value in cflow IP header.
CSCvk21769	C2960L packet loss on 10M/Full port.
CSCvk38377	C4K_SNIPSMAN-3-GTXRXRESETFAILURE: Gtx Rx Reset Error in Snips.
CSCvm36476	C2960 plus handling GARP unexpectedly.
CSCvm24330	Tracebacks seen on loadversion due to MTU mismatch.
CSCvo37003	C4500 not showing MAC add of device (Avaya phone) in "show mac add" table after enabling mab,dot1x.
CSCvo38680	C6800IA-48FPD (FEX) reloads with a last reload reason of "Unknown reason".

Caveats Resolved in Cisco IOS Release 15.2(4)E10

None.

Caveats Resolved in Cisco IOS Release 15.2(4)E9

Bug ID	Headline
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"
CSCuv90519	IKEv2 session fails to come up after tunnel source address change
CSCve21224	ewlc: wncd crash seen at auth_mgr_pre_shim_handle_pre_event
CSCve57810	Device failing over without 'fail next-method' or 'no-response next method'
CSCvj23301	IOS: Crypto Ruleset fails to get deleted
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvn13735	Failure to detect the back to back CoA requests, leading to policy deletion.
CSCvn00129	After CoA push from ISE, Result of "show cts policy sgt" has multiple policies for "to unknown"
CSCvp76403	Defaulting interface config on dot1x interface results in incorrect port-control state on port

Caveats Resolved in Cisco IOS Release 15.2(4)E8

Bug ID	Headline
CSCvc71220	Fix the quotes issue in SA build infra
CSCve89361	Crash in SISF while processing IPv6 packet
CSCvj86626	Clients stuck in authentication loop when interface template is pushed from Radius server
CSCvk62735	3750 | high CPU | HACL Acl Manager
CSCvm43071	[IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list
CSCvm52157	Cat4K/sup8-E VSS 3.8.5aE- running out of CPU and IO memory resources while clearing access-session

Caveats Resolved in Cisco IOS Release 15.2(4)E7

Bug ID	Headline
CSCva10393	System crashed during boot up on 4948E.
CSCvd87317	The **ip access-list logging hash-generation** command not function expectedly.
CSCve37498	Switch sends duplicate accounting message, that causing ISE to generate misconfigured NAS Alarms.
CSCve69049	Crash when it tries to write over a TTY session.
CSCve73467	Link not up on M-gig line cards WS-X4748-12X48U+E with cable length of 300Ft.
CSCvg82674	VSS Standby crashes @ /k5/aclman/K5AclProfileMapEntry.cxx:135

CSCvh28285	H/W mac address table learn wrong mac address on C4500X VSS with Flexlink switchover.
CSCvh79168	Crash on numPolicersPerBank with Invalid policerBaseIndex.
CSCvh89534	4500 Sup 8E DACL applied to the incorrect interface.
CSCvi01706	Removing ACE from long ACL interrupts traffic.
CSCvi25365	2960x - session to the member switch fails in stack.
CSCvi50136	Repeated Modification of ACL causes standby switch to crash.
CSCvj29126	RADIUS client on network fails to solicit PAC key from Cisco TrustSec even though the device has a valid PAC.
CSCvj41439	ACL TCAM USAGE is different when using the same ACL configuration but different IOS version.
CSCvk23596	Additional fix needed for CSCvg34881 (Catalyst 4500 crash when WS-X4748 card goes down).
CSCvk52487	3750X Switch crash due to memory leak in HL2MCM process.

Caveats Resolved in Cisco IOS Release 15.2(4)E6

Bug ID	Headline
CSCvd40673	Cisco Smart Install Denial of Service Vulnerability.
CSCve53124	Stack of Catalyst 2960x Series Switches block ARP req after port flap when Port security enabled with DHCP Snooping.
CSCvf96579	Catalyst 2960 Series Switches: AAA Radius authentication fails with **switchport voice vlan dot1p** command.
CSCvg01818	Device crashes after defaulting configuration interface with dot1x enabled.
CSCvg70852	Unknown MAC addresses appear on port when trying to authenticate using dot1x.
CSCvg97016	Memory Leak with IPDT [IP Device Tracking].
CSCvf24186	Catalyst 2960X- Switch failed to boot with IOS version 152-2.E5 and 15.2(4)E4
CSCvf42171	Multiple Ports on a C2960X / C2960XR Stack stops providing PoE

Caveats Resolved in Cisco IOS Release 15.2(4)E5

Bug ID	Headline
CSCva86436	No export ipv4 unicast map triggered router to crash.
CSCvc72751	Endpoint bypasses restriction given by ISE and gets network access.
CSCuz61109	Self ping to port channel subinterface dropped with LISP decap log.
CSCuz94245	IGP-LDP sync interoperability for OSPF multiarea adjacency.
CSCuz95753	Paramiko SSH client, having password authentication, fails to connect to IOS.
CSCva83873	2960-X-:POST: Failed PortMacLoopback- in 2960-X.

Caveats Resolved in Cisco IOS Release 15.2(4)E4

Bug ID	Headline
CSCun71347	3850 Crash in "CEF: IPv4" Process While Processing ARP Throttle Elements
CSCuq91509	2960X/XR : Hibernation can not be configured for overnight period
CSCux05246	smnpwalk and snmpget have incorrect behavior on IP SLA
CSCuz28618	sup2t: sup crashed after MFIB errors
CSCva45821	IOS switch does not update native VLAN in LLDP
CSCva60320	(2960-X) 2960-X switch does not come up after software upgrade
CSCvb47673	SYS-2-MALLOCFAIL- Traceback and Crash observed in 2k stack
CSCvb91425	Output drops increased after enabling PIM on VLAN

CSCvc03727	IPDT host tracking max limit doesn't work correctly
CSCvc84352	IP Phone connectivity loss with dynamically assigned vlan and MDA

Caveats Resolved in Cisco IOS Release 15.2(4)E3

There are no resolved caveats in this release.

Caveats Resolved in Cisco IOS Release 15.2(4)E2

Bug ID	Headline
CSCur64110	Queue-based Transmit/Drop QoS counters for Cisco Catalyst 4000 Series Switches.
CSCuu66503	HTTPs: IOS HTTPS client not enforcing subject-name verification.
CSCuv27265	ENH: Enable support for TLSv1.1 & TLSv1.2 for HTTP secure server/client.
CSCuv41355	Unable to telnet: No wild listener: port 23.
CSCuv92875	Add prefix information in IPv6 RA when system/ SVI is shutdown.
CSCuw36080	SNMP with extended ACL.
CSCuw48118	Cisco ASR 920 Series switches: crash in bcopy called from addnew during reassembly.
CSCuw49406	“no ip routing protocol purge interface” delete with reload
CSCux26097	Debug logging - parser issue.
CSCux38417	Cisco IOS and IOS-XE IKEv2 fragmentation DoS.
CSCux85039	Cisco Catalyst 3650 and 3850 Series Switches: Syslog produces no output when set to logging queue-limit X.
CSCux99025	Evaluation of Cisco IOS and IOS-XEl for NTP January 2016.
CSCux99594	EEM policies may not be able to send emails.
CSCuy03680	V3Lite IGMP packets sent instead of V3 when UDP based feature is present.
CSCuy05927	IPC-WATERMARK and CHKPT-5-HIGHBUFFER logs leading to reload.
CSCuy12271	Wrong LSP size calculation following MAC move with OTV.
CSCuy43392	Cisco 5760 Wireless LAN Controller crash at snmp_subagent.
CSCuy44377	Syslog: Source-Interface address change does not take effect in IPv6.
CSCuy87667	Crash due to block overrun by AAA banner.
CSCuy92281	VLAN 1 interface is shutdown during bootup.
CSCuz52528	Evaluation of all for OpenSSL May 2016.
CSCuv37518	BEMS410419: IE2k PoE ports report faulty when shut and/or PoE disabled.

Caveats Resolved in Cisco IOS Release 15.2(4)E

Bug ID	Headline
CSCur47730	(Catalyst 2960-X Switches) C2960X doesn't link up when connected with ws-4424-GB-rj45
CSCus13924	Device crashes while configuring 'Identity' commands
CSCut53599	(Catalyst 2960-X Switches) C2960X RPS is not functioning correctly, reports "RPS is not responding"
CSCuu69332	Frame with special DesMac is forwarded by STP block port
CSCuu83085	Memory leaks @ AAA Account Response.
CSCuu92224	2960X - EPM vlan plugin crash
CSCuu96300	(Catalyst 2960-X Switches) High CPU every 10min by process SFF8472
CSCuv53498	(Catalyst 2960XR/6800IA) FRU Power Supply is not responding

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015-2019 Cisco Systems, Inc. All rights reserved