Release Notes for Catalyst 3560-CX and 2960-CX Series Switches, Cisco IOS Release 15.2(4)E and Later

First Published: October 1, 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 3560-CX and the Catalyst 2960-CX 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 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Software Image" section on page 5.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://www.cisco.com/download/navigator.html

Contents

Introduction

The Catalyst 3560-CX and Catalyst 2960-CX switches are compact Gigabit Ethernet (GE) switches that have features comparable to high-end Cisco switches but in smaller form factors. Some of the key features are:

- Up to 10 Gigabit uplinks for high-bandwidth applications and business growth
- Cisco Catalyst Instant Access mode (on 3560cx-12PD-S and 3560CX-8XPD-S switches) for management simplicity on switches with 10G uplink. See Instant Access FAQ here.
- Support for Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) for software-defined networking (SDN) and programmability
- Integration with Cisco TrustSec® for identity, segmentation, and security
- Up to 240W of available power for PoE+ per switch — twice the available power of previous generation switches — for supporting more PoE devices
- Switch Hibernation Mode and Energy Efficient Ethernet (EEE) for lower energy costs
- NetFlow Lite for end to end visibility to the flows in the network

Supported Hardware

Switch Models

Table 1 Catalyst 3560-CX Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3560CX-8TC-S	IP Base IP Services	Non-PoE, 8 downlink ports, 8 access ports of 1G access ports, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G[1]
WS-C3560CX-8PC-S	IP Base IP Services	240W PoE+, 8 downlink ports, 8 access ports of 1G access ports, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G
WS-C3560CX-12TC-S	IP Base IP Services	Non-PoE, 12 downlink ports, 12 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G
WS-C3560CX-12PC-S	IP Base IP Services	240W PoE+, 12 downlink ports, 12 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G
WS-C3560CX-12PD-S	IP Base IP Services	240W PoE+, 12 downlink ports, 12 access ports of 1G, 2 SFP+ uplink ports of 10G, 2 uplink Cu ports of 1G

Table 1 Catalyst 3560-CX Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3560CX-8PT-S	IP Base IP Services	146W PoE+, 8 downlink ports, 8 access ports of 1G, 2 uplink UPoE+ ports of 1G
WS-C3560CX-8XPD-S	IP Base IP Services	240W PoE+, 8 downlink ports, 6 access ports of 1G, 2 access ports of 100M/1G/2.5G/5G/10G, 2 SFP+ uplink ports of 10G

1. For all switch models, the SFP ports and Cu ports are usable concurrently.

Table 2 Catalyst 2960-CX Switch Models

Switch Model	Cisco IOS Image	Description
WS-C2960CX-8TC-L	LAN Base	Non-PoE, 8 downlink ports, 8 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G[1]
WS-C2960CX-8PC-L	LAN Base	124W PoE+, 8 downlink ports, 8 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G

1. For all switch models, the SFP ports and Cu ports are usable concurrently.

Optics Modules

The Catalyst 3560-CX and 2960-CX 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 26.0 with JavaScript enabled.

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 3560-CX

Image	Filename	Description
Universal image	c3560cx-universalk9-mz.152-4.E	IP Base and IP Services images.
Universal image	c3560cx-universalk9-tar.152-4.E	IP Base and IP Services cryptographic images with Device Manager.

Table 5 Software Image for Cisco Catalyst 2960-CX

Image	Filename	Description
Universal image	c2960cx-universalk9-mz.152-4.E	LAN Base image.
Universal image	c2960cx-universalk9-tar.152-4.E	LAN Base cryptographic image with Device Manager.

Features of the Switch

Cisco Catalyst 3560-CX switches features:

- PoE+ and non-PoE, 8 and 12 downlink ports, 1G SFP and 10G SFP+ uplink port models
- IPv4 and IPv6 routing, Multicast routing, advanced quality of service (QoS), and security features in hardware
- Cisco Catalyst Instant Access mode (on 3560cx-12PD-S and WS-C3560CX-8XPD-S switches) for management simplicity on switches with 10G uplink
- Up to 240W of available power for PoE+ per switch
- Switch Hibernation Mode and Energy Efficient Ethernet (EEE) for lower energy costs
- Horizontal Stacking (on WS-C3560CX-12PD-S and WS-3560CX-8XPD-S switches
- Enhanced Limited Lifetime Warranty (E-LLW) with next business day (NBD) advance hardware replacement and 90 day access to Cisco Technical Assistance Center (TAC) support
- Enhanced Cisco EnergyWise for operational cost optimization by measuring actual power consumption of the PoE devices, reporting, and reducing energy consumption across the network
- USB Type-A and Type-B ports for storage and console respectively
- Application visibility and capacity planning with integrated NetFlow Lite
- Hardware support for Secure Group Access Control lists (SGACL) and IEEE 802.1AE MACsec.
- Software support for IEEE 802.1AE MACsec from Cisco IOS Release 15.2(4)E.

Cisco Catalyst 2960-CX switches features:

- PoE+ and non-PoE models, 8 downlink ports, 1G SFP uplink port models
- Reduced power consumption and advanced energy management features
- USB Type-A and Type-B ports for storage and console respectively
- Application visibility and capacity planning with integrated NetFlow Lite

- Switch Hibernation Mode and Energy Efficient Ethernet (EEE) for lower energy costs
- Enhanced Limited Lifetime Warranty (E-LLW) with next business day (NBD) advance hardware replacement and 90 day access to Cisco Technical Assistance Center (TAC) support
- Enhanced Cisco EnergyWise for operational cost optimization by measuring actual power consumption of the PoE devices, reporting, and reducing energy consumption across the network

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).
- Cisco S-Class Optics Support on Cisco Catalyst 3560-CX Series Switches: The following S-Class Optics are supported:
  - SFP-10G-SR-S
  - SFP-10G-ZR-S
  - SFP-10G-ER-S
  - SFP-10G-LR-S

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 PoE-powered devices before LLDP negotiation starts.
- (LAN Lite, IP Base, LAN Base) Fast Power over Ethernet (PoE): After a power outage, when power is restored, PoE to the endpoints on switch ports are restored quickly
- (IP Base, LAN Base) Security Group Tag Over SGT Exchange Protocol (SXP): SGT Exchange Protocol (SXP) propagates the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec. SGACL support is also available in this release for Catalyst 3560-CX switches.
- 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 the 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, 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.
- Switches that support 10G SFP+ uplink ports (with optical cables) and MGig ports (on copper cables) can now be a part of Horizontal Stacking.
- (LAN Base) 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+: Rapid PVST+ is now the default spanning-tree mode used on all Ethernet port-based VLANs.
- (Catalyst 3560-CX switches) 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.
- Cisco TrustSec NDAC MACsec: MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange
- MKA MACsec encryption: 802.1AE MACsec encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between the switch and host devices.

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.

Limitations and Restrictions

- Effective with Cisco IOS Release 15.2(4)E5, Smart Install feature is not available in Cisco IOS software.

- 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)

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.
CSCvf96579	Catalyst 2960 Series Swtiches :AAARadius authentication fails with **switchport voice vlan dot1p** command.
CSCvg70852	Unknown MAC addresses appear on port when trying to authenticate using dot1x.
CSCvg97016	Memory Leak with IPDT [IP Device Tracking].

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.

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
CSCvb47673	(3560-CX) SYS-2-MALLOCFAIL- Traceback and Crash observed in 2k stack
CSCvb91425	(3560-CX) 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.
CSCuz02766	Crash in IOSd with ‘EPC SM Liaison Update proc’.
CSCud37408	PerfMon entries not idle timing out.

Caveats Resolved in Cisco IOS Release 15.2(4)E

Bug ID	Headline
CSCus13924	Device crashes while configuring 'Identity' commands
CSCuu69332	(Catalyst 3560-CX Switches) Frame with special DesMac is forwarded by STP block port

Bug ID	Headline
CSCuu83085	Memory leaks @ AAA Account Response.
CSCuu92224	2960X - EPM vlan plugin crash

Related Documentation

- Catalyst 3560-CX and Catalyst 2960-CX switch documentation at these URLs:

  http://www.cisco.com/c/en/us/support/switches/catalyst-2960-cx-series-switches/tsd-products-support-series-home.html

  http://www.cisco.com/c/en/us/support/switches/catalyst-3560-cx-series-switches/tsd-products-support-series-home.html
- 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 "Notices" 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.