Release Notes for Cisco Catalyst 1000 Series Switches, Cisco IOS Release 15.2(7)Ex

First Published: 2019-12-25

Last Modified: 2024-03-29

Release Notes for Cisco Catalyst 1000 Series Switches, Cisco IOS Release 15.2(7)Ex

Introduction

This release note describes the features, modifications, and caveats for the Cisco IOS Release 15.2(7)Ex software on the Cisco Catalyst 1000 Series Switches.

Supported Hardware

Cisco Catalyst 1000 Series Switches—Model Numbers

The following table lists the supported hardware models.

Switch Model	Description
Cisco Catalyst C1000 8-Port and 16-Port Switch Models and Description	
C1000-8T-2G-L	8 10/100/1000 Ethernet ports; 2 1-Gigabit small form-factor pluggable (SFP) module uplink slots or 2 RJ-45 slots.
C1000-8T-E-2G-L	Externally powered; 8 10/100/1000 Ethernet ports; 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots.
C1000-8P-2G-L	8 10/100/1000 Power over Ethernet plus (PoE+) ports (PoE budget of 67W); 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots.
C1000-8P-E-2G-L	Externally powered; 8 10/100/1000 PoE+ ports (PoE budget of 67W); 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots.
C1000-8FP-2G-L	8 10/100/1000 PoE+ ports (PoE budget of 120W); 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots.

Switch Model	Description
C1000-8FP-E-2G-L	Externally powered; 8 10/100/1000 PoE+ ports (PoE budget of 120W); 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots.
C1000-16T-2G-L	16 10/100/1000 Ethernet ports; 2 1-Gigabit small form-factor pluggable (SFP) module uplink slots.
C1000-16T-E-2G-L	Externally powered; 16 10/100/1000 Ethernet ports; 2 1-Gigabit SFP module uplink slots.
C1000-16P-2G-L	16 10/100/1000 PoE+ ports (PoE budget of 120W); 2 1-Gigabit SFP module uplink slots.
C1000-16P-E-2G-L	Externally powered; 16 10/100/1000 PoE+ ports (PoE budget of 120W); 2 1-Gigabit SFP module uplink slots.
C1000-16FP-2G-L	16 10/100/1000 PoE+ ports (PoE budget of 240W); 2 1-Gigabit SFP module uplink slots.
Cisco Catalyst C1000 24-Port and 48-Port Switch Models and Description	
C1000-24T-4G-L	24 10/100/1000 Ethernet ports; four 1-Gigabit Ethernet SFP module uplink slots
C1000-24P-4G-L	24 10/100/1000 PoE+ ports (PoE budget of 195W); four 1-Gigabit Ethernet SFP module uplink slots
C1000-24FP-4G-L	24 10/100/1000 PoE+ ports (PoE budget of 370W); four 1-Gigabit Ethernet SFP module uplink slots
C1000-48T-4G-L	48 10/100/1000 Ethernet ports; four 1-Gigabit Ethernet SFP module uplink slots
C1000-48P-4G-L	48 10/100/1000 PoE+ ports (PoE budget of 370W); four 1-Gigabit Ethernet SFP module uplink slots
C1000-48FP-4G-L	48 10/100/1000 PoE+ ports (PoE budget of 740W); four 1-Gigabit Ethernet SFP module uplink slots
C1000-24T-4X-L	24 10/100/1000 Ethernet ports; four 10-Gigabit Ethernet small form-factor pluggable plus (SFP+) module uplink slots
C1000-24P-4X-L	24 10/100/1000 Ethernet ports; limited PoE+ ports (PoE budget of 195W); four 10-Gigabit Ethernet SFP+ module uplink slots
C1000-24FP-4X-L	24 10/100/1000 PoE+ ports (PoE budget of 370W); four 10-Gigabit Ethernet SFP+ module uplink slots
C1000-48T-4X-L	48 10/100/1000 Ethernet ports; four 10-Gigabit Ethernet SFP+ module uplink slots

Switch Model	Description
C1000-48P-4X-L	48 10/100/1000 PoE+ ports (PoE budget of 370W); four 10-Gigabit Ethernet SFP+ module uplink slots
C1000-48FP-4X-L	48 10/100/1000 PoE+ ports (PoE budget of 740W); four 10-Gigabit Ethernet SFP+ module uplink slots
Cisco Catalyst C1000 24-Port and 48-Port FastEthernet Switch Models and Description	
C1000FE-24T-4G-L	24 10/100 Fast Ethernet ports; 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots combo ports; 2 1-Gigabit Ethernet SFP module uplink slots.
C1000FE-24P-4G-L	24 10/100 Fast Ethernet ports (PoE budget of 195W); 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots combo ports; 2 1-Gigabit Ethernet SFP module uplink slots.
C1000FE-48T-4G-L	48 10/100 Fast Ethernet ports; 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots combo ports; 2 1-Gigabit Ethernet SFP module uplink slots.
C1000FE-48P-4G-L	48 10/100 Fast Ethernet ports (PoE budget of 370W); 2 1-Gigabit SFP module uplink slots or 2 RJ-45 slots combo ports; 2 1-Gigabit Ethernet SFP module uplink slots.

Optics Modules

The Catalyst 1000 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: https://tmgmatrix.cisco.com

Features of the Switch

Ease of Operation

This section lists the ease-of-operation features supported by Cisco Catalyst 1000 Series Switches:

- Cisco Catalyst Smart Operations is a comprehensive set of features that simplify LAN deployment, configuration, and troubleshooting. Catalyst Smart Operations is a set of features that includes Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:
  - Cisco Auto Smartports provide automatic configuration as devices connect to the switch port, allowing auto detection, and plug and play of the device onto the network.
  - Cisco Smart 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).

- Auto Configuration determines the level of network access provided to an endpoint based on the type of the endpoint device.
- Interface templates provide 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.

Network Security

The Cisco Catalyst 1000 Series Switches provide a range of security features to limit access to the network and mitigate threats.

- In Cisco IOS Release 15.2(7)E3 and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.
- Port security: secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.
- Dynamic Host Control Protocol (DHCP) snooping: filters untrusted DHCP messages between untrusted hosts and DHCP servers.
- Dynamic ARP Inspection (DAI): prevents malicious attacks on the device by not relaying invalid Address Resolution Protocol (ARP) requests and responses to other ports in the same VLAN.
- Flexible authentication: supports multiple authentication mechanisms including 802.1X, MAC Authentication Bypass, and web authentication.
- Open mode: creates a user-friendly environment for 802.1X operations.
- RADIUS Change of Authorization (CoA): enables asynchronous policy management.
- Standard and extended access control lists (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 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.
- TACACS+ and RADIUS authentication: facilitates the centralized control of a device and restricts unauthorized users from altering the configuration.
- MAC address notification: notifies administrators about users added to or removed from the network.
- Multilevel security on console access: prevents unauthorized users from altering the device configuration.
- Bridge protocol data unit (BPDU) Guard: shuts down Spanning Tree Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- Internet Group Management Protocol (IGMP) filtering: provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port.

- 802.1x monitor mode: enables authentication across the wired infrastructure in an audit mode without affecting wired users or devices. It helps IT administrators to 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

This section lists the deployment and control features:

- Auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
- Dynamic Host Configuration Protocol (DHCP) auto-configuration of multiple switches through a boot server eases switch deployment.
- 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.
- Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad.
- 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 wiring. Also, port faults can be detected and disabled on the interfaces.
- 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 requester.
- Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.
- 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.
- Storm control for unicast, broadcast and multicast traffic to prevent disruption in the network due to packet flooding on the LAN.
- 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.
- Switch-port auto-recovery (error-disable) automatically attempts to reactivate a link that is disabled because of a network error

Quality of Service

This section lists the quality of service (QoS) features:

- Multilayer Switching (MLS) QoS provides the ability to configure granular policies and classes on every interface. These policies include policers, markers, and classifiers.
- Supports up to 4 egress queues per port, and finer flow segregation using 2 threshold markers for non-strict-priority queues.
- Strict priority queuing to ensure that the highest-priority packets are serviced ahead of all other traffic.
- Shared Round Robin (SRR) scheduling to ensure differential prioritization of packet flows.

Software Features in Cisco IOS Release 15.2(7)E1

New Software Features

Feature Name	Description
IPv6 RA Guard	Allows the network administrator to block or reject unwanted or rogue router advertisement (RA) guard messages that arrive at the network device platform.
Dual Active Detection Using Enhanced PAgP	If the device is connected to a Virtual Switch System (VSS) using a PAgP EtherChannel, it automatically serves as a VSS client, using enhanced PAgP on this EtherChannel for dual-active detection.
Sampled Flow (sFlow)	This feature allows you to monitor real-time traffic in data networks containing switches and routers. It uses the sampling mechanism in the sFlow agent software on switches to monitor traffic and to forward the sample data to the central data collector.
IP Source Guard Support for EtherChannels	You can now configure IP source guard on EtherChannel interfaces.
Single IP Management	Cisco Catalyst 1000 Series Switches that support 1G and 10G SFP/SFP+ uplink ports can be part of single IP management. You can use SFP/SFP+ ports with optical cables to connect boxes placed at different locations to form a group, where the compact boxes are placed in different floors or buildings.
SSH File Transfer Protocol	The device supports SSH File Transfer Protocol (SFTP). The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device. Therefore, any SFTP server user with the appropriate permission can copy files to and from the device.

Software Features in Cisco IOS Release 15.2(7)E2

New Software Features

Feature Name	Description
Dying Gasp	Dying Gasp is a signal or alert that is generated when a device is about to go down due to a reset or power failure. The system holds enough residual power to send out dying gasp messages after a power failure, notifying the administrator or user.

Software Features in Cisco IOS Release 15.2(7)E3

New Software Features

Feature Name	Description
Enable Password Masking	A new keyword **masked-secret** is added to the **username** command to enable the secret masking functionality. The secret input will be masked on the console and will be converted to type 9 by default.
Show Upgrade and Downgrade History	The command, **show archive sw-upgrade history** command displays the upgrades and downgrades performed on a device. Note that manual upgrades done through TFTP of tar files or binary files are not displayed.

Software Features in Cisco IOS Release 15.2(7)E4

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E5

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E6

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E7

New Software Features

Feature Name	Description
Data Sanitization	Supports the use of the National Institute of Standards and Technology (NIST) purge method that renders data unrecoverable through simple, non-invasive data recovery techniques or through state-of-the-art laboratory techniques. For more information, see the "Data Sanitization" chapter of the *System Management Configuration Guide*.

Software Features in Cisco IOS Release 15.2(7)E8

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E9

New Software Features

None.

Software Features in Cisco IOS Release 15.2(7)E10

New Software Features

None.

Compatibility Matrix

The following table provides software compatibility information.

Catalyst 1000 Switches	Cisco Identity Services Engine	Cisco Configuration Professional for Catalyst
Cisco IOS Release 15.2(7)E1	2.7	1.7.1
Cisco IOS Release 15.2(7)E3	3.0	1.8.0

Device Manager System Requirements

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

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1280 x 800	Small

1 We recommend 1 GHz
2 We recommend 1 GB DRAM

Software Requirements

Operating Systems

- Windows 10 or later
- Mac OS X 10.11 or later

Browsers

- Google Chrome: Version 38 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox: Version 42 or later (On Windows and Mac)
- Safari: Version 9 or later (On Mac)

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 1: Software Image for Cisco Catalyst 1000 Switch

Image	Filename
Universal image	c1000-universalk9-mz.152-7.E1.bin
Universal image	c1000-universalk9-tar.152-7.E1.tar

Web UI

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

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

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

2. Configure the username and password with privilege 15.

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

3. Clear the browser cache and relaunch the Web UI.
4. Login by entering the privilege 15 username and password.

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 1000 Series Switches datasheet at: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/nb-06-cat1k-ser-switch-ds-cte-en.html

Limitations and Restrictions

- Speeds of 10/100Mbps are not supported on uplink ports with GLC-TE.
- Uplink or downlink ports do not support the amber-colored physical light emitting diode (LED). For all port-related LED verification, use the **show hardware led** command.
- The uplink and downlink LED do not blink when the traffic rate changes.
- Multi-chassis EtherChannel (MEC) is not supported.
- Fast Ethernet ports do not support single IP management.
- When no cable is connected to Fast Ethernet ports, in the output of the **show cable-diagnostics tdr interface** command, the pair status is displayed as *Normal* instead of *Open*. The pair status is reported as *Open* only when the cable breaks.
- The Time Domain Reflectometry (TDR) gives the correct length to fault status only when the overall cable length is greater than 10m. All the other fields in the cable diagnostics result, such as pair polarity,

speed, and pair status shows the correct result for cables of any length. The TDR may not report the correct length if one end is terminated.

- Protocol Independent Multicast (PIM) is not supported.

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Cisco Bug Search Tool

The Cisco Bug Search Tool (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 BST is designed to improve the effectiveness in network risk management and device troubleshooting. 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, click on the identifier.

Open Caveats in Cisco IOS Release 15.2(7)E1

Caveat ID Number	Description
CSCvs21192	Catalyst 1000: Multicast address are set to invalid IP and traffic impact after querier port flap.
CSCvs23382	Catalyst 1000: Multicast stale entries created on STP flap.

Open Caveats in Cisco IOS Release 15.2(7)E2

There are no open caveats in Cisco IOS Release 15.2(7)E2.

Open Caveats in Cisco IOS Release 15.2(7)E3

Caveat ID Number	Description
CSCvv60364	Cisco Catalyst 1000 Series Switches FE -Link flaps seen on random downlink ports on soak testing.
CSCvv86851	TACACS not working if TACACS group server has the **server-private** *ip* **key** *passw* command in the Cisco IOS Release 15.2(7)E3 and Cisco IOS XE Release 3.11.3E.

Open Caveats in Cisco IOS Release 15.2(7)E4

Caveat ID Number	Description
CSCvx42435	Cisco Catalyst 1000 Series Switches: DHCPv6 relay is not happening, solicit packets are not forwarded.

Open Caveats in Cisco IOS Release 15.2(7)E5

Caveat ID Number	Description
CSCvz53228	C1000 not send leave group message to mroute port

Open Caveats in Cisco IOS Release 15.2(7)E6

Table 2: Open Caveats

Bug ID	Headline
CSCwa92718	MAC-move does not install the MAC learnt from the auth port as *static*
CSCwb19078	Catalyst 1000: When MAB is configured on an interface, specific clients will lose communication.

Open Caveats in Cisco IOS Release 15.2(7)E7

Table 3: Open Caveats

Bug ID	Headline
CSCwc50095	Crash on Cisco Switch while handling Ethernet Configuration Testing P Pt. 2.

Open Caveats in Cisco IOS Release 15.2(7)E8

None

Open Caveats in Cisco IOS Release 15.2(7)E9

None

Open Caveats in Cisco IOS Release 15.2(7)E10

None

Resolved Caveats in Cisco IOS Release 15.2(7)E3

Table 4: Resolved Caveats

Caveat ID Number	Description
CSCvt16192	Remove switch licensing for Cisco Catalyst 1000 Series SKUs.
CSCvt16716	IPv6 source guard feature is broken in Cisco IOS Release 15.2(7)Ex.
CSCvu10399	Cisco IOS and IOS XE Software Information Disclosure Vulnerability.
CSCvu22034	Idle timeout does not clear sessions even if no endpoint is connected.

Caveat ID Number	Description
CSCvq41676	Multicast packets are replicated twice on Cisco Catalyst 1000 Series Switches two-member stack.
CSCvv00134	VTY telnet disable, enable SSH-based on platform request.

Resolved Caveats in Cisco IOS Release 15.2(7)E3k

Table 5: Resolved Caveats

Caveat ID Number	Description
CSCvv99161	Cisco Catalyst 1000 Series Switches FIPS enablement.

Resolved Caveats in Cisco IOS Release 15.2(7)E4

Table 6: Resolved Caveats

Caveat ID Number	Description
CSCvw95683	Cisco Catalyst 1000 Series Switches may exhibit random crash/hang/silent-reload.
CSCvv93417	Member switch fails wired dot1x; primary switch passes dot1x using the same configuration.
CSCvw18208	Cisco Catalyst 1000 Series Switch members boots up with different version from the primary switch.
CSCvv23128	Disparity between the configured **load-interval** command and the value show in **show interface** command.
CSCvv75698	Switch gets hung with traces and error logs.
CSCvv86851	TACACS not working if TACACS group server has the **server-private** *ip* **key** *passw* command in the Cisco IOS Release 15.2(7)E3 and Cisco IOS XE Release 3.11.3E.
CSCvx03576	Cisco Catalyst 1000 Series Switch traffic via specific SVI may fail after network loop.

Resolved Caveats in Cisco IOS Release 15.2(7)E5

Table 7: Resolved Caveats

Caveat ID Number	Description
CSCvu61737	Config hidden on member switch after defaulting the interface.
CSCvx76066	Switch crashes due to "HTTP Core".
CSCvy03539	C1000: **no cdp enable** change to **no cdp tlv app** after reload.

Caveat ID Number	Description
CSCvy40917	Username <username> privilege command is not accepted without specifying a password.
CSCvz05103	DACL is not being removed from the interface on C1000 Series Switches.
CSCvx37117	C1000 stack switch 2 traffic does not flow between interfaces on different ASIC.
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability.

Resolved Caveats in Cisco IOS Release 15.2(7)E6

Table 8: Resolved Caveats

Bug ID	Headline
CSCvz63002	QoS not working properly when class-maps are matched through ACE u Catalyst 1000.
CSCvz30562	Catalyst 1000 does not flood IGMP membership reports even though th **snooping** command is set.
CSCvx17595	Catalyst 1000: **switchport autostate exclude** and **no power efficient-eth** added after the stack member powers off or on.
CSCvz53228	Catalyst 1000 does not send a leave group message to mroute port.

Resolved Caveats in Cisco IOS Release 15.2(7)E7

Table 9: Resolved Caveats

Bug ID	Headline
CSCwa92718	MAC-move does not install the MAC learnt from the auth port as STAT
CSCwb05242	24 port switch may crash in a stack with 48 port switches.
CSCwb20452	Inactivity timer does not work, and session information persists even if disconnected from the hub for Cisco Catalyst 1000 Series Switches.
CSCwb42475	1000 LST is not working on combo port.
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvx63027	Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability.
CSCwa96810	Cisco IOS and IOS XE Software Common Industrial Protocol Request I Vulnerability.

Resolved Caveats in Cisco IOS Release 15.2(7)E8

Table 10: Resolved Caveats

Bug ID	Headline
CSCvw82249	Dot1x authentication using EAP-TLS is failing on the stack member
CSCwc50095	Crash on Cisco Switch while handling Ethernet Configuration Testi Pt. 2
CSCwe38982	MAC flaps observed in network when one member link is suspended 9200L stack

Resolved Caveats in Cisco IOS Release 15.2(7)E9

Table 11: Resolved Caveats

Bug ID	Headline
CSCvv18787	C1000: ILPOWER-5-ILPOWER_POWER_CDP_SHUT for Class 4 P
CSCwf20452	Cat1000 reports macflap for a host in VLAN between two ports.
CSCwf70981	"%USB_CONSOLE-3-APP_I2C_WRITE: Application write error"
CSCwh22016	C1000-8T-2G-L uplink combo port goes up - down - up after reloadi
CSCwh49745	When the FWD port goes down in MST0 of C1000, the Altn port be Sts:BLK

Resolved Caveats in Cisco IOS Release 15.2(7)E10

Table 12: Resolved Caveats

Bug ID	Headline
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerabil
CSCwd92370	Sending large dot1x frames (>5028) leads to buffer failure
CSCwh96519	For PoE used and remaining power on 3560, the SNMP walk result i data
CSCwi79812	Unable to form STACK with C1000 8 port devices when upgrade to
CSCwi06388	c1000 : Vendor OID sysUpTime.6.1.2.1.47.1.1 = NULL TYPE/VAL
CSCwe32897	C1000-48T-4X-L/C1000-48P-4X-L // 15.2(7)E7 // TenGigaInterfac

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE 16 at this URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

Cisco Validated Designs documents at this URL: https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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.