Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-08-10

Last Modified: 2023-10-30

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Amsterdam 17.3.x

Introduction

Cisco Catalyst 9600 Series Switches are the next generation purpose-built 40 GigabitEthernet, 50 GigabitEthernet, 100 GigabitEthernet, and 400 GigabitEthernet modular core and aggregation platform providing resiliency at scale with the industry's most comprehensive security while allowing your business to grow at the lowest total operational cost. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver hardware and software convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 3.0 and Cisco Silicon One Q200. The platform runs an Open Cisco IOS XE that supports model driven programmability, Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) local storage, and a higher memory footprint). The series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

It also supports features that provide high availability, advanced routing and infrastructure services, security capabilities, and application visibility and control.

Whats New in Cisco IOS XE Amsterdam 17.3.8a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Whats New in Cisco IOS XE Amsterdam 17.3.8

Hardware Features in Cisco IOS XE Amsterdam 17.3.8

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.8

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.7

Hardware Features in Cisco IOS XE Amsterdam 17.3.7

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.7

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.6

Hardware Features in Cisco IOS XE Amsterdam 17.3.6

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.6

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.5

Hardware Features in Cisco IOS XE Amsterdam 17.3.5

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.5

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.4

Hardware Features in Cisco IOS XE Amsterdam 17.3.4

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.4

There are no new software features in this release.

Whats New in Cisco IOS XE Amsterdam 17.3.3

Hardware Features in Cisco IOS XE Amsterdam 17.3.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.3

Feature Name	Description, Documentation Link, and License Level Information
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem. Minimum Required SSM On-Prem Version: Version 8, Release 202102. Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3. See System Mangement → Smart Licening Using Policy and System Management Commands. (A license level does not apply)
MLDP-Based MVPN	The MLDP-based MVPN feature provides extensions to Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) label switched paths (LSPs) for transport in the Multicast Virtual Private Network (MVPN) core network. See IP Multicast Routing Configuration Guide → MLDP-Based MVPN. (Network Advantage)

Whats New in Cisco IOS XE Amsterdam 17.3.2a

Hardware Features in Cisco IOS XE Amsterdam 17.3.2a

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.2a

Feature Name	Description, Documentation Link, and License Level Information
Smart Licensing Using Policy	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date. Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy. For conceptual, configuration, migration, and troubleshooting information for Smart Licensing Using Policy, see the documentation links below. See System Mangement → Smart Licening Using Policy and System Management Commands. (A license level does not apply)
Cisco DNA Center Support for Smart Licensing Using Policy	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release on the Cisco Catalyst 9600 Series Switches is Cisco IOS XE Amsterdam 17.3.2a. Implement the "Connected to CSSM Through a Controller" topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM), and returns the acknowledgement (RUM ACK). In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options. See System Mangement → Smart Licening Using Policy. (A license level does not apply)

Whats New in Cisco IOS XE Amsterdam 17.3.1

Hardware Features in Cisco IOS XE Amsterdam 17.3.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE Amsterdam 17.3.1

Feature Name	Description, Documentation Link, and License Level Information
BGP EVPN VXLAN • Broadcast, Unknown Unicast, and Multicast (BUM) Traffic Rate Limiting • Enhanced rendezvous point (RP) Functionality for Layer 3 TRM for IPv4 and IPv6 traffic • Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic • Layer 3 Tenant Routed Multicast (TRM) for IPv6 Traffic	The following BGP EVPN VXLAN features are introduced in this release: • BUM Traffic Rate Limiting: Allows you to use a policer and set the flood rate limit of the BUM traffic in the network to a predefined value. • Enhanced RP Functionality for Layer 3 TRM for IPv4 and IPv6 traffic: Allows you to configure an RP for TRM with PIM-Sparse Mode (PIM-SM) on a single or multiple VTEPs inside the BGP EVPN VXLAN fabric or on a device outside the fabric. • Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic: Allows you to forward IPv4 Layer 3 multicast traffic between sources and receivers of an EVPN VXLAN network and an MVPN network. • Layer 3 Tenant Routed Multicast for IPv6 Traffic: Introduces support to configure Layer 3 TRM for IPv6 traffic with PIM-Source Specific Mode (PIM-SSM) and with PIM-SM. See BGP EVPN VXLAN. (Network Advantage)
Customizable Switching Database Manager (SDM) Templates	Allows you to configure a customizable SDM template. In the customized template, you can assign resources to different features based on your requirement. See System Management → Configuring SDM Templates. (Network Advantage)
EIGRP Loop-Free Alternate (LFA) IP Fast Reroute (IPFRR)	Enables the Enhanced Interior Gateway Routing Protocol (EIGRP) to reduce the routing transition time to less than 50 ms by precomputing repair paths or backup routes and installing these paths or routes in the Routing Information Base (RIB). See IP Routing → Configuring EIGRP Loop-Free Alternate IP Fast Reroute. (Network Advantage)
Enhanced SGACL Logging	Introduces support for Security Group Access Control List (SGACL) logging using NetFlow hardware, which allows much higher logging rates. See Cisco TrustSec → Configuring Security Group ACL Policies. (Network Advantage)
IPv6 Multicast Virtual Private Network (MVPNv6)	Enables service providers to use their existing IPv4 backbone to provide multicast-enabled private IPv6 networks to their customers. See IP Multicast Routing → Configuring MVPNv6. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Link Aggregation Control Protocol (LACP) 1:1 Redundancy and Dampening	Introduces support for: • LACP 1:1 Redundancy: Supports an EtherChannel configuration with one active link and fast switchover to a hot standby link. • LACP 1:1 Hot Standby Dampening: Configures a timer that delays switchover back to the higher priority port after it becomes active. See Layer 2 → Configuring EtherChannels. (Network Advantage)
MPLS QoS - WRED	Introduces support for weighted random early detection (WRED) in MPLS Quality of Service (QoS). This feature configures WRED to use the MPLS experimental bits (EXP) to calculate the drop probability of a packet. See Multiprotocol Label Switching → Configuring MPLS QoS. (Network Advantage)
MPLS VPN InterAS Option AB	Enables different autonomous systems to interconnect by using a single Multiprotocol Border Gateway Protocol (MP-BGP) session, which is enabled globally on the router. When different autonomous systems are interconnected in an MPLS VPN InterAS Option AB configuration, the entire network configuration is scaled and simplified, and maintains IP quality of service (QoS) functions between Autonomous System Boundary Router (ASBR) peers. See Multiprotocol Label Switching → Configuring MPLS VPN InterAS Options. (Network Advantage)
Open Shortest Path First Nonstop Routing (OSPF NSR)	Enables a device with redundant Route Processors (RPs) to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned RP switchovers, by checkpointing state information from OSPF on the active RP to the standby RP. OSPF uses this checkpointed information to continue operation without interruption when the switchover to standby RP occurs. See IP Routing. (Network Advantage)
OSPFv2 Loop-Free Alternate (LFA) IP Fast Reroute (IP FRR)	Enables Open Shortest Path First version 2 (OSPFv2) to use a precomputed alternate next hop to reduce failure reaction time when the primary next hop fails. You can configure a per-prefix LFA path that redirects traffic to a next hop other than the primary neighbor. See IP Routing → Configuring OSPFv2 Loop-Free Alternate IP Fast Reroute. (Network Advantage)
Private VLAN (PVLAN) on Trunk Ports and Portchannels	Enables configuration of private VLANs on isolated trunk ports, promiscuous trunk ports, and on port channels. See VLAN → Configuring Private VLANs. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • gNMI Configuration Persistence • gNOI Certificate Management • gNOI Bootstrapping with Certificate Service • YANG Data Models	The following programmability features are introduced in this release: • gNMI (gRPC Network Management Interface) Configuration Persistence: Ensures that all successful changes made through the gNMI SET RPC persist after a device restart. • gNOI Certificate Management: The gRPC Network Operations Interface (gNOI) Certificate Management service provides RPCs to install, rotate, get certificate, revoke certificate, and generate certificate signing request (CSR). • gNOI Bootstrapping with Certificate Service: After installing gNOI certificates, bootstrapping is used to configure or operate a target. gNMI bootstrapping is enabled by using the **gnxi-secure-int** command and disabled by using the **secure-allow-self-signed-trustpoint** command. • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1731. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release. (Network Essentials and Network Advantage)
Switch Integrated Security Features (SISF) - Throttling of ARP Packets	Starting with this release, ARP packets are throttled to mitigate high CPU utilization scenarios. In a five second window, a maximum of 50 ARP broadcast packets per binding entry are processed by SISF. When the limit is reached, incoming ARP packets are dropped. Note that the limit of 50 in five seconds is for each binding entry, that is, for each source IP.

New on the Web UI
There are no new features on the Web UI in this release.

Serviceability	
monitor capture match	The command was modified. The following keywords were introduced: • **packet-length**: Specifies packet length filter for packet capture • **access-list**: Specifies access-list filter for packet capture
show bootflash:	The command was modified. The following keywords were introduced: • **namesort**: Sorts the output based on file name • **sizesort**: Sorts the output based on file size • **timesort**: Sorts the output based on the timestamp of the file
show platform hardware fed active fwd-asic counters tla	• The command output was enhanced to display the TLA counters information. • The **change** keyword was deprecated.

Serviceability	
show switch stack-ports	The command was modified. The **detail** keyword was introduced. It displays the stack interface link status and errors.
show mpls ldp	The command was introduced. It provides the following options: • **show mpls ldp discovery**: Displays the status of the LDP discovery process • **show mpls ldp neighbor**: Displays the status of LDP sessions. • **show mpls ldp bindings**: Displays the contents of the Label Information Base (LIB).
show tech-support	The command was modified. The following keywords were introduced: • **show tech-support confidential**: The **confidential** keyword was introduced, to mask sensitive information in the output of **show tech-support** command. • **show tech-support monitor**: The **monitor** keyword was introduced. It displays Switched Port Analyzer (SPAN) monitor-related information. • **show tech-support pvlan**: The **pvlan** keyword was introduced. It displays Private VLAN-related information.

Important Notes

Unsupported Features

- Cisco Application Visibility and Control (AVC)
- IPsec VPN
- Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at https://cfnng.cisco.com.

Accessing Hidden Commands

This section provides information about hidden commands in Cisco IOS XE and the security measures that are in place, when they are accessed. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented.

Hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

Further, the following applies to hidden commands under Category 1 and 2:

- The commands have CLI help. Enter enter a question mark (?) at the system prompt to display the list of available commands.

  Note: For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

- The system generates a %PARSER-5-HIDDEN syslog message when a hidden command is used. For example:

  ```
  *Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
   is a hidden command.
  Use of this command is not recommended/supported and will be removed in future.
  ```

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.

Important We recommend that you use any hidden command only under TAC supervision.

If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

Default Behaviour

Beginning from Cisco IOS XE Gibraltar 16.12.5 and later, do not fragment bit (DF bit) in the IP packet is always set to 0 for all outgoing RADIUS packets (packets that originate from the device towards the RADIUS server).

Supported Hardware

Cisco Catalyst 9600 Series Switches—Model Numbers

The following table lists the supported switch models. For information about the available license levels, see section *License Levels*.

Switch Model (append with "=" for spares)	Description
C9606R	Cisco Catalyst 9606R Switch • Redundant supervisor module capability • Four linecard slots • Hot-swappable fan tray, front and rear serviceable, fan tray assembly with 9 fans. • Four power supply module slots

Supported Hardware on Cisco Catalyst 9600 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9600-SUP-1	Cisco Catalyst 9600 Series Supervisor 1 Module This supervisor module is supported on the C9606R chassis.
SATA[1] SSD[2] Modules (for the Supervisor)	
C9K-F2-SSD-240GB	Cisco Catalyst 9600 Series 240GB SSD Storage
C9K-F2-SSD-480GB	Cisco Catalyst 9600 Series 480GB SSD Storage
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage
Line Cards	
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port SFP56 line card. • C9600X-SUP-2 • 48 SFP56 ports of 50G/25G/10G • C9600X-SUP-1 • 48 SFP28 ports of 25G/10G/1G
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40G/12-Port 100G line card. • C9600X-SUP-2 • 24 QSFP28 ports of 100G/40G • C9600-SUP-1 • 12 ports of 100G or 24 ports of 40G

Product ID (append with "=" for spares)	Description
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-Port MultiGigabit RJ45 line card. • C9600X-SUP-2 • 48 ports of 10G/5G/2.5G • C9600X-SUP-1 • 48 ports of 10G/5G/2.5G/1G and 100M/10M
C9600-LC-48S	Cisco Catalyst 9600 Series 48-Port SFP line card. • C9600X-SUP-2 • Not supported • C9600-SUP-1 • 48 SFP ports of 1G
AC Power Supply Modules	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]
DC Power Supply Modules	
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module

[1] Serial Advanced Technology Attachment (SATA)
[2] Solid State Drive (SSD) Module
[3] Power supply output capacity is 1050W at 110 VAC.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9600 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.3.8a	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.8	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.7	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.6	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack See Cisco Prime Infrastructure 3.10 → **Downloads**.
Amsterdam 17.3.5	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.4	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.3	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Amsterdam 17.3.2a	2.7	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → **Downloads**.
Amsterdam 17.3.1	2.7	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → **Downloads**.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.2.1	2.7	-	PI 3.7 + PI 3.7 latest maintenance release + PI 3.7 latest device pack See Cisco Prime Infrastructure 3.7 → **Downloads**.
Amsterdam 17.1.1	2.7	-	-
Gibraltar 16.12.8	2.6	-	-
Gibraltar 16.12.7	2.6	-	-
Gibraltar 16.12.6	2.6	-	-
Gibraltar 16.12.5b	2.6	-	-
Gibraltar 16.12.5	2.6	-	-
Gibraltar 16.12.4	2.6	-	-
Gibraltar 16.12.3a	2.6	-	-
Gibraltar 16.12.3	2.6	-	-
Gibraltar 16.12.2	2.6	-	-
Gibraltar 16.12.1	2.6	-	-
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	-

Web UI System Requirements

The following subsections list the hardware and software required to access the Web UI:

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[4]	512 MB[5]	256	1280 x 800 or higher	Small

[4] We recommend 1 GHz
[5] We recommend 1 GB DRAM

Software Requirements

Operating Systems

- Windows 10 or later

- Mac OS X 10.9.5 or later

Browsers

- Google Chrome—Version 59 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox—Version 54 or later (On Windows and Mac)
- Safari—Version 10 or later (On Mac)

ROMMON Versions

ROMMON, also known as the boot loader, is firmware that runs when the device is powered up or reset. It initializes the processor hardware and boots the operating system software (Cisco IOS XE software image). The ROMMON is stored on the following Serial Peripheral Interface (SPI) flash devices on your switch:

- Primary: The ROMMON stored here is the one the system boots every time the device is powered-on or reset.
- Golden: The ROMMON stored here is a backup copy. If the one in the primary is corrupted, the system automatically boots the ROMMON in the golden SPI flash device.

ROMMON upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release.

The following table provides ROMMON version information for the Cisco Catalyst 9600 Series Supervisor Modules. For ROMMON version information of Cisco IOS XE 16.x.x releases, refer to the corresponding Cisco IOS XE 16.x.x release notes of the respective platform.

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
Amsterdam 17.3.8a	17.3.1r[FC2]	-
Amsterdam 17.3.8	17.3.1r[FC2]	-
Amsterdam 17.3.7	17.3.1r[FC2]	-
Amsterdam 17.3.6	17.3.1r[FC2]	-
Amsterdam 17.3.5	17.3.1r[FC2]	-
Amsterdam 17.3.4	17.3.1r[FC2]	-
Amsterdam 17.3.3	17.3.1r[FC2]	-
Amsterdam 17.3.2a	17.3.1r[FC2]	-
Amsterdam 17.3.1	17.3.1r[FC2]	-
Amsterdam 17.2.1	17.1.1[FC2]	-
Amsterdam 17.1.1	17.1.1[FC1]	-

Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

Note You cannot use the Web UI to install, upgrade, or downgrade device software.

Finding the Software Version

The package files for the Cisco IOS XE software are 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 Images

Release	Image Type	File Name
Cisco IOS XE Amsterdam 17.3.8a	CAT9K_IOSXE	cat9k_iosxe.17.03.08a.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.08a
Cisco IOS XE Amsterdam 17.3.8	CAT9K_IOSXE	cat9k_iosxe.17.03.08.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.08.
Cisco IOS XE Amsterdam 17.3.7	CAT9K_IOSXE	cat9k_iosxe.17.03.07.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.07.
Cisco IOS XE Amsterdam 17.3.6	CAT9K_IOSXE	cat9k_iosxe.17.03.06.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.06.
Cisco IOS XE Amsterdam 17.3.5	CAT9K_IOSXE	cat9k_iosxe.17.03.05.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.05.
Cisco IOS XE Amsterdam 17.3.4	CAT9K_IOSXE	cat9k_iosxe.17.03.04.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.04.

Release	Image Type	File Name
Cisco IOS XE Amsterdam 17.3.3	CAT9K_IOSXE	cat9k_iosxe.17.03.03.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.03.SPA
Cisco IOS XE Amsterdam 17.3.2a	CAT9K_IOSXE	cat9k_iosxe.17.03.02a.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.02a.SP
Cisco IOS XE Amsterdam 17.3.1	CAT9K_IOSXE	cat9k_iosxe.17.03.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.03.01.SPA

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 14.

You can upgrade the ROMMON before, or, after upgrading the software version. If a new ROMMON version is available for the software version you are upgrading to, proceed as follows:

- Upgrading the ROMMON in the primary SPI flash device

  This ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch when you boot up your switch with the new image for the first time.

- Upgrading the ROMMON in the golden SPI flash device

  You must manually upgrade this ROMMON. Enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.

Note

- In case of a Cisco StackWise Virtual setup, upgrade the active and standby supervisor modules.
- In case of a High Availability set up, upgrade the active and standby supervisor modules.

After the ROMMON is upgraded, it will take effect on the next reload. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

Software Installation Commands

Summary of Software Installation Commands
To install and activate the specified file, and to commit changes to be persistent across reloads: **install add file** *filename* [**activate commit**] To separately install, activate, commit, cancel, or remove the installation file: **install ?**

Summary of Software Installation Commands	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [**auto-abort-timer**]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, using **install** commands, in install mode. To perform a software image upgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

Caution You must comply with these cautionary guidelines during an upgrade:

- Do not power cycle the switch.
- Do not disconnect power or remove the supervisor module.
- Do not perform an online insertion and replacement (OIR) of either supervisor (in a High Availability setup), if one of the supervisor modules in the chassis is in the process of a bootloader upgrade or when the switch is booting up.
- Do not perform an OIR of a switching module (linecard) when the switch is booting up.

Note that you can use this procedure for the following upgrade scenarios:

When upgrading from ...	To...
Cisco IOS XE Amsterdam 17.2.x or earlier releases	Cisco IOS XE Amsterdam 17.3.x

Use the procedure described here to upgrade the device in the following configurations:

- Standalone
- Cisco StackWise Virtual
- Cisco StackWise Virtual without ISSU

The sample output in this section displays upgrade from Cisco IOS XE Amsterdam 17.2.1 to Cisco IOS XE Amsterdam 17.3.1 using **install** commands.

Procedure

Step 1 Clean-up

install remove inactive

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
install_remove: START Fri Jul 17 19:51:48 UTC 2020
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat9k-cc_srdriver.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-webui.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.02.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-wlc.17.01.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y

[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.01.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.01.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Fri Jul 17 19:52:25 UTC 2020
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp:***[[//location]/directory]/filename***flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.03.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.03.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.03.01.SPA.bin...
Loading /cat9k_iosxe.17.03.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

b) **dir flash:*.bin**

Use this command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 601216545    Jul 17 2020 10:18:11 -07:00 cat9k_iosxe.17.03.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

a) **boot system flash:packages.conf**

Use this command to set the boot variable to **flash:packages.conf**.

```
Switch(config)# boot system flash:packages.conf
```

b) **no boot manual**

Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.

```
Switch(config)# no boot manual
Switch(config)# exit
```

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar**

Use this command to verify the boot variable (packages.conf) and manual boot setting (no):

```
Switch# show bootvar
BOOT variable = bootflash:packages.conf
MANUAL_BOOT variable = no
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =

Standby BOOT variable = bootflash:packages.conf
Standby MANUAL_BOOT variable = no
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =
```

Step 4 Install image to flash

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on a TFTP server or the flash , if you have copied the image to flash memory.

The following sample output displays installation of the Cisco IOS XE Amsterdam 17.3.1 software image to flash:

```
Switch# install add file flash:cat9k_iosxe.17.03.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Jul 17 16:37:25 IST 2020

*Jul 17 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.02.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Copying image file: flash:cat9k_iosxe.17.03.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.03.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add
```

```
Image added. Version: 17.3.01

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.03.01.SPA.pkg
/flash/cat9k-webui.17.03.01.SPA.pkg
/flash/cat9k-srdriver.17.03.01.SPA.pkg
/flash/cat9k-sipspa.17.03.01.SPA.pkg
/flash/cat9k-sipbase.17.03.01.SPA.pkg
/flash/cat9k-rpboot.17.03.01.SPA.pkg
/flash/cat9k-rpbase.17.03.01.SPA.pkg
/flash/cat9k-guestshell.17.03.01.SPA.pkg
/flash/cat9k-espbase.17.03.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.03.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on Active/Standby
*Jul 17 16:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate

*Jul 17 16:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Jul 17 16:46:18 IST 2020
```

Note The system reloads automatically after executing the **install add file activate commit command**. You do not have to manually reload the system.

Step 5 Verify installation

After the software has been successfully installed, use the **dir flash:** command to verify that the flash partition has ten new .pkg files and two .conf files.

a) **dir flash:*.conf**

The following is sample output of the **dir flash:*.pkg** command:

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104    Mar 31 2020 09:52:41 -07:00 cat9k-cc_srdriver.17.02.01.SPA.pkg
475141 -rw- 70333380   Mar 31 2020 09:52:44 -07:00 cat9k-espbase.17.02.01.SPA.pkg
475142 -rw- 13256      Mar 31 2020 09:52:44 -07:00 cat9k-guestshell.17.02.01.SPA.pkg
475143 -rw- 349635524  Mar 31 2020 09:52:54 -07:00 cat9k-rpbase.17.02.01.SPA.pkg
475149 -rw- 24248187   Mar 31 2020 09:53:02 -07:00 cat9k-rpboot.17.02.01.SPA.pkg
475144 -rw- 25285572   Mar 31 2020 09:52:55 -07:00 cat9k-sipbase.17.02.01.SPA.pkg
475145 -rw- 20947908   Mar 31 2020 09:52:55 -07:00 cat9k-sipspa.17.02.01.SPA.pkg
```

```
475146 -rw- 2962372    Mar 31 2020 09:52:56 -07:00 cat9k-srdriver.17.02.01.SPA.pkg
475147 -rw- 13284288   Mar 31 2020 09:52:56 -07:00 cat9k-webui.17.02.01.SPA.pkg
475148 -rw- 13248      Mar 31 2020 09:52:56 -07:00 cat9k-wlc.17.02.01.SPA.pkg

491524 -rw- 25711568   Jul 17 2020 11:49:33 -07:00  cat9k-cc_srdriver.17.03.01.SPA.pkg
491525 -rw- 78484428   Jul 17 2020 11:49:35 -07:00  cat9k-espbase.17.03.01.SPA.pkg
491526 -rw- 1598412    Jul 17 2020 11:49:35 -07:00  cat9k-guestshell.17.03.01.SPA.pkg
491527 -rw- 404153288  Jul 17 2020 11:49:47 -07:00  cat9k-rpbase.17.03.01.SPA.pkg
491533 -rw- 31657374   Jul 17 2020 11:50:09 -07:00  cat9k-rpboot.17.03.01.SPA.pkg
491528 -rw- 27681740   Jul 17 2020 11:49:48 -07:00  cat9k-sipbase.17.03.01.SPA.pkg
491529 -rw- 52224968   Jul 17 2020 11:49:49 -07:00  cat9k-sipspa.17.03.01.SPA.pkg
491530 -rw- 31130572   Jul 17 2020 11:49:50 -07:00  cat9k-srdriver.17.03.01.SPA.pkg
491531 -rw- 14783432   Jul 17 2020 11:49:51 -07:00  cat9k-webui.17.03.01.SPA.pkg
491532 -rw- 9160       Jul 17 2020 11:49:51 -07:00  cat9k-wlc.17.03.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

b) **dir flash:*.conf**

The following is sample output of the **dir flash:*.conf** command. It displays the .conf files in the flash partition; note the two .conf files:

- `packages.conf`—the file that has been re-written with the newly installed .pkg files.
- `cat9k_iosxe.17.03.01.SPA.conf`— a backup copy of the newly installed packages.conf file.

```
Switch# dir flash:*.conf

Directory of flash:/*.conf
Directory of flash:/

16631  -rw- 4882 Jul 17 2020 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Jul 17 2020 05:34:06 +00:00  cat9k_iosxe.17.03.01.SPA.conf
```

Step 6 Upgrade the ROMMON version

upgrade rom-monitor capsule golden

A new ROMMON version is available for Cisco IOS XE Amsterdam 17.3.1. After you enter the command, confirm upgrade at the system prompt.

In case of a high availability set up or a Cisco StackWise Virtual set up, remember to upgrade the active and standby.

```
Switch# upgrade rom-monitor capsule golden R0
This operation will reload the switch and take a few minutes to complete. Do you want to
proceed (y/n)? [confirm]y
Switch#
Initializing Hardware...
<output truncated>
```

For more information about this, see Upgrading the ROMMON, on page 16 in this document.

Step 7 Verify version

show version

After the image boots up, use this command to verify the version of the new image.

The following sample output of the **show version** command displays the Cisco IOS XE Amsterdam 17.3.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.03.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc..
<output truncated>
```

Downgrading in Install Mode

Follow these instructions to downgrade from one release to another, in install mode. To perform a software image downgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

Note that you can use this procedure for the following downgrade scenarios:

When downgrading from ...	To ...
Cisco IOS XE Amsterdam 17.3.x	Cisco IOS XE Amsterdam 17.2.x or earlier releases.

Note New switch models that are introduced in a release cannot be downgraded. The release in which a module is introduced is the minimum software version for that model. We recommend upgrading all existing hardware to the same release as the latest hardware.

Use the procedure described here to downgrade the device in the following configurations:

- Standalone
- Cisco StackWise Virtual
- Cisco StackWise Virtual without ISSU

The sample output in this section shows downgrade from Cisco IOS XE Amsterdam 17.3.1 to Cisco IOS XE Amsterdam 17.2.1, using **install** commands.

Procedure

Step 1 Clean-up

install remove inactive

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
 install_remove: START Fri Jul 17 11:42:27 IST 2020

Cleaning up unnecessary package files
```

```
No path specified, will use booted path bootflash:packages.conf

Cleaning bootflash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k-cc_srdriver.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-srdriver.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-webui.17.03.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.17.03.01.SSA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.

SUCCESS: install_remove  Fri Jul 17 11:42:39 IST 2020

--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Fri Jul 17 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp:***[[//location]/directory]/filename***flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.02.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.02.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.02.01.SPA.bin...
Loading /cat9k_iosxe.17.02.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

b) **dir flash:**

Use this command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 508584771 Jul 17 2020 13:35:16 -07:00 cat9k_iosxe.17.02.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Set boot variable

a) **boot system flash:packages.conf**

Use this command to set the boot variable to **flash:packages.conf**.

```
Switch(config)# boot system flash:packages.conf
```

b) **no boot manual**

Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.

```
Switch(config)# no boot manual
Switch(config)# exit
```

c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

d) **show bootvar**

Use this command to verify the boot variable (packages.conf) and manual boot setting (no):

```
Switch# show bootvar
BOOT variable = bootflash:packages.conf
MANUAL_BOOT variable = no
BAUD variable = 9600
ENABLE_BREAK variable = yes
BOOTMODE variable does not exist
IPXE_TIMEOUT variable does not exist
CONFIG_FILE variable =

Standby BOOT variable = bootflash:packages.conf
Standby MANUAL_BOOT variable = no
Standby BAUD variable = 9600
Standby ENABLE_BREAK variable = yes
Standby BOOTMODE variable does not exist
Standby IPXE_TIMEOUT variable does not exist
Standby CONFIG_FILE variable =
```

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on a TFTP server or the flash , if you have copied the image to flash memory.

The following example displays the installation of the Cisco IOS XE Amsterdam 17.2.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.02.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Jul 17 21:37:25 IST 2020
```

```
*Jul 17 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.02.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Copying image file: flash:cat9k_iosxe.17.02.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.02.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add

Image added. Version: 17.02.1
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.02.01.SPA.pkg
/flash/cat9k-webui.17.02.01.SPA.pkg
/flash/cat9k-srdriver.17.02.01.SPA.pkg
/flash/cat9k-sipspa.17.02.01.SPA.pkg
/flash/cat9k-sipbase.17.02.01.SPA.pkg
/flash/cat9k-rpboot.17.02.01.SPA.pkg
/flash/cat9k-rpbase.17.02.01.SPA.pkg
/flash/cat9k-guestshell.17.02.01.SPA.pkg
/flash/cat9k-espbase.17.02.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.02.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on Active/Standby

*Jul 17 21:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate


*Jul 17 21:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit
```

```
Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Jul 17 21:46:18 IST 2020
```

Note The system reloads automatically after executing the **install add file activate commit** command. You do not have to manually reload the system.

Step 5 Verify version

show version

After the image boots up, use this command to verify the version of the new image.

Note When you downgrade the software image, the ROMMON version does not downgrade. It remains updated.

The following sample output of the **show version** command displays the Cisco IOS XE Amsterdam 17.2.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.02.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.2.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

In Service Software Upgrade (ISSU) with Cisco StackWise Virtual and Dual Supervisor Module Configuration

Follow the instructions described here to perform an In Service Software Upgrade (ISSU) upgrade. Use the procedure described here, only for the releases indicated in the table below. For more general information about ISSU release support and recommended releases, see this technical reference document: In-Service Software Upgrade (ISSU).

Before you begin

Note that you can use this ISSU procedure only for the following scenarios:

When upgrading from...	Use these commands...	To...
Cisco IOS XE Amsterdam 17.3.1	**install add file activate issu commit**	Cisco IOS XE Amsterdam 17.3.x
Not applicable	ISSU does not support downgrade. To downgrade, see Downgrading in Install Mode, on page 23.	Not applicable

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Switch# enable
```

Step 2 **install add file activate issu commit**

Use this command to automate the sequence of all the upgrade procedures, including downloading the images to both the switches, expanding the images into packages, and upgrading each switch as per the procedures.

```
Switch# install add file tftp:cat9k_iosxe.17.3.02.SPA.bin activate issu commit
```

The following sample output displays installation of Cisco IOS XE Amsterdam 17.3.2a software image with ISSU procedure.

```
Switch# install add file tftp:cat9k_iosxe.17.03.02.SPA.bin activate issu commit
install_add_activate_commit: START Thu Nov 19 06:16:32 UTC 2020
Downloading file tftp://172.27.18.5//cat9k_iosxe.17.03.02.SPA.bin

*Nov 19 06:16:34.064: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
 install one-shot ISSU tftp://172.27.18.5//cat9k_iosxe.17.03.02.SPA.bin
Finished downloading file tftp://172.27.18.5//cat9k_iosxe.17.03.02.SPA.bin to
flash:cat9k_iosxe.17.03.02.SPA.bin
install_add_activate_commit: Adding ISSU

--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.17.03.02.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.17.03.02.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on switch 1
  [1] Finished Add on switch 1
  [2] Add package(s) on switch 2
  [2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

install_add_activate_commit: Activating ISSU

NOTE: Going to start Oneshot ISSU install process

STAGE 0: Initial System Level Sanity Check before starting ISSU
===================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
Finished Initial System Level Sanity Check


STAGE 1: Installing software on Standby
===================================================
--- Starting install_remote ---
Performing install_remote on Chassis remote
[2] install_remote package(s) on switch 2
[2] Finished install_remote on switch 2
install_remote: Passed on [2]
Finished install_remote


STAGE 2: Restarting Standby
===================================================
--- Starting standby reload ---
Finished standby reload
```

```
--- Starting wait for Standby to reach terminal redundancy state ---

*Nov 19 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Nov 19 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Nov 19 06:24:16.466: %HMANRP-5-CHASSIS_DOWN_EVENT: Chassis 2 gone DOWN!
*Nov 19 06:24:16.497: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Nov 19 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Nov 19 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Nov 19 06:24:16.674: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Nov 19 06:24:16.679: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected switch 2 is no longer
 standby
*Nov 19 06:24:16.416: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1 R0/0: nif_mgr: Port 1 on front
side stack link 0 is DOWN.
*Nov 19 06:24:16.416: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 1 R0/0: nif_mgr: Port 1 on
 front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Nov 19 06:24:16.416: %NIF_MGR-6-STACK_LINK_DOWN: Switch 1 R0/0: nif_mgr: Front side stack
 link 0 is DOWN.
*Nov 19 06:24:16.416: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port
1 on Switch 1 is down

<output truncated>

*Nov 19 06:29:36.393: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Nov 19 06:29:36.392: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has
been elected STANDBY.
*Nov 19 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))
*Nov 19 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Nov 19 06:29:42.257: %REDUNDANCY-3-IPC: IOS versions do not match.
*Nov 19 06:30:24.323: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeededFinished
wait for Standby to reach terminal redundancy state


*Nov 19 06:30:25.325: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
STAGE 3: Installing software on Active
===================================================
--- Starting install_active ---
Performing install_active on Chassis 1

<output truncated>

[1] install_active package(s) on switch 1
[1] Finished install_active on switch 1
install_active: Passed on [1]
Finished install_active


STAGE 4: Restarting Active (switchover to standby)
===================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_add_activate_commit  Thu Nov 19 23:06:45 UTC 2020
Nov 19 23:06:45.731: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot ISSU flash:cat9k_iosxe.17.03.02.SPA.bin
Nov 19 23:06:47.509: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Nov 19 23:06:48.776: %PM

Initializing Hardware...

System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)
Compiled Fri 08/17/2018 10:48:42.68 by rel
```

```
Current ROMMON image : Primary
Last reset cause     : PowerOn
C9500-40X platform with 16777216 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
##################################################################################################################################################################################################################



Nov 19 23:08:30.238: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:

Waiting for 120 seconds for other switches to boot
######################
Switch number is 1
All switches in the stack have been discovered. Accelerating discovery



Switch console is now available


Press RETURN to get started.






Nov 19 23:14:17.080: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit
Nov 19 23:15:48.445: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit ISSU
```

Step 3 **show version**

Use this command to verify the version of the new image.

The following sample output of the **show version** command displays the Cisco IOS XE Amsterdam 17.3.2a image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.2,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
<output truncated>
```

Step 4 **show issu state** [*detail*]

Use this command to verify that no ISSU process is in pending state.

```
Switch# show issu state detail
--- Starting local lock acquisition on chassis 2 ---
Finished local lock acquisition on chassis 2

No ISSU operation is in progress

Switch#
```

Step 5 **exit**

Exits privileged EXEC mode and returns to user EXEC mode.

Field-Programmable Gate Array Version Upgrade

A field-programmable gate array (FPGA) is a type of programmable memory device that exists on Cisco switches. They are re-configurable logic circuits that enable the creation of specific and dedicated functions.

To check the current FPGA version, enter the **show firmware version all** command in IOS mode or the **version -v** command in ROMMON mode.

Note

- Not every software release has a change in the FPGA version.
- The version change occurs as part of the regular software upgrade and you do not have to perform any other additional steps. The version is not downgraded when you downgrade the software image.

Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 9000 Series Switches.

License Levels

The software features available on Cisco Catalyst 9600 Series Switches fall under these base or add-on license levels.

Base Licenses

- Network Advantage

Add-On Licenses

Add-On Licenses require a Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Advantage

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://cfnng.cisco.com. An account on cisco.com is not required.

Available Licensing Models and Configuration Information

- Cisco IOS XE Gibraltar 16.11.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.

In the software configuration guide of the required release, see **System Management** → **Configuring Smart Licensing**.

- Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

  In the software configuration guide of the required release (17.3.x onwards), see **System Management** → **Smart Licensing Using Policy**.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

License Levels - Usage Guidelines

- The duration or term for which a purchased license is valid:

Smart Licensing Using Policy	Smart Licensing
• Perpetual: There is no expiration date for such a license. • Subscription: The license is valid only until a certain date (for a three, five, or seven year period).	• Permanent: for a license level, and without an expiration date. • Term: for a license level, and for a three, five, or seven year period. • Evaluation: a license that is not registered.

- Base licenses (Network-Advantage) are ordered and fulfilled only with a perpetual or permanent license type.
- Add-on licenses (DNA Advantage) are ordered and fulfilled only with a subscription or term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload. This applies only to *Smart Licensing*. The notion of evaluation licenses does not apply to *Smart Licensing Using Policy*.

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9600 Series Switches datasheets at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-ser-sup-eng-data-sheet-cte-en.html

Limitations and Restrictions

- Auto negotiation: The SFP+ interface (TenGigabitEthernet0/1) on the Ethernet management port with a 1G transceiver does not support auto negotiation.
- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Convergence: During SSO, a higher convergence time is observed while removing the active supervisor module installed in slot 3 of a C9606R chassis.
- Hardware Limitatons — Optics:
  - Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapater —This adapter must not be installed on an even numbered port where the corresponding odd numbered port is configured as 40GE port. For example, if port 1 is configured as 40GE, CVR-QSFP-SFP10G must not be installed in port 2.

    Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapater — If you insert a 40-Gigabit Ethernet Transceiver Module to odd numbered port, the corresponding even numbered port does not work with CVR-QSFP-SFP10G adapter.
- Hardware Limitatons — Power Supply Modules:
  - Input voltage for AC power supply modules—All AC-input power supply modules in the chassis must have the same AC-input voltage level.
  - Using power supply modules of different types—When mixing AC-input and DC-input power supplies, the AC-input voltage level must be 220 VAC.
- In-Service Software Upgrade (ISSU)
  - While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
  - If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
  - If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.

  - When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

    Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- Smart Licensing Using Policy: Starting with Cisco IOS XE Amsterdam 17.3.2a, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

  The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.

- USB Authentication—When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

  ```
  Device(config)# password encryption aes
  Master key change notification called without new or old key
  ```

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.

- HTTP Services Restriction—If you configure **ip http active-session-modules none** and **ip http secure-active-session-modules none** commands, NGINX process will be held down. This will prevent HTTP or HTTPS from running. Use the **ip http session-module-list** command to enable the required HTTP modules.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.

- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.

- The File System Check (fsck) utility is not supported in install mode.

Caveats

Caveats describe unexpected behavior in Cisco IOS-XE 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 XE Amsterdam 17.3.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8a

Identifier	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6

Identifier	Description
CSCvx38149	Switch crash while removing private vlan mapping from port-channel interface.
CSCwa83315	IOS-FMAN-PTP ERROR: seen on console during issu

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5

Identifier	Description
CSCvs33050	SVL Hung - CPU HOG by Process - "Crimson Flush Transaction"
CSCvv79275	chassis 2 PS0 not getting SYS log message on OIR – inconsistent
CSCvv91195	1 Gigabit Fiber SFPs may not link up in C9600-LC-48YL module
CSCvx38654	Memory leakage is getting incremented whenever dnac-ca crl fails
CSCvx94276	%CRIMSON-3-DATABASE_MEMLEAK: Database memory leak detected in /tmp/rp/tdldb/0/IOS_PRIV_OPER_DB

Identifier	Description
CSCvy13512	Fragmented ESP packets not forwarded
CSCvy51582	SNMP: sub-interface octet counter reports wrong value
CSCvz01398	Incorrect L3 LISP instance ID on Cef table for VN's
CSCvz32969	Cat9k | DHCP unicast ACK not forwarded to the client when DHCP snooping is enabled
CSCwa17838	Stackwise virtual drop ARP request in secondary private VLAN after reload

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.4

Identifier	Description
CSCvt16172	Wrong values for transceivers (DOM) in Cat9k Core switches
CSCvt34738	SVL // DHCP discover relayed in a different vlan
CSCvv82819	Manually configured MAC address is programmed in hardware when interface is admin down
CSCvv97807	Netconf & Netconf-yang are not enabled on the Ext-Nodes as part of PnP config.
CSCvv97823	Yang requests from DNAC to IoT devices related to device Licensing are failing on the device
CSCvw13923	Vlan randomly stop forwarding DHCP pkts - Wedged input interface queue
CSCvw32545	STACK : Stale mac entry in the member switch causing the connectivity issues.
CSCvw51810	Disruption of IP communication due to AUTH_DRIVEN_DROP on uplinks when flapping downlink ports
CSCvw77744	Inconsistant syslog generation when power cycle done on PSUs on standby switch
CSCvx06374	Profinet (PN-PTCP) frames overwhelming L2 Control CoPP queue on Cat9K
CSCvx25344	Private Native Vlan packets are erroneously tagged
CSCvx60124	Traffic failed if incoming interface MPLS and 2+ outgoing interfaces (ECMP) with recursive routing
CSCvx83266	DHCP snooping and PVLAN dropping DHCP Offer unicast packet on C9K
CSCvx87277	Cat9XXX may experience an unexpected reboot with Critical process fed fault on fp_0_0
CSCvx94722	Radius protocol generate jumbo frames for dot1x packets
CSCvy02075	Switch forwards traffic received on ports in blocking BLK state
CSCvy07376	Catalyst 9K Switch may crash on ISSU upgrade if run debug issu all

Identifier	Description
CSCvy15243	Cat9600 silent reload due to CpuCatastrophicError

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Identifier	Description
CSCvt33159	SVL Crash when performing SUP failover on a scaled setup
CSCvt73669	Ports remains in notconnect state when moved from L2 to L3 to L2
CSCvu38231	Configuring reserved PO 127 & 128 in SVL setup disables show etherchannel CLI
CSCvu90016	Catalyst 9k: FED crash after reaching webauth scale of about 1k sessions
CSCvv26018	Loopback error is not detected on trunk interface
CSCvv27849	Unexpected reload caused by the FED process.
CSCvv39593	'SL using Policy' to SL downgrade to 16.12.4 leads to \"Initial Registration-First Attempt Pending\"
CSCvv40631	Catalyst 9606 40Gb port bounce when DWDM failover
CSCvv56278	Dot1x Client mac in dropped state post switchover
CSCvv79293	Te0/1: Error reading DOM data from transceiver
CSCvv88670	[SDA] SISF marking mac as tentative
CSCvw04604	Standby chassis goes for continuous reload and active switch crashed with template mismatch
CSCvw17639	Traceback: C9600 LineCard IDPROM read failure generates Fatal call
CSCvw18461	Switch Crashes when enabling RSPAN Destination port
CSCvw20225	Cat9k switches may roll back to old software after unexpected switchover event
CSCvw28418	VRF leaking using self-GRE tunnels causes traffic to be punted to CPU.
CSCvw32481	EVPN Type-2 IP/MAC route is created for not-connected SVI

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.2a

Identifier	Description
CSCvq13832	Whenever Acct-terminate-cause is 24 the duplicate set of traffic counts is sent as 0.
CSCvt18739	Cat9K - incorrect source mac address used for L3 packets after L3 link flap
CSCvt25139	%PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled interrupt

Identifier	Description
CSCvt93918	Cat9k reboot due to ACL count being huge.
CSCvt95680	Unexpected Reload when a VLAN is created within the range 2-1002
CSCvu24011	Interface Not Passing Traffic after Boot-up with IE 3400 with forced speed/duplex setting on IE
CSCvu25931	DHCPv6 RELAY-REPLY dropped when punted on cat9k
CSCvu51611	Quadsup:lacp l3 PO is going down on active sw power-off or switchover
CSCvu52246	sessmgrd memory leak when CTS PAC download fails
CSCvu53267	Failed Identification Test for C9600-SUP-1 log message appearing after bootup
CSCvu62273	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading
CSCvu82477	Random L3 ports stop traffic processing on SDA internal border nodes
CSCvu94010	Cat9k Active stack switch crash while applying the CTS configuration
CSCvv16874	CAT9K: PRD18: SISF Crash seen on device when left traffic running overnight
CSCvv24756	In SVL, syslog is not getting generated for PS0 status of standby switch after SSO intermittently
CSCvv26075	On Auth port, timestamp update is not happening for Authz MAC address upon RX of control-plane/BPDU
CSCvv33848	value 9 being displayed when snmp walk on the OID cefcFRUPowerOperStatus for PSU after SSO sometimes
CSCvv34688	IPv6 communication stops working post applying ipv6 source-guard on interface
CSCvv35565	L3 ECMP load balancing not working as expected for fragmented packets.
CSCvv44720	IPV4 and IPV6 Per-User ACL is not working together on singe authentication session
CSCvv45801	inconsistent behaviour for autoconf template binding after switchover
CSCvv48305	Route not fully programmed in the hardware for macsec enabled end-point
CSCvv69764	Dot1Q Native vlan tag is ignored after configuring Layer2 Vlan on 16.12.4 code
CSCvv77355	Cat9k in VXLAN with directed-broadcast on egress interface duplicates broadcast traffic
CSCvv86246	CAT9K reload due to "Critical process cmand fault on rp_0_0 (rc=139)"

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.1

Identifier	Description
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvs14673	SVL node may get removed if one of the SVL links goes bad.
CSCvs15485	Cat9k PoE models - when configuring speed 100 and duplex full on both sides, interface will not come up
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs39968	CAT 9500 & 9600 crashes on transceiver insertion
CSCvs84212	DHCP server sends out a NAK packet during DHCP renewal process.
CSCvs89792	INJECT_FEATURE_ESCAPE: Egress IP packet delivered via legacy inject path for NetBios packets
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt13518	QoS ACL matching incorrectly when udp range is used
CSCvt35095	Connection for L3 interfaces and SVIs may go down when power cycled SVL active switch comes online.
CSCvt59448	LACP link suspend or PAgP link getting into error-disabled if stack-mac persistent timer is set
CSCvt99199	MACSEC issue in SDA deployment
CSCvu87973	Catalyst 9600 cannot further fragment multicast fragments

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 at this URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

All support documentation for Cisco Catalyst 9600 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9600-series-switches/tsd-products-support-series-home.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.

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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)