Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Amsterdam 17.2.x

First Published: 2020-03-30

Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS XE Amsterdam 17.2.x

Introduction

Cisco Catalyst 9200 Series Switches are entry level enterprise-class access switches that extend the power of intent-based networking and Cisco Catalyst 9000 Series Switches hardware and software innovation to a broader scale of deployments. These switches focus on offering features for the mid-market and simple branchdeployments. With its family pedigree, Cisco Catalyst 9200 Series Switches offer simplicity without compromise - it is secure, always on and provides IT simplicity.

As a foundational building block for Cisco Digital Network Architecture, this platform is built with security, mobility, cloud and IoT at its core. This gives you out of the box upgrades in security, resiliency and programmability regardless of where you are in the intent-based networking journey.

With access to Cisco’s best in class security portfolio anchored trustworthy solutions, MACsec encryption and segmentation, the platform provides advanced security features that protect the integrity of the hardware as well as the software and all data that flows through the switch and the network. These switches provide enterprise-level resiliency and keep your business up and running seamlessly with field-replaceable power supplies and fans, modular uplinks, cold patching, perpetual PoE, and the industry’s highest mean time between failures (MTBF). Combine the application visibility of full flexible NetFlow with telemetry and the open APIs of Cisco IOS XE and programmability of the UADP ASIC technology and these switches give you the best simple experience provisioning and managing your network now with investment protection on future innovations.

Whats New in Cisco IOS XE Amsterdam 17.2.1

Hardware Features in Cisco IOS XE Amsterdam 17.2.1

Feature Name	Description and Documentation Link
Cisco Catalyst 9200 Series Switches (C9200-24PB, C9200-48PB)	These new switch models with support for 32 VRFs are introduced: • C9200-24PB • C9200-48PB For information about the hardware, see the Cisco Catalyst 9200 Series Switches Hardware Installation Guide.

Feature Name	Description and Documentation Link
Cisco SFP-25G Direct-Attach and Active Optical Cables	• Supported active optical cable: SFP-25G-AOC4M • Supported direct-attach copper cable product numbers: • SFP-H25G-CU1.5M • SFP-H25G-CU2.5M • SFP-H25G-CU4M • Compatible switch models: C9200 and C9200L SKUs For information about these cables, see Cisco 25GBASE SFP28 Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Amsterdam 17.2.1

Feature Name	Description, Documentation Link, and License Level Information
Factory Reset with 3-pass Overwrite	Enables factory reset with 3-pass overwrite. A secure 3-pass keyword has been introduced. • Pass 1: Overwrites all addressable locations with binary zeroes. • Pass 2: Overwrites all addressable locations with binary ones. • Pass 3: Overwrites all addressable locations with a random bit pattern. See System Management → Performing Factory Reset. (Network Essentials and Network Advantage)
IPv6: HTTP SGACL enforcement with IPv6 Policy Server	Supports 8 IPv4 and 8 IPv6 addresses per server for SGACL and Environment Data Download over REST. See Cisco TrustSec → SGACL and Environment Data Download over REST. (Network Advantage)
Loop Detection Guard	Provides a way of detecting network loops. The feature can be used in situations where there may be unmanaged switches in a network that do not understand Spanning Tree Protocol (STP) or where STP is not configured on the network. You can take one of these actions when a loop is detected: error-disable either the source port or the destination port, or have the system display a syslog message (and not disable a port). See Layer 2 → Configuring Loop Detection Guard. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Multiple Administrative VLANS in Resilient Ethernet Protocol (REP)	You can now configure multiple administrative VLANs to manage an REP domain that has multiple REP segments that are mutually exclusive. Configure the additional administrative VLANs by entering the **rep admin vlan** command in global configuration mode. See Layer 2 → Configuring Resilient Ethernet Protocol. (Network Essentials and Network Advantage)
Programmability • TLDP On-Change Notifications • YANG Data Models	The following programmability features are introduced in this release: • TLDP On-Change Notifications: Notifies users when Targeted Label Distribution Protocol (TLDP) sessions come up or go down and when TLDP is configured or disabled. TLDP must be enabled for the notifications to work. (Network Essentials and Network Advantage) • 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/1721. 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) See Programmability.
SCP Performance Improvements	Secure Shell (SSH) bulk data transfer mode can now be used to enhance the throughput performance of Secure Copy Protocol (SCP) operating in the capacity of a client or server. You can enable this by using the **ip ssh bulk-mode** global configuration command. See System Management → Secure Copy. (Network Essentials and Network Advantage)
Session Limit - To prevent MAC address flooding DOS attack	Enables you to configure an access session limit profile, which will allow you to limit the number of voice and data hosts connecting to a port. See Security → Configuring IEEE 802.1x Port-Based Authentication. (Network Essentials and Network Advantage)
VLAN Load Balancing for FlexLink+	Introduces support for VLAN load balancing on a FlexLink+ pair (along with providing the redundancy). Both ports of a FlexLink+ pair can now simultaneously forward traffic in mutually exclusive VLANs. If one of the ports fail, the other active port forwards all traffic. When the failed port is available again, it resumes forwarding of traffic in the preferred VLANs. See Layer 2 → Configuring Flexlink+. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
VRFs	The C9200-24PB and C9200-48PB models of the Cisco Catalyst 9200 Series Switches support 32 VRFs. See IP Routing → Configuring Multi-VRF CE and Stack Manager and High Availability → Managing Switch Stacks. (Network Advantage)
VRF Support for TCL Socket	The Tool Command Language (TCL) socket feature supports Virtual Routing and Forwarding (VRF). See Network Management Commands. (Network Essentials and Network Advantage)

New on the Web UI	
• HSRP • Passwordless Login	Use the WebUI for: • HSRP: Provides high network availability by providing redundancy for IP traffic from hosts on networks. • Passwordless Login: Supports login to WebUI without password using Personal Identity Verification (PIV) compatible smart cards.

Serviceability	
See Command Reference, Cisco IOS XE Amsterdam 17.2.x (Catalyst 9200 Switches)	
factory-reset	The command has been modified. The **switch** keyword is introduced for devices that support stacking. You can perform factory reset on all the switches or on a specificed switch in a stack.
show platform hardware fed switch active fwd-asic resource tcam utilization	The command output is enhanced to display TCAM utilization categorised by IPv4, IPv6, MPLS and other protocols.
debug condition vrf **debug ip pim** **debug ipv6 pim**	The **debug condition vrf** and **debug ip pim** commands enable you to debug multiple VRFs at the same time. The **debug ipv6 pim** introduces IPv6 support for debugging multiple VRFs at the same time.

Important Notes

Unsupported Features

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Border Gateway Protocol (BGP) including BGP EVPN VXLAN.
- Cisco StackWise Virtual
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Fabric Enabled Wireless on C9200L SKUs
- Gateway Load Balancing Protocol (GLBP)
- Hot patching (for SMUs)
- IPsec VPN
- MACSec Encryption
  - MACsec configuration on EtherChannel
  - 256-bit AES MACsec (IEEE 802.1AE) host link encryption with MACsec Key Agreement (MKA)
- Multiprotocol Label Switching (MPLS)
- Non Stop Forwarding (NSF)
- Performance Monitoring (PerfMon)
- Programmability (Cisco Plug-in for OpenFlow 1.3, Third-Party Application Hosting)
- Virtual Routing and Forwarding (VRF)-Aware web authentication
- Web Cache Communication Protocol (WCCP)

Complete List of Supported Features

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

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 9200 Series Switches—Model Numbers

The following table lists the supported hardware models and the default license levels they are delivered with. For information about the available license levels, see section *License Levels*.

[1] See Table: Table 1: Permitted Combinations, on page 21, for information about the add-on licenses that you can order.

Network Modules

The following table lists the optional uplink network modules with 1-GigabitEthernet and 10-GigabitEthernet slots. You should only operate the switch with either a network module or a blank module installed.

Network Module	Description
C9200-NM-4G [1]	Four 1-GigabitEthernet SFP module slots
C9200-NM-4X [1]	Four 10-GigabitEthernet SFP+ module slots
C9200-NM-2Y[2]	Two 25-GigabitEthernet SFP28 module slots

Network Module	Description
C9200-NM-2Q[2]	Two 40-GigabitEthernet slots with a QSFP+ connector in each slot

Note These network modules are supported only on the C9200 SKUs of the Cisco Catalyst 9200 Series Switches.

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 9200 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Amsterdam 17.2.1	2.7	C9200 and C9200L: 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	C9200 and C9200L: PI 3.6 + PI 3.6 latest maintenance release + PI 3.6 latest device pack See Cisco Prime Infrastructure 3.6 → **Downloads**.
Gibraltar 16.12.8	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.7	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.6	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5b	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Gibraltar 16.12.5	2.6	C9200 and C9200L: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.4	2.6	C9200 and C9200L: PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.2	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	C9200 and C9200L: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.11.1	2.6 2.4 Patch 5	C9200 and C9200L: PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4 → **Downloads**.
Gibraltar 16.10.1	2.4	C9200: PI 3.4 + Device Pack 9 C9200L: PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.8	2.5 2.1	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9200	Cisco Identity Services Engine	Cisco Prime Infrastructure
Fuji 16.9.5	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2[2]	2.4	PI 3.4 + Device Pack 7 See Cisco Prime Infrastructure 3.4→ **Downloads**.

[2] The compatibility information for Fuji 16.9.2 applies only to the C9200L SKUs.

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[3]	512 MB[4]	256	1280 x 800 or higher	Small

[3] We recommend 1 GHz
[4] 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)

Boot Loader Versions

The following table provides boot loader version information for the Cisco Catalyst 9200 Series Switches.

Release	ROMMON Version
Amsterdam 17.2.1	17.2.1r [FC2]
Amsterdam 17.1.1	17.1.1 [FC3]

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 17.2.1	CAT9K_LITE_IOSXE	cat9k_lite_iosxe.17.02.01.SPA

Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated boot loader supports all previous releases.

Caution Do not power cycle your switch during the upgrade.

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 ?`	
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, in install mode. To perform a software image upgrade, you must be booted into IOS through **boot flash:packages.conf**.

Before you begin

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

When upgrading from ...	To...
Cisco IOS XE Amsterdam 17.1.x or earlier releases	Cisco IOS XE Amsterdam 17.2.1

The sample output in this section displays upgrade from Cisco IOS XE Amsterdam 17.1.1 to Cisco IOS XE Amsterdam 17.2.1 using **install** commands.

Procedure

Step 1 Clean Up

a) **install remove inactive**

Use this command to clean up unused installation files in case of insufficient space. Ensure that you have at least 1GB of space in flash to expand a new image.

```
Switch# install remove inactive
install_remove: START Mon Mar 23 17:46:18 IST 2019
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k_lite-rpbase.17.01.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.01.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.01.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.01.01.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_lite_iosxe.17.01.01.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.01.01.SPA.bin ... 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  Mon Mar 23 17:47:20 IST 2020
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

Use this command to copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

```
Switch# copy tftp://10.8.0.6//cat9k_lite_iosxe.17.02.01.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.02.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.02.01.SPA.bin...
Loading /cat9k_lite_iosxe.17.02.01.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**

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 Mar 23 2020 10:18:11 -07:00 cat9k_lite_iosxe.17.02.01.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
Switch(config)# exit
```

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

The output should display **BOOT variable** = **flash:packages.conf**.

```
Switch# show boot system
```

Step 4 Software install image to flash

a) **install add file activate commit**

Use this command to install the target image. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

```
Device# install add  file
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/cat9k_lite_iosxe.17.02.01.SPA.bin activate
 commit


*Mar 23 12:51:38.722 IST: %PLATFORM-4-ELEMENT_WARNING: Switch 1 R0/0: smand: 1/RP/0:
flash: usage has returned to appropriate level value 29% (547 MB) is below warning level
 70% (1337 MB).
install_add_activate_commit: START Mon Mar 23 12:51:55 IST 2020
Mar 23 12:51:57.795: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 one-shot tftp://203.0.113.1/auto/tftp-ex-user0/exuser/cat9k_lite_iosxe.17.02.01.SPA.bin
Downloading file
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/cat9k_lite_iosxe.17.02.01.SPA.bin
*Mar 23 12:51:57.758 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
 Started install one-shot
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/cat9k_lite_iosxe.17.02.01.SPA.bin
*Mar 23 12:51:59.370 IST: %IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'fts bipc'
 has taken 504 msec (runtime: 412 msec) to process a 'req_binos_copy_info' message
Finished downloading file
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/cat9k_lite_iosxe.17.02.01.SPA.bin to
flash:cat9k_lite_iosxe.17.02.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.17.02.01.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
```

```
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: 17.02.01.0.276
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.02.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.02.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.02.01.SPA.pkg
/flash/cat9k_lite-rpbase.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 all members
Mar 23 13:03:24.337: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds
  [1] Activate package(s) on switch 1
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.17.01.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.01.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.01.01.SPA.pkg
      Removed cat9k_lite-webui.17.01.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.02.01.SPA.pkg
      Added cat9k_lite-rpboot.17.02.01.SPA.pkg
      Added cat9k_lite-srdriver.17.02.01.SPA.pkg
      Added cat9k_lite-webui.17.02.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

*Mar 23 13:03:24.298 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds--- Starting Commit
 ---
Performing Commit on all members
  [1] Commit package(s) on switch 1
  [1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Mar 23 13:04:23 IST 2020
Mar 23 13:04:24.586: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install one-shot PACKAGE flash:cat9k_lite_iosxe.17.02.01.SPA.bin
Mar 23 13:04:24.586 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.02.01.SPA.bin
```

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

b) **dir flash:**

After the software has been successfully installed, use this command to verify that the flash partition has four new `.pkg` files and two `.conf` files.

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/

48582  -rw- 298787860 Nov 26 2019 05:13:32 +00:00  cat9k_lite-rpbase.17.01.01.SPA.pkg
48585  -rw- 35713901  Nov 26 2019 05:14:12 +00:00  cat9k_lite-rpboot.17.01.01.SPA.pkg
48583  -rw- 4252692   Nov 26 2019 05:13:33 +00:00  cat9k_lite-srdriver.17.01.01.SPA.pkg
48584  -rw- 8119312   Nov 26 2019 05:13:34 +00:00  cat9k_lite-webui.17.01.01.SPA.pkg

16640  -rw- 301188116 Mar 23 2020 05:33:25 +00:00  cat9k_lite-rpbase.17.02.01.SPA.pkg
16647  -rw- 35112025  Mar 23 2020 05:34:06 +00:00  cat9k_lite-rpboot.17.02.01.SPA.pkg
16642  -rw- 4326420   Mar 23 2020 05:33:25 +00:00  cat9k_lite-srdriver.17.02.01.SPA.pkg
16643  -rw- 8328208   Mar 23 2020 05:33:25 +00:00  cat9k_lite-webui.17.02.01.SPA.pkg
```

The following sample output 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_lite_iosxe.17.02.01.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  Mar 23 2020 05:39:42 +00:00  packages.conf
16634 -rw- 4882  Mar 23 2020 05:34:06 +00:00  cat9k_lite_iosxe.17.02.01.SPA.conf
```

Step 5 Reload

a) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

b) **show version**

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

Note When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

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_LITE_IOSXE), Version
 17.2.1, RELEASE SOFTWARE (fc2)
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 17.2.1	Cisco IOS XE Amsterdam 17.1.x or earlier releases.

The sample output in this section shows downgrade from Cisco IOS XE Amsterdam 17.2.1 to Cisco IOS XE Amsterdam 17.1.1, using **install** commands.

Important 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.

Procedure

Step 1 Clean Up

a) **install remove inactive**

Use this command to clean up unused installation files in case of insufficient space. Ensure that you have at least 1GB of space in flash to expand a new image.

```
Switch# install remove inactive
install_remove: START Mon Mar 23 17:46:18 IST 2020
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k_lite-rpbase.17.02.01.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-rpboot.17.02.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-srdriver.17.02.1.SPA.pkg
      File is in use, will not delete.
    cat9k_lite-webui.17.02.1.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_lite_iosxe.17.02.1.SPA.bin

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k_lite_iosxe.17.02.1.SPA.bin ... 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  Mon Mar 23 17:47:20 IST 2020
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

Use this command to copy the new image to flash: (Or skip this step if you want to use the new image from your TFTP server).

```
Switch# copy tftp://10.8.0.6//cat9k_lite_iosxe.17.01.1.SPA.bin flash:

Destination filename [cat9k_lite_iosxe.17.01.1.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_lite_iosxe.17.01.1.SPA.bin...
Loading /cat9k_lite_iosxe.17.01.1.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. (Or skip this step if you want to use the new image from your TFTP server).

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

Directory of flash:/

434184 -rw- 508584771 Mon Mar 23 2019 13:35:16 -07:00 cat9k_lite_iosxe.17.01.1.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

a) **install add file activate commit**

The following example displays the installation of the Cisco IOS XE Amsterdam 17.1.1 software image to flash, by using the **install add file activate commit** command. You can point to the source image on your tftp server or in flash if you have it copied to flash.

```
Device# install add file
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/iosxe_lite_imp_img/cat9k_lite_iosxe.17.01.01.SPA.bin
 activate commit

install_add_activate_commit: START Mon Mar 23 13:17:28 IST 2020
Mar 23 13:17:31.568: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/iosxe_lite_imp_img/cat9k_lite_iosxe.17.01.01.SPA.bin
Mar 23 13:17:31.568 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/iosxe_lite_imp_img/cat9k_lite_iosxe.17.01.01.SPA.bin
Downloading file
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/iosxe_lite_imp_img/cat9k_lite_iosxe.17.01.01.SPA.bin
```

```
*Mar 23 13:17:31.530 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install one-shot
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/iosxe_lite_imp_img/cat9k_lite_iosxe.17.01.01.SPA.bin
Finished downloading file
tftp://203.0.113.1/auto/tftp-ex-user0/exuser/iosxe_lite_imp_img/cat9k_lite_iosxe.17.01.01.SPA.bin
 to flash:cat9k_lite_iosxe.17.01.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.17.01.01.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
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: 17.01.01.0.203
install_add_activate_commit: Activating PACKAGE

gzip: initramfs.cpio.gz: decompression OK, trailing garbage ignored
Following packages shall be activated:
/flash/cat9k_lite-webui.17.01.01.SPA.pkg
/flash/cat9k_lite-srdriver.17.01.01.SPA.pkg
/flash/cat9k_lite-rpboot.17.01.01.SPA.pkg
/flash/cat9k_lite-rpbase.17.01.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
Mar 23 13:29:31.133: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds

*Mar 23 13:29:31.093 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Activate package(s)
 on switch 1
    --- Starting list of software package changes ---
    Old files list:
      Removed cat9k_lite-rpbase.17.02.01.SPA.pkg
      Removed cat9k_lite-rpboot.17.02.01.SPA.pkg
      Removed cat9k_lite-srdriver.17.02.01.SPA.pkg
      Removed cat9k_lite-webui.17.02.01.SPA.pkg
    New files list:
      Added cat9k_lite-rpbase.17.01.01.SPA.pkg
      Added cat9k_lite-rpboot.17.01.01.SPA.pkg
      Added cat9k_lite-srdriver.17.01.01.SPA.pkg
      Added cat9k_lite-webui.17.01.01.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

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

```
Send model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Mon Mar 23 13:30:52 IST 2020
Mar 23 13:30:53.573: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.01.01.SPA.bin
Mar 23 13:30:53.573 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE flash:cat9k_lite_iosxe.17.01.01.SPA.bin

switch3#
Chassis 1 reloading, reason - Reload command

*Mar 23 13:30:53.529 IST: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
 Completed install one-shot PACKAGE flash:cat9k_lite_iosxe.17.01.01.SPA.bin
*Mar 23 13:30:54.526 IST: %STACKMGR-1-RELOAD: Switch 1 R0/0: stack_mgr: Reloading due to
reason Reload commandMar 23 13:30:58.121: %PMAN-5-EXITACTION: F0/0: pvp: Process manager
is exiting: reload fp actionrequested
Mar 23 13:31:01.303: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes
 exit with reload switch code
```

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

Step 4 Reload

a) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

Note When you downgrade the software image, the boot loader does not automatically downgrade. It remains updated.

b) **show version**

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

Note When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the **show version** command displays the Cisco IOS XE Amsterdam 17.1.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 17.01.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version
 17.1.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

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 9200 Series Switches   fall under these base or add-on license levels.

Base Licenses

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

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 Essentials
- DNA Advantage— Includes features available with the DNA Essentials license and more.

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.

License Types

The following license types are available:

- 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.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a 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.

- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 1: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[5]	Yes

[5] You will be able to purchase this combination only at the time of the DNA license renewal and not when you purchase DNA-Essentials the first time.

- 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*.

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (http://software.cisco.com).

Important Cisco Smart Licensing is the default and the only available method to manage licenses.

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

Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

Step 1 Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.

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

Step 2 Create and activate your Smart Account, or login if you already have one.

To create and activate Smart Account, go to Cisco Software Central → Create Smart Accounts. Only authorized users can activate the Smart Account.

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

b) Set up the required number of Virtual Accounts, users and access rights for the virtual account users.

Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

c) Generate the registration token in the Cisco Smart Software Manager portal and register your device with the token.

In the software configuration guide of the required release, see *System Management* → *Configuring Smart Licensing* → *Registering the Device in CSSM*

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

Using Smart Licensing on an Out-of-the-Box Device

If an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

In the software configuration guide of the required release, see *System Management* → *Configuring Smart Licensing* → *Registering the Device in CSSM*

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9200 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

Limitations and Restrictions

- 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.

- Hardware limitations
  - Management Port—You cannot modify the configured port speed, duplex mode and flow control and disable auto-negotiation on the Ethernet Management port (GigabitEthernet0/0). Port speed and duplex mode can only be changed from a peer port.
  - Network Module — When the C9200-NM-4X network module is plugged into the C9200 SKUs of the Cisco Catalyst 9200 Series Switches, the downlink interface remains in down state until the network module is recognized by the switch. The time taken for the switch to recognize the network module is longer in comparison to the time taken by the switch to recognize other interconnected devices.
  - If the 1-meter and 1.5-meter 10-GBase-CX1 cables, which are connected on the 10-G ports of the Catalyst 9200L switches, are connected to the 10-G peer ports of the Catalyst 9200L or Catalyst 9200 switches, the peer device might go into the error-disabled state because of link flapping if the local device is restarted. As a workaround, run the **shut** and **no shut** commands on the error-disabled peer interfaces.
- 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.
- Stacking
  - Stacking is supported on Cisco Catalyst 9200 Series Switches. A switch stack supports up to eight stack members. However, you cannot stack C9200 SKUs with C9200L SKUs

    The supported stacking bandwidth on C9200L SKUs is up to 80Gbps; on C9200 SKUs, this is up to 160Gbps.
  - The C9200-24PB and C9200-48PB switch models can be stacked only with each other and not with other models of the Cisco Catalyst 9200 Series Switches.
  - Auto upgrade for a new member switch is supported only in the install mode.
- 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.
- 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.
- Upgrading the software image from Cisco IOS XE Gibraltar 16.12.x to any of the later releases can result in a persistent database operation failure and after which the persistent database cannot be restored.

  To avoid the persistent database operation failure, use the **dir bootflash:.dbpersist** command to list all DB persist files and then use **delete bootflash:/.dbpersist/folder_name/file_name** and **bootflash:/.dbpersist/folder_name/file_name.meta** commands to delete individual database and meta files from each persistent database folder.
- The File System Check (fsck) utility is not supported in install mode.
- The DiagMemoryTest GOLD test is not supported on the Catalyst 9200 Series Switches.

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 17.2.x

Identifier	Description
CSCvs84212	DHCP server sends out a NAK packet during DHCP renewal process.
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt13518	QoS ACL matching incorrectly when udp range is used

Resolved Caveats in Cisco IOS XE Amsterdam 17.2.1

Identifier	Description
CSCvr87505	Mac addr count discrepancy b/w active/standby fed post core flap / sso even when no VC discrepancy
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvs14893	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port
CSCvs20185	DAD iface not being shown under Device360 (StackWise Virtual)

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 9200 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9200-r-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.