Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Amsterdam 17.2.x

First Published: 2020-03-30

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Amsterdam 17.2.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 17.2.1

Hardware Features in Cisco IOS XE Amsterdam 17.2.1

Feature Name	Description and Documentation Link
C9600-LC-48S	Cisco Catalyst 9600 Series 48-port supporting 1 G on each of its 48 SFP ports. See Cisco Catalyst 9600 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-CU1M
	  • SFP-H25G-CU1.5M
	  • SFP-H25G-CU2M
	  • SFP-H25G-CU2.5M
	  • SFP-H25G-CU3M
	  • SFP-H25G-CU4M
	  • SFP-H25G-CU5M
	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.

Cisco QSFP-40G Direct-Attach Cables	Supported direct-attach copper cable product numbers: • QSFP-H40G-CU0-5M • QSFP-H40G-CU1M • QSFP-H40G-CU2M • QSFP-H40G-CU3M • QSFP-H40G-CU4M • QSFP-H40G-CU5M • QSFP-H40G-ACU7M • QSFP-H40G-ACU10M For information about these cables, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Feature Name	Description and Documentation Link
Cisco QSFP-100G Direct Attached Cables	Supported direct-attach copper cable product numbers: • QSFP-100G-CU1M • QSFP-100G-CU2M • QSFP-100G-CU3M • QSFP-100G-CU5M For information about these cables, see Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 40GBASE QSFP Modules (40G to 4x10G Breakout Modules)	Supported transceiver module product numbers: • Cisco 40GBASE-CSR4 QSFP Module: QSFP-40G-CSR4 • Cisco 4x10GBASE-LR QSFP module: QSFP-4X10G-LR-S • Cisco 40GBASE-SR4 QSFP module: QSFP-40G-SR4 • Cisco 40GBASE-SR4 QSFP module: QSFP-40G-SR4-S For information about these cables, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Feature Name	Description and Documentation Link
Cisco QSFP-40G Direct-Attach and Active Optical Breakout Cables	• Supported direct-attach copper breakout cable product numbers: • QSFP-4SFP10G-CU0-5M • QSFP-4SFP10G-CU1M • QSFP-4SFP10G-CU2M • QSFP-4SFP10G-CU3M • QSFP-4SFP10G-CU4M • QSFP-4SFP10G-CU5M • QSFP-4X10G-AC7M • QSFP-4X10G-AC10M • Supported active optical breakout cable product numbers: • QSFP-4X10G-AOC1M • QSFP-4X10G-AOC2M • QSFP-4X10G-AOC3M • QSFP-4X10G-AOC5M • QSFP-4X10G-AOC7M • QSFP-4X10G-AOC10M For information about these cables, see Cisco 40GBASE QSFP 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
Breakout Interfaces (C9600-LC-24C)	The twelve ports of the top row (odd numbers) of a C9600-LC-24C line card now support breakout configuration. See Interface and Hardware Components → Configuring Interface Characteristics. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information

Cisco StackWise Virtual	The following enhancements have been made to the feature:
	• Dual-Active Detection (DAD) links are now supported for the following interface and line card configurations:
	  • 1G interface on a C9600-LC-48TX line card.
	  • 1G interface if configured between a C9600-LC-48TX line card and either a C9600-LC-48YL line card or a C9600-LC-24C line card.
	  • 1G interface and 10G interface if configured between two C9600-LC-48YL line cards or between two C9600-LC-24C line cards.
	  • 1G interface and 10G interface if configured between a C9600-LC-48YL line card and a C9600-LC-24C line card.
	• StackWise Virtual Links (SVLs) are supprted only on 10G interfaces on a C9600-LC-48TX line card.
	See High Availability → Configuring Cisco StackWise Virtual.
	(Network Advantage)

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 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 Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • Native Docker Support • YANG Data Models	The following programmability features are introduced in this release: • Native Docker Support: Application Hosting supports Docker applications. Application Hosting is a virtualization environment that runs a guest Docker application on the host operating system. The Cisco IOS-XE virtualization services provide manageability and networking models for running a guest application. (DNA 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.
Quad-Supervisor with Route Processor Redundancy (RPR)	Provides intra-chassis redundancy in a setup where Cisco StackWise Virtual is configured between two chassis. The feature requires the installation of at least one redundant supervisor in one of the chassis (in addition to the Cisco StackWise Virtual active and standby). The added redundancy reduces the time taken to reach a ready state with full bandwidth in the event of a failure or a forced switchover. Ensure that your setup complies with the following guidelines to implement Quad-Supervisor with RPR: • All supervisor modules in the setup are running at least the minimum required software version, which is Cisco IOS XE Amsterdam 17.2.1. • All supervisor modules in the setup are running the same software version. See High Availability → Quad-Supervisor with Route Processor Redundancy. (Network Advantage)
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 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 Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Hierarchical VPLS with MPLS access	Reduces signaling overhead and packet replication between devices when compared to configuring VPLS. See Multiprotocol Label Switching (MPLS) → Configuring Hierarchical VPLS with MPLS Access. (Network Advantage)
VPLS: Routed Pseudowire IRB for IPv4 Unicast	Enables a switch interface to route traffic instead of using a router. See Multiprotocol Label Switching (MPLS) → Configuring VPLS: Routed Pseudowire IRB for IPv4 Unicast. (Network Advantage)
VPN ID in NetFlow	Supports Virtual Private Network Identifier (VPN-ID) configuration in Flexible NetFlow. A VPN-ID is global and unique. It is used to identify a VPN across autonomous systems (ASes). See Network Management → Configuring Flexible NetFlow. (Network Advantage)
VRF Aware NAT	VRF awareness enables NAT to carry out address translation by taking the VRF of the private networks into consideration. This feature allows private networks to be placed in different VRFs. See IP Addressing Services → Configuring Network Address Translation. (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 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 9600 Switches)	
factory-reset	The command has been modified. The **switch** keyword is introduced for devices that support the Cisco StackWise Virtual solution. You can perform factory reset on the active and standby switch.
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.

Serviceability	
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, on page 8
- Complete List of Supported Features, on page 8
- Accessing Hidden Commands, on page 8
- Default Behaviour, on page 9

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://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 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

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

Product ID (append with "=" for spares)	Description
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

To view the software compatibility information between Cisco Catalyst 9600 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure, go to Cisco Catalyst 9000 Series Switches Software Version Compatibility Matrix.

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 17.2.1	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 17.2.1	CAT9K_IOSXE	cat9k_iosxe.17.02.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.02.01.

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 12.

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 switch.

In case of a High Availability set up, upgrade the active and standby switch.

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.

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.

There is no FPGA upgrade in Cisco IOS XE Amsterdam 17.2.1. 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.

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

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 17.1.x or an earlier release	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 Fri Mar 13 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to 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 Mar 13 19:52:25 UTC 2019
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_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 - 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 13 2019 10:18:11 -07:00 cat9k_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.

```
Switch# install add file flash:cat9k_iosxe.17.02.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Mar 13 16:37:25 IST 2019

*Mar 13 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: 17.1.1
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

*Mar 13 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


*Mar 13 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 Mar 13 16:46:18 IST 2019
```

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 ten new `.pkg` files and two `.conf` files.

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104    Nov 20 2019 09:52:41 -07:00 cat9k-cc_srdriver.17.01.01.SPA.pkg
475141 -rw- 70333380   Nov 20 2019 09:52:44 -07:00 cat9k-espbase.17.01.01.SPA.pkg
475142 -rw- 13256      Nov 20 2019 09:52:44 -07:00 cat9k-guestshell.17.01.01.SPA.pkg
475143 -rw- 349635524  Nov 20 2019 09:52:54 -07:00 cat9k-rpbase.17.01.01.SPA.pkg
475149 -rw- 24248187   Nov 20 2019 09:53:02 -07:00 cat9k-rpboot.17.01.01.SPA.pkg
475144 -rw- 25285572   Nov 20 2019 09:52:55 -07:00 cat9k-sipbase.17.01.01.SPA.pkg
475145 -rw- 20947908   Nov 20 2019 09:52:55 -07:00 cat9k-sipspa.17.01.01.SPA.pkg
475146 -rw- 2962372    Nov 20 2019 09:52:56 -07:00 cat9k-srdriver.17.01.01.SPA.pkg
475147 -rw- 13284288   Nov 20 2019 09:52:56 -07:00 cat9k-webui.17.01.01.SPA.pkg
475148 -rw- 13248      Nov 20 2019 09:52:56 -07:00 cat9k-wlc.17.01.01.SPA.pkg

491524 -rw- 25711568   Mar 13 2019 11:49:33 -07:00  cat9k-cc_srdriver.17.02.01.SPA.pkg
491525 -rw- 78484428   Mar 13 2019 11:49:35 -07:00  cat9k-espbase.17.02.01.SPA.pkg
491526 -rw- 1598412    Mar 13 2019 11:49:35 -07:00  cat9k-guestshell.17.02.01.SPA.pkg
491527 -rw- 404153288  Mar 13 2019 11:49:47 -07:00  cat9k-rpbase.17.02.01.SPA.pkg
491533 -rw- 31657374   Mar 13 2019 11:50:09 -07:00  cat9k-rpboot.17.02.01.SPA.pkg
491528 -rw- 27681740   Mar 13 2019 11:49:48 -07:00  cat9k-sipbase.17.02.01.SPA.pkg
491529 -rw- 52224968   Mar 13 2019 11:49:49 -07:00  cat9k-sipspa.17.02.01.SPA.pkg
491530 -rw- 31130572   Mar 13 2019 11:49:50 -07:00  cat9k-srdriver.17.02.01.SPA.pkg
491531 -rw- 14783432   Mar 13 2019 11:49:51 -07:00  cat9k-webui.17.02.01.SPA.pkg
491532 -rw- 9160       Mar 13 2019 11:49:51 -07:00  cat9k-wlc.17.02.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

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_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 13 2019 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Mar 13 2019 05:34:06 +00:00  cat9k_iosxe.17.02.01.SPA.conf
```

Step 5 **upgrade rom-monitor capsule golden switch**

Use this command to upgrade the ROMMON version. After you enter the command, confirm upgrade at the system prompt.

For more information about this, see Upgrading the ROMMON, on page 13, in this document.

```
Switch# upgrade rom-monitor capsule golden switch active 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>
```

Step 6 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

c) **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_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>
```

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 an earlier release.

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 Fri Mar 13 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.17.02.01.SPA.pkg
/flash/cat9k-espbase.17.02.01.SPA.pkg
/flash/cat9k-guestshell.17.02.01.SPA.pkg
/flash/cat9k-rpbase.17.02.01.SPA.pkg
/flash/cat9k-rpboot.17.02.01.SPA.pkg
/flash/cat9k-sipbase.17.02.01.SPA.pkg
/flash/cat9k-sipspa.17.02.01.SPA.pkg
/flash/cat9k-srdriver.17.02.01.SPA.pkg
/flash/cat9k-webui.17.02.01.SPA.pkg
/flash/cat9k-wlc.17.02.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.02.01.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-guestshell.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.02.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.02.01.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 Mar 13 19:52:25 UTC 2019
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_iosxe.17.01.01.SPA.bin flash:

Destination filename [cat9k_iosxe.17.01.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.01.01.SPA.bin...
Loading /cat9k_iosxe.17.01.01.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 Mar 13 2019 20:52:25 -07:00 cat9k_iosxe.17.01.01.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.

```
Switch# install add file flash:cat9k_iosxe.17.01.01.SPA.bin activate commit
_install_add_activate_commit: START Fri Mar 13 21:37:25 IST 2019

*Mar 13 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.01.01.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.17.01.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.01.01.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: 16.12.1
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.01.01.SPA.pkg
/flash/cat9k-webui.17.01.01.SPA.pkg
/flash/cat9k-srdriver.17.01.01.SPA.pkg
/flash/cat9k-sipspa.17.01.01.SPA.pkg
/flash/cat9k-sipbase.17.01.01.SPA.pkg
/flash/cat9k-rpboot.17.01.01.SPA.pkg
/flash/cat9k-rpbase.17.01.01.SPA.pkg
/flash/cat9k-guestshell.17.01.01.SPA.pkg
/flash/cat9k-espbase.17.01.01.SPA.pkg
/flash/cat9k-cc_srdriver.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 Active/Standby

*Mar 13 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


*Mar 13 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 Mar 13 21:46:18 IST 2019
```

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) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **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.

c) **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 [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
17.01.1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
<output truncated>
```

Licensing

For information about licenses required for the features available on Cisco Catalyst 9000 Series Switches, see Configuring Licenses on Cisco Catalyst 9000 Series Switches.

All licensing information relating to Cisco Catalyst 9000 Series Switches are available on this collection page: Cisco Catalyst 9000 Switching Family Licensing.

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.
- 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.

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.

- 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.
- The File System Check (fsck) utility is not supported in install mode.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

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
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
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
CSCwq83338	On the C9600 Dual-Sup, performing a redundancy force-switchover immediately after reaching STANDBY HOT causes the process to halt at "in progress to standby cold-config"

Resolved Caveats in Cisco IOS XE Amsterdam 17.2.1

Identifier	Description
CSCvr09103	SVL : OSPFv3 and BFD flapping when the standby is coming up
CSCvr20139	Packet loss and FSC/RCV Error seen when pumping with mgig IXIA card (1518-9216bytes)
CSCvr28169	Fed crashes when show cli for btrace counters is executed
CSCvr87505	Mac addr count discrepancy b/w active/standby fed post core flap / sso even when no VC discrepancy
CSCvr88090	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr98368	CAT9K intermittently not responding to SNMP
CSCvs14893	802.1x-MultiAuth/MultiDomain: C9K - Traffic drop in egress direction for Data-Vlan on a Auth port

Identifier	Description
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 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: https://cfnng.cisco.com/mibs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results 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 DevNet.
- 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)

© 2020 Cisco Systems, Inc. All rights reserved.