Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2022-09-22

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Gibraltar 16.12.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 Gibraltar 16.12.8

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.7

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.6

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.5b

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.5

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.4

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.3a

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.3

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.2

Hardware Features in Cisco IOS XE Gibraltar 16.12.2

Feature Name	Description and Documentation Link
Cisco SFP Modules for Gigabit Ethernet	

Feature Name	Description and Documentation Link
	Supported Cisco SFP Modules for Gigabit Ethernet on C9600-LC-48YL line card are: • GLC-T (1G) • GLC-TE (1G) • GLC-LH-SM • GLC-LH-SMD • GLC-SX-MM • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SM • GLC-ZX-SMD • GLC-BX-D • GLC-BX-U • GLC-SX-MM-RGD • GLC-LX-SM-RGD • GLC-ZX-SM-RGD • CWDM-SFP-xxxx • DWDM-SFP-xxxx • GLC-BX40-U-I • GLC-BX40-DA-I • GLC-BX80-D-I • GLC-BX80-U-I Supported Cisco SFP Modules for Gigabit Ethernet on C9600-LC-24C line card using Cisco QSFP 40-Gigabit Ethernet to SFP+ 10G Adapter Module (CVR-QSFP-SFP10G) are: • GLC-T (1G) • GLC-TE (1G) • GLC-LH-SMD • GLC-SX-MMD For information about a module, see the Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Whats New in Cisco IOS XE Gibraltar 16.12.1

Hardware Features in Cisco IOS XE Gibraltar 16.12.1

Feature Name	Description and Documentation Link

Cisco 10GBASE SFP+ modules and Cisco SFP+ active optical cables	• Supported transceiver module product numbers:
	  • SFP-10G-SR-X
	  • SFP-10G-LR-X
	• Supported cable product numbers:
	  • SFP-H10GB-CU1-5M
	  • SFP-H10GB-CU2-5M
	  • SFP-H10GB-CU2M
	For information about the module, see Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Cisco 25GBASE SFP28 Modules	Supported transceiver module product number—Cisco SFP-10/25G-LR-S For information about the module, see the Cisco 25GBASE SFP28 Modules Data Sheet and Cisco 25G Transceivers and Cables Enable 25 Gigabit Ethernet over a Fiber or Copper Cable. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 40GBASE QSFP Modules	Supported transceiver module product number—QSFP-4X10G-LR-S **Note** Only the 40G mode is supported; the 4X10G breakout out mode is not supported. For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 100GBASE QSFP-100G Modules	Supported cable product numbers: • QSFP-40/100-SRBD 40G and 100G modes are supported. • QSFP-100G-ER4L-S For information about the module, see Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Gibraltar 16.12.1

Feature Name	Description, Documentation Link, and License Level Information
Autoconf Device Granularity to PID of Cisco Switch	Introduces the **platform type** filter option for class map and parameter map configurations. Use the **map platform-type** command in parameter map filter configuration mode, to set the parameter map attribute and the **match platform-type** command in control class-map filter configuration mode, to evaluate control classes. See Network Management → Configuring Autoconf. (Network Essentials and Network Advantage)
Border Gateway Protocol (BGP) Ethernet VPN (EVPN) Route Target (RT) Autonomous System Number (ASN) Rewrite	Introduces support for the **rewrite-evpn-rt-asn** command in address-family configuration mode. This command enables the rewrite of the ASN portion of the EVPN route target that originates from the current autonomous system, with the ASN of the target eBGP EVPN peer. See IP Routing Commands → rewrite-evpn-rt-asn. (Network Advantage)
Bidirectional Protocol Independent Multicast (PIM)	Introduces support for bidirectional PIM. This feature is an extension of the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-sparse mode, bidirectional PIM avoids keeping source-specific state in a router and allows trees to scale to an arbitrary number of sources. See IP Multicast Routing → Configuring Protocol Independent Multicast (PIM). (Network Advantage)
Cisco StackWise Virtual	Introduces support for a network system virtualization technology that pairs two switches into one virtual switch, to simplify operational efficiency with a single control and management plane. See High Availability → Configuring Cisco StackWise Virtual. (Network Advantage)
Cisco StackWise Virtual—Cisco QSFP to SFP or SFP+ Adapter (QSA module)	Introduces support for QSA module with Cisco StackWise Virtual. • Cisco QSA module with 10G SFP modules can be used as data ports and to configure StackWise Virtual links (SVLs) or Dual-Active Detection (DAD) links. • Cisco QSA module with 1G SFP modules can be used as data ports and to configure DAD links; they cannot be used to configure SVLs since SVLs are not supported on 1G interfaces. See High Availability → Configuring Cisco StackWise Virtual. (Network Advantage)
Ethernet over MPLS (EoMPLS) Xconnect on Subinterfaces	Transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN through a single virtual circuit over an Multiprotocol Label Switching (MPLS) network. See Multiprotocol Label Switching → Configuring Ethernet-over-MPLS and Pseudowire Redundancy. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
High Availability support for MACsec Key Agreement (MKA)	Support for high availability for MKA sessions is introduced. MKA sessions are now SSO-aware. In the event of failure of the active switch, the standby switch takes over the existing MKA sessions in a minimally disruptive switchover. See Security → MACsec Encryption. (Network Advantage)
IPv4 and IPv6: Object Groups for access control lists (ACLs)	Enables you to classify users, devices, or protocols into groups and apply them to ACLs, to create access control policies for these groups. With this feature, you use object groups instead of individual IP addresses, protocols, and ports, which are used in conventional ACLs. It allows multiple access control entries (ACEs), and you can use each ACE to allow or deny an entire group of users the access to a group of servers or services. See Security → Object Groups for ACLs. (Network Advantage)
IPv6: Neighbor Discovery	IPv6 support is introduced for the following Neighbor Discovery features: • IPv6: Global IPv6 entries for unsolicited NA • IPv6: HA support (Network Advantage and Network Essentials)
MPLS Layer 2 VPN over GRE	Provides a mechanism for tunneling Layer 2 MPLS packets over a non-MPLS network. See Multiprotocol Label Switching → Configuring MPLS Layer 2 VPN over GRE. (Network Advantage)
MPLS Subinterface Support	MPLS is now supported on Layer 3 subinterfaces. See VLAN → Configuring Layer 3 Subinterfaces. (Network Advantage)
MPLS Layer 3 VPN over Generic Routing Encapsulation (GRE)	Provides a mechanism for tunneling Layer 3 MPLS packets over a non-MPLS network. See Multiprotocol Label Switching → Configuring MPLS Layer 3 VPN over GRE. (Network Advantage)
Network Address Translation (NAT) license level change	The NAT feature is now available with the Network Advantage license. See IP Addressing Services → Configuring Network Address Translation. (Network Advantage)
Port Channel with Subinterface	Subinterfaces can now be created on Layer 3 port channels. See VLAN → Configuring Layer 3 Subinterfaces. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • Zero-Touch Provisioning (ZTP) • IoX Support of Docker • Model-Driven Telemetry gNMI Dial-In • NETCONF-YANG SSH Server Support • YANG Data Models	The following programmability features are introduced in this release: • ZTP—Open Zero Touch Provisioning (ZTP) interface to allow devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network. This feature is supported on C9200 SKUs and not on c9200L SKUs. • Model-Driven Telemetry gNMI Dial-In—Support for telemetry subscriptions and updates over a gRPC Network Management Interface (gNMI). • NETCONF-YANG SSH Server Support—NETCONF-YANG supporting the use of IOS Secure Shell (SSH) public keys (RSA) to authenticate users as an alternative to password-based authentication. • 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/16121. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121/BIC. 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. See Programmability. (Network Essentials and Network Advantage)
Seamless MPLS	Integrates multiple networks into a single MPLS domain. It removes the need for service-specific configurations in network transport nodes. See Multiprotocol Label Switching → Configuring Seamless MPLS. (Network Advantage)
Simplified Factory Reset for Removable Storage	Performing a factory reset now also erases the contents of removable storage devices such as Serial Advanced Technology Attachment (SATA), Solid State Drive (SSD), and USB. See System Management → Performing Factory Reset. (Network Advantage)
Source Group Tag (SGT), Destination Group Tag (DGT) over FNF for IPv6 traffic	Introduces support for SGT and DGT fields over FNF, for IPv6 traffic. See Network Management → Configuring Flexible NetFlow. (Network Advantage)
VPN Routing and Forwarding-aware Policy Based Routing (VRF-aware PBR)	The PBR feature is now VRF-aware and can be configured on VRF lite interfaces. You can enable policy based routing of packets for a VRF instance. See IP Routing → Configuring VRF aware PBR. (Network Advantage)

New on the Web UI	
• 802.1X Port-Based Authentication • Audio Video Bridging	Use the WebUI for: • 802.1X Port-Based Authentication—Supports IEEE 802.1X authentication configuration at the interface level. This type of access control and authentication protocol restricts unauthorized clients from connecting to a LAN through publicly accessible ports • Audio Video Bridging—Supports configuration and monitoring of Ethernet based audio/video deployments using the IEEE 802.1BA standard. This enables low latency and high dedicated bandwidth for time-sensitive audio and video streams for a professional grade experience.

Important Notes

- Unsupported Features
- Complete List of Supported Features
- Accessing Hidden Commands
- Default Behaviour, on page 10

Unsupported Features

- Breakout Cables
- Cisco Application Visibility and Control (AVC)
- IPsec VPN
- Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- Programmability (Cisco Plug-in for OpenFlow 1.3, Third-Party Application Hosting)

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 in place, when they are accessed. Hidden commands are meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface → Understanding the Help System* chapter of the Command Reference document.

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. Entering enter a question mark (?) at the system prompt displays 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 the 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
AC Power Supply Modules	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]
DC Power Supply Modules	
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module

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

Optics Modules

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

Compatibility Matrix

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

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.8	2.6	-	-
Gibraltar 16.12.7	2.6	-	-
Gibraltar 16.12.6	2.6	-	-
Gibraltar 16.12.5b	2.6	-	-
Gibraltar 16.12.5	2.6	-	-
Gibraltar 16.12.4	2.6	-	-
Gibraltar 16.12.3a	2.6	-	-
Gibraltar 16.12.3	2.6	-	-
Gibraltar 16.12.2	2.6	-	-
Gibraltar 16.12.1	2.6	-	-
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	-

Web UI System Requirements

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

Minimum Hardware Requirements

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

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

Software Requirements

Operating Systems

- Windows 10 or later
- Mac OS X 10.9.5 or later

Browsers

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

ROMMON Versions

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

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

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

The following table provides ROMMON version information for the Cisco Catalyst 9600 Series Supervisor Modules. For ROMMON version information of Cisco IOS XE 17.x.x releases, refer to the corresponding Cisco IOS XE 17.x.x release notes of the respective platform.

Release	ROMMON Version (C9600-SUP-1)
Gibraltar 16.12.8	17.1.1[FC2]
Gibraltar 16.12.7	17.1.1[FC2]
Gibraltar 16.12.6	17.1.1[FC2]
Gibraltar 16.12.5b	17.1.1[FC2]
Gibraltar 16.12.5	17.1.1[FC2]
Gibraltar 16.12.4	17.1.1[FC2]
Gibraltar 16.12.3a	17.1.1[FC2]
Gibraltar 16.12.3	17.1.1[FC2]
Gibraltar 16.12.2	17.1.1[FC2]

Release	ROMMON Version (C9600-SUP-1)
Gibraltar 16.12.1	16.12.1r[FC2]
Gibraltar 16.11.1	16.11.1r[FC2]

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 Gibraltar 16.12.8	CAT9K_IOSXE	cat9k_iosxe.16.12.08.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.08.SPA
Cisco IOS XE Gibraltar 16.12.7	CAT9K_IOSXE	cat9k_iosxe.16.12.07.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.07.SPA
Cisco IOS XE Gibraltar 16.12.6	CAT9K_IOSXE	cat9k_iosxe.16.12.06.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.06.SPA
Cisco IOS XE Gibraltar 16.12.5b	CAT9K_IOSXE	cat9k_iosxe.16.12.05b.SPA.bi
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05b.SP

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.12.5	CAT9K_IOSXE	cat9k_iosxe.16.12.05.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05.
Cisco IOS XE Gibraltar 16.12.4	CAT9K_IOSXE	cat9k_iosxe.16.12.04.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.04.
Cisco IOS XE Gibraltar 16.12.3a	CAT9K_IOSXE	cat9k_iosxe.16.12.03a.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03a
Cisco IOS XE Gibraltar 16.12.3	CAT9K_IOSXE	cat9k_iosxe.16.12.03.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03.
Cisco IOS XE Gibraltar 16.12.2	CAT9K_IOSXE	cat9k_iosxe.16.12.02.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.02.
Cisco IOS XE Gibraltar 16.12.1	CAT9K_IOSXE	cat9k_iosxe.16.12.01.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.01.

Automatic Boot Loader Upgrade



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

- Do not power cycle your 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.

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.

The FPGA upgrade process is part of the software image upgrade. The FPGA version does not downgrade when you downgrade the software image.

After completing the upgrade procedure, you can verify the FPGA version against the value in the table below. Enter the **show firmware version all** command in IOS mode or **version -v** command in ROMMON mode.

Platform	FPGA Version in Cisco IOS XE Gibraltar 16.12.1
Cisco Catalyst 9600 Series Switches	• I/O FPGA on Supervisor Modules - 0x19041620 • Flash FPGA on Supervisor Modules - 0x190308B9 • FPGA on Line Cards - 0x19070619 **Note** FPGA version is upgraded only if the setup is reloaded. In case of upgrade with ISSU, the line card should be power-cycled for their FPGA to 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 with In Service Software Upgrade (ISSU)

Follow these instructions to perform ISSU upgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Gibraltar 16.12.x, in install mode. The sample output in this section displays upgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Gibraltar 16.12.2 using install commands.

Before you begin

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

When upgrading from ...	To...
Cisco IOS XE Gibraltar 16.12.1	Cisco IOS XE Gibraltar 16.12.x

Note Downgrade with ISSU is not supported. To downgrade, follow the instructions in the Downgrading in Install Mode, on page 22 section.

For more information about ISSU release support and recommended releases, see Technical References → In-Service Software Upgrade (ISSU).

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Switch# enable
```

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

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

```
Switch# install add file tftp:cat9k_iosxe.16.12.02.SPA.bin activate issu commit
```

Step 3 **show version**

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

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.02
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.12.2,
 RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

Step 4 **exit**

Exits privileged EXEC mode and returns to user EXEC mode.

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 Gibraltar 16.11.x	Cisco IOS XE Gibraltar 16.12.x

The sample output in this section displays upgrade from Cisco IOS XE Gibraltar 16.11.1 to Cisco IOS XE Gibraltar 16.12.1 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 Wed Jul 24 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.16.11.01.SPA.pkg
/flash/cat9k-espbase.16.11.01.SPA.pkg
/flash/cat9k-guestshell.16.11.01.SPA.pkg
/flash/cat9k-rpbase.16.11.01.SPA.pkg
/flash/cat9k-rpboot.16.11.01.SPA.pkg
/flash/cat9k-sipbase.16.11.01.SPA.pkg
/flash/cat9k-sipspa.16.11.01.SPA.pkg
/flash/cat9k-srdriver.16.11.01.SPA.pkg
/flash/cat9k-webui.16.11.01.SPA.pkg
/flash/cat9k-wlc.16.11.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.11.01.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 Wed Jul 24 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.16.12.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin...
Loading /cat9k_iosxe.16.12.01.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 Jul 24 2019 10:18:11 -07:00 cat9k_iosxe.16.12.01.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.16.12.01.SPA.bin activate commit
_install_add_activate_commit: START Wed Jul 24 16:37:25 IST 2019

*Jul 24 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.16.12.01.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.16.12.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.16.12.01.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.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby

*Jul 24 16:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [R0] Activate
package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate


*Jul 24 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  Wed Jul 24 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 four new `.pkg` files and two `.conf` files.

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104    Mar 29 2019 09:52:41 -07:00 cat9k-cc_srdriver.16.11.01.SPA.pkg
475141 -rw- 70333380   Mar 29 2019 09:52:44 -07:00 cat9k-espbase.16.11.01.SPA.pkg
475142 -rw- 13256      Mar 29 2019 09:52:44 -07:00 cat9k-guestshell.16.11.01.SPA.pkg
475143 -rw- 349635524  Mar 29 2019 09:52:54 -07:00 cat9k-rpbase.16.11.01.SPA.pkg
475149 -rw- 24248187   Mar 29 2019 09:53:02 -07:00 cat9k-rpboot.16.11.01.SPA.pkg
475144 -rw- 25285572   Mar 29 2019 09:52:55 -07:00 cat9k-sipbase.16.11.01.SPA.pkg
475145 -rw- 20947908   Mar 29 2019 09:52:55 -07:00 cat9k-sipspa.16.11.01.SPA.pkg
475146 -rw- 2962372    Mar 29 2019 09:52:56 -07:00 cat9k-srdriver.16.11.01.SPA.pkg
475147 -rw- 13284288   Mar 29 2019 09:52:56 -07:00 cat9k-webui.16.11.01.SPA.pkg
475148 -rw- 13248      Mar 29 2019 09:52:56 -07:00 cat9k-wlc.16.11.01.SPA.pkg

491524 -rw- 25711568   Jul 24 2019 11:49:33 -07:00  cat9k-cc_srdriver.16.12.01.SPA.pkg
491525 -rw- 78484428   Jul 24 2019 11:49:35 -07:00  cat9k-espbase.16.12.01.SPA.pkg
491526 -rw- 1598412    Jul 24 2019 11:49:35 -07:00  cat9k-guestshell.16.12.01.SPA.pkg
491527 -rw- 404153288  Jul 24 2019 11:49:47 -07:00  cat9k-rpbase.16.12.01.SPA.pkg
491533 -rw- 31657374   Jul 24 2019 11:50:09 -07:00  cat9k-rpboot.16.12.01.SPA.pkg
491528 -rw- 27681740   Jul 24 2019 11:49:48 -07:00  cat9k-sipbase.16.12.01.SPA.pkg
491529 -rw- 52224968   Jul 24 2019 11:49:49 -07:00  cat9k-sipspa.16.12.01.SPA.pkg
491530 -rw- 31130572   Jul 24 2019 11:49:50 -07:00  cat9k-srdriver.16.12.01.SPA.pkg
491531 -rw- 14783432   Jul 24 2019 11:49:51 -07:00  cat9k-webui.16.12.01.SPA.pkg
491532 -rw- 9160       Jul 24 2019 11:49:51 -07:00  cat9k-wlc.16.12.01.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.16.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

16631  -rw-             4882  Jul 24 2019 05:39:42 +00:00  packages.conf
16634  -rw-            4882  Jul 24 2019 05:34:06 +00:00  cat9k_iosxe.16.12.01.SPA.conf
```

Step 5 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
```

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 Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1, RELEASE SOFTWARE (fc2)
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 via " 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 Gibraltar 16.12.x	Cisco IOS XE Gibraltar 16.11.x or an earlier release.

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Gibraltar 16.11.1, 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 Jul 22 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.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.12.01.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 Mon Jul 22 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.16.11.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.11.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.11.01.SPA.bin...
Loading /cat9k_iosxe.16.11.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

b) **dir flash:**

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

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

Directory of flash:/

434184 -rw- 508584771 Jul 22 2019 20:52:25 -07:00 cat9k_iosxe.16.11.01.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 Gibraltar 16.11.1 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.16.11.01.SPA.bin activate commit
_install_add_activate_commit: START Mon Jul 22 21:37:25 IST 2019

*Jul 24 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.16.11.01.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.16.11.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.16.11.01.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: 16.11.1
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.11.01.SPA.pkg
/flash/cat9k-webui.16.11.01.SPA.pkg
/flash/cat9k-srdriver.16.11.01.SPA.pkg
/flash/cat9k-sipspa.16.11.01.SPA.pkg
/flash/cat9k-sipbase.16.11.01.SPA.pkg
/flash/cat9k-rpboot.16.11.01.SPA.pkg
/flash/cat9k-rpbase.16.11.01.SPA.pkg
/flash/cat9k-guestshell.16.11.01.SPA.pkg
/flash/cat9k-espbase.16.11.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.11.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby

*Jul 22 21:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
```

```
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate


*Jul 22 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  Mon Jul 22 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 Gibraltar 16.11.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.11.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.11.1,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
```

```
Compiled Mon 22-Jul-19 22:38 by mcpre
<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 9600 Series Switches fall under these base or add-on license levels.

Base Licenses

- Network Advantage

Add-On Licenses

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

- DNA Advantage

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

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

- 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: Cisco License Central 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 License Central. For a more detailed overview on Cisco Licensing, visit the Licensing Hub.



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

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 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.
- Hardware Limitations — Optics:
  - Copper cables are not supported with 25GE, 40GE, and 100GE configurations
  - Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter —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 adapter — 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 Limitations — 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.
- Convergence: During SSO, a higher convergence time is observed while removing the active supervisor module installed in slot 3 of a C9606R chassis.
- 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%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - 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 Gibraltar 16.12.x

Identifier	Description
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 Gibraltar 16.12.8

Identifier	Description
CSCwa68343	Cisco IOS XE Software for Catalyst Switches MPLS Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.7

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

Identifier	Description
CSCvv27849	Cat 9K & 3K: Unexpected reload caused by the FED process.
CSCvx94722	Radius protocol generate jumbo frames for dot1x packets
CSCvy25845	SNMP: ifHCInOctets - snmpwalk on sub-interface octet counter does not increase

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5b

Identifier	Description
CSCvr73771	Session not getting authenticated via MAB after shut/no shut of interface
CSCvv27849	Cat 9K & 3K fed crash when running 16.12.5
CSCvw64798	Cisco IOx for IOS XE Software Command Injection Vulnerability
CSCvx23125	SVL Link Instability May Result in IOMD Exhaustion

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5

Identifier	Description
CSCvu62273	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading
CSCvv16874	Catalyst Switch: SISF Crash due to a memory leak
CSCvw63161	ZTP failing with error in creating downloaded_script.py

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.4

Identifier	Description
CSCvp77133	systemd service flash-recovery.service always in the running mode
CSCvq17488	show module info for active switch is n/a after booting remaining switches
CSCvr41932	17.1.1 - Memory leak @ SAMsgThread.
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs71084	Cat9k - Not able to apply Et-analytics on an interface
CSCvs73383	"show mac address-table" does not show remote EIDs when vlan filter used
CSCvs74413	Modifying the child service policy causes the standby chassis/switch to reboot due to sync failure.

Identifier	Description
CSCvs75010	Traffic forwarding stops when Session Idle time out is configured 10 sec with active traffic running
CSCvs77781	Critical auth failing to apply DEFAULT_CRITICAL_DATA_TEMPLATE
CSCvs89792	INJECT_FEATURE_ESCAPE: Egress IP packet delivered via legacy inject path for NetBios packets
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs91593	offer is dropped in data vlan with dhcp snooping using dot1x/mab
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt01187	Eigrp neighbor down up occurred frequently
CSCvt13067	Nvram Failed to initializae (startup missing)
CSCvt30243	connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt35095	Connection for L3 interfaces and SVIs may go down when power cycled SVL active switch comes online.
CSCvt60712	Switch crashed after removing route-map
CSCvt64058	Loopback error is not detected on trunk interface
CSCvt72401	MACSEC protected link no longer passes traffic.
CSCvt72427	Cat3k/9k Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan
CSCvt82323	Interface storm-control configuration causes policing of same-type traffic elsewhere on the device.
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvu15007	Crash when invalid input interrupts a role-based access-list policy installation

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3a

Identifier	Description
CSCvt17460	SVL/DAD links will be err-disabled when there is link-flap due to faulty SFPs
CSCvt41134	Unexpected reload (or boot loop) caused by Smart Agent (SASRcvWQWrk2)
CSCvt72427	Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3

Identifier	Description
CSCvm55401	DHCP snooping may drop dhcp option82 packets w/ ip dhcp snooping information option allow-untrusted
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvq75887	intermediate hop with SVI in PIM domain is not forwarding multicast traffic
CSCvr23358	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr46622	Cat9k || scaled mVPN || tracebacks and errors seen in FED trace
CSCvr59959	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr88090	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction
CSCvr90442	Unknown status shown in "show platform software status control-processor"
CSCvr90477	Cat3k/Cat9k incorrectly set more-fragment flag for double fragmentation
CSCvr91162	Layer 2 flooding floods IGMP queries causing network outage
CSCvr92638	OSPF External Type-1 Route Present in OSPF Database but not in RIB
CSCvr98281	After valid ip conflict, SVI admin down responds to GARP
CSCvr98368	CAT9K intermittently not responding to SNMP
CSCvs01943	"login authentication VTY_authen" is missing on "line vty 0 4" only
CSCvs03124	In stackwise, PSU status of standby switch is not shown correctly
CSCvs14374	Standby crashes on multiple port flaps
CSCvs14920	Block overrun crash due to Corrupted redzone
CSCvs20038	qos softmax setting doesn't take effect on Catalyst switch in Openflow mode
CSCvs25412	CTS Environmental Data download request triggered before PAC provisioned
CSCvs25428	Netconf incorrectly activate IPv4 address-family for IPv6 BGP peer.
CSCvs36803	When port security applied mac address not learned on hardware
CSCvs39968	C9606R on Stackwise Virtual crashes on transceiver insertion
CSCvs42476	Crash during authentication failure of client

Identifier	Description
CSCvs45231	Memory exhaustion in sessmgrd process due to EAPoL announcement
CSCvs50391	FED crash when premature free of SG element
CSCvs50868	Fed memory leak in 16.9.X related to netflow
CSCvs61571	Cat3k/Cat9k- OBJ_DWNLD_TO_DP_FAILED after exceeding hardware capacity for adjacency table
CSCvs62003	In COPP policy, ARP traffic should be classified under the "system-cpp-police-forus" class
CSCvs68255	Traceback seen when IS-IS crosses LSP boundary and tries to add information in new LSP
CSCvs73580	Memory leak in fed main event qos
CSCvt00402	cat3k Switch with 1.6GB flash size unable to do SWIM upgrade between 16.12.x images

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.2

Identifier	Description
CSCvp97892	Incorrect speed config & status after SSO for interface with SFP-10/25G-LR-S/CSR-S.
CSCvq54265	Ip bootp server should be disabled by default as a device hardening best practice.
CSCvr02957	Re-add app-hosting move support was removed.
CSCvp93578	SG-SVL : MKA Session got stuck when we change key-chain value on the fly with delay-protection
CSCvr70470	sessmgrd crash with "clear dot1x mac" command

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1

Identifier	Description
CSCvm89086	cat 9300 | span destination interface not dropping ingress traffic
CSCvn04524	IP Source Guard blocks traffic after host IP renewal
CSCvn31653	Missing/incorrect FED entries for IGMP Snooping on Cat9300/Cat3850/Cat3650
CSCvn77683	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvn83940	Cat9k TFTP copy failed with Port Security enabled
CSCvo15594	Hardware MAC address programming issue for remote client catalyst 9300

Identifier	Description
CSCvo17778	Cat9k not updating checksum after DSCP change
CSCvo24073	multiple CTS sessions stuck in HELD/SAP_NE
CSCvo32446	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo33983	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo47513	Active supervisor crashed during insertion/removal of a line card
CSCvo56629	Cat9500 - Interface in Admin shutdown showing incoming traffic and interface Status led in green.
CSCvo59504	Cat3K | Cat9K - SVI becomes inaccesible upon reboot
CSCvo71264	Cat3k / Cat9k Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo75559	Cat9300 | First packet not forwarded when (S,G) needs to be built
CSCvo83305	MAC Access List Blocks Unintended Traffic
CSCvp49518	DHCP SNOOPING DATABASE IS NOT REFRESHED AFTER RELOAD
CSCvp69629	Authentication sessions does not come up on configuring dot1x when there is active client traffic .
CSCvp72220	crash at sisf_show_counters after entering show device-tracking counters command
CSCvq27812	Sessmgr CPU is going high due to DB cursor is not disabled after switchover

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 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.

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)

© 2019–2021 Cisco Systems, Inc. All rights reserved.