Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2022-09-22

Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Gibraltar 16.12.x

Introduction

Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise switching access platform and have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence with the rest of the Cisco Catalyst 9000 Series Switches in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 and UADP 3.0. The platform runs an Open Cisco IOS XE that supports model driven programmability, has the capacity to host containers, and run 3rd party applications and scripts natively within the switch (by virtue of x86 CPU architecture, local storage, and a higher memory footprint). This series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

Cisco Catalyst 9400 Series Switches are enterprise optimized with a dual-serviceable fan tray design, side to side airflow, and are closet-friendly with a16-inch depth

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

There are no new hardware features in this release.

Software Features in Cisco IOS XE Gibraltar 16.12.2

Feature Name	Description, Documentation Link, and License Level Information
Cisco StackWise Virtual	Introduces support for configuring StackWise Virtual link (SVL) and dual-active detection (DAD) links on Cisco Catalyst 9400 Series Switch 10-Gigabit Ethernet line cards. See High Availability → Configuring Cisco StackWise Virtual. (Network Advantage)

Whats New in Cisco IOS XE Gibraltar 16.12.1c

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 55.

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
C9400-LC-48H	Cisco Catalyst 9400 Series 48-port, 10/100/1000 BASE-T Gigabit Ethernet, IEEE 802.3bt compliant module supporting up to 90 W Cisco UPOE+ on each of its 48 RJ45 ports. See Cisco Catalyst 9400 Series Switching Module Installation Note.

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)
Automatic line card (autoLC) shutdown	Starting with this release, autoLC shutdown (**power supply autolc shutdown**) is always enabled and cannot be disabled. In all earlier releases, autoLC shutdown continues to be disabled by default and must be manually enabled if you want the system hardware to shut down line cards in the event of a power constraint. See System Management → Environmental Monitoring and Power Management (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)

Feature Name	Description, Documentation Link, and License Level Information
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)
Bluetooth Dongle	Introduces support for external USB Bluetooth dongles. The connected dongle acts as a Bluetooth host and serves as a management port connection on the device. See Interface and Hardware Components → Configuring an External USB Bluetooth Dongle. (Network Essentials)
Energy Efficient Ethernet (EEE) support on Multigigabit (mGig) Ethernet ports	EEE is now supported on linecards with mGig ports. See Interface and Hardware Components → Configuring EEE. (Network Essentials and 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 (EoMPLS). (Network Advantage)
Flexlink+	Configures a pair of Layer 2 interfaces - one interface is configured to act as a backup for the other interface. See Layer 2 → Configuring Flexlink+. (Network Essentials and Network Advantage)
In Service Software Upgrade (ISSU) with CiscoStackWise Virtual	Introduces support for ISSU with Cisco StackWise Virtual configured on the C9410R switch model, in dual supervisor module configuration, with single supervisor per C9410R. See High Availability → Configuring ISSU. (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 Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: BGP	IPv6 support is introduced for the following features: • IPv6: BGP Hide Local Autonomous System • IPv6: BGP Named Community Lists • IPv6: BGP Neighbor Policy • IPv6: BGP Prefix-Based Outbound Route Filtering • IPv6: BGP Restart Neighbor Session After Max-Prefix Limit Reached • IPv6: BGP Support for Fast Peering Session Deactivation • IPv6: BGP Selective Address Tracking • IPv6: BGP IPv6 PIC Edge and Core for IP/MPLS • IPv6: Multiprotocol BGP Link-local Address Peering • IPv6: BGP Route-Map Continue • IPv6: BGP Route-Map Continue Support for Outbound Policy • IPv6: BGP Support for IP Prefix Import from Global Table into a VRF Table • IPv6: BGP Named Community Lists • IPv6: BGP Support for Sequenced Entries in Extended Community Lists • IPv6: BGP Support for TTL Security Check • IPv6: BGP Support for BFD (Network Advantage)
IPv6: Intermediate System to Intermediate System (IS-IS)	IPv6 support is introduced for the following IS-IS features: • Integrated ISIS Point to Point Adjacency over Broadcast Media • Integrated ISIS Protocol Shutdown Support Maintaining Configuration Parameters
IPv6: IP Enhanced IGRP Route Authentication	IPv6 support is introduced for IP Enhanced IGRP Route Authentication (Network Advantage and Network Essentials)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: IP Service Level Agreements (SLAs)	IPv6 support is introduced for following IP SLA features: • IPv6: IP SLAs - Multi Operation Scheduler • IPv6: IP SLAs - One Way Measurement • IPv6: IP SLAs - VoIP Threshold Traps • IPv6: IP SLAs - Additional Threshold Traps • IPv6: IP SLAs - Random Scheduler • IPv6: IP SLAs - Sub-millisecond Accuracy Improvements (Network Advantage and Network Essentials)
IPv6: MIBs for IPv6 Traffic	IPv6 support is introduced for the following MIBs: • IP Forwarding Table MIB (RFC4292) • Management Information Base for the Internet Protocol (IP) (RFC4293 (Network Advantage and Network Essentials)
IPv6: Multiprotocol Label Switching (MPLS)	IPv6 support is introduced for the following MPLS features: • IPv6: MPLS VPN VRF CLI for IPv4 and IPv6 VPNs • IPv6: EIGRP IPv6 NSF/GR • IPv6: EIGRP MPLS VPN PE-CE • IPv6: Route Target Rewrite • IPv6: eiBGP Multipath (Network Advantage)
IPv6: Multicast Routing	IPv6 support is introduced for the following multicast routing features: • IPv6: Address Family Support for Multiprotocol BGP • IPv6: Address Group Range Support • IPv6: PIMv6 Anycast RP solution (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)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: PBR Recursive Next-Hop	IPv6 support is introduced for PBR Recursive Next-Hop option. (Network Advantage and Network Essentials)
IPv6-based Posture Validation	IPv6 support is introduced for Posture Validation. (Network Advantage and Network Essentials)
IPv6: Proxy Mobile	IPv6 support is introduced for PMIPv6 Hybrid Access.
IPv6: Open Shortest Path First (OSPF)	IPv6 support is introduced for the following OSPF features: • IPv6: NSF - OSPF • IPv6: OSPF Flooding Reduction • IPv6: OSPF Link State Database Overload Protection • IPv6: OSPF On Demand Circuit (RFC 1793) • IPv6: OSPF Packet Pacing • IPv6: OSPF Support for Multi-VRF on CE Routers • IPv6: OSPFv3 NSR • IPv6: OSPFv3 Retransmission Limits • IPv6: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec • IPv6: OSPFv3 Graceful Restart • IPv6: VRF aware OSPFv3, EIGRPv6, BGPv6 • IPv6: OSPFv3 Fast Convergence - LSA and SPF throttling (Network Advantage and Network Essentials)
IPv6: Services	IPv6 support is introduced for AAAA DNS Lookups over an IPv6 Transport. (Network Advantage and Network Essentials)
IPv6: Time-Based Access Lists Using Time Ranges	IPv6 support is introduced for Time-Based Access Lists using time ranges. (Network Advantage and Network Essentials)
IPv6: Triggered RIP	IPv6 support is introduced for Triggered Extensions to RIP.
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)

Feature Name	Description, Documentation Link, and License Level Information
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)
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)
Programmability • IoX Support of Docker • Model-Driven Telemetry gNMI Dial-In • NETCONF-YANG SSH Server Support • OpenFlow Power over Ethernet • YANG Data Models	The following programmability features are introduced in this release: • 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. • OpenFlow Power over Ethernet—Power over Ethernet (PoE) support on OpenFlow ports. • 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)

Feature Name	Description, Documentation Link, and License Level Information
Stack troubleshooting optimization	The output of the **show tech-support stack** command has been enhanced to include more stack-related information. See High Availability Commands → show tech-support stack. (A license level does not apply)
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

Cisco StackWise Virtual - Supported and Unsupported Features

When you enable Cisco StackWise Virtual on the device

- Layer 2, Layer 3, Security, Quality of Service, Multicast, Application, Monitoring and Management, Multiprotocol Label Switching, High Availability, and VXLAN BGP EVPN are supported.

  Contact the Cisco Technical Support Centre for the specific list of features that are supported under each one of these technologies.

- Resilient Ethernet Protocol, Remote Switched Port Analyzer, and Sofware-Defined Access are NOT supported

Unsupported Features

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Fast PoE
- IPsec VPN
- MACsec Switch to Switch Connections on C9400-SUP-1XL-Y.
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

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

Starting with Cisco IOS XE Fuji 16.8.1a, as an improved security measure, the way in which hidden commands can be accessed has changed.

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. Such hidden commands are only 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 9400 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
C9404R	Cisco Catalyst 9400 Series 4 slot chassis • Redundant supervisor module capability • Two switching module slots • Hot-swappable, front and rear serviceable, non-redundant fan tray assembly • Four power supply module slots
C9407R	Cisco Catalyst 9400 Series 7 slot chassis • Redundant supervisor module capability • Five switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots
C9410R	Cisco Catalyst 9400 Series 10 slot chassis • Redundant supervisor module capability • Eight switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots

Supported Hardware on Cisco Catalyst 9400 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9400-SUP-1	Cisco Catalyst 9400 Series Supervisor 1 Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.
C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor 1XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.
C9400-SUP-1XL-Y	Cisco Catalyst 9400 Series Supervisor 25XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.
Line Cards	
C9400-LC-24S	24-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP
C9400-LC-24XS	24-port Gigabit Ethernet module that supports 1 and 10 Gbps connectivity.
C9400-LC-48H	48-port Gigabit Ethernet UPOE+ module supporting up to 90W on each of its 48 RJ45 ports.
C9400-LC-48P	48 Port, 1 Gigabit Ethernet POE/POE+ module supporting up to 30W per port.
C9400-LC-48S	48 Port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP.
C9400-LC-48T	48-port, 10/100/1000 BASE-T Gigabit Ethernet module.
C9400-LC-48U	48-Port UPOE 10/100/1000 (RJ-45) module supporting up to 60W per port.
C9400-LC-48UX	48-port, UPOE Multigigabit Ethernet Module with: • 24 ports (Ports 1 to 24) 1G UPOE 10/100/1000 (RJ-45) • 24 ports (Ports 25 to 48) MultiGigabit Ethernet 100/1000/2500/5000/10000 UPOE ports
M.2 SATA SSD Modules[1] **(for the Supervisor)**	
C9400-SSD-240GB	Cisco Catalyst 9400 Series 240GB M2 SATA memory
C9400-SSD-480GB	Cisco Catalyst 9400 Series 480GB M2 SATA memory

Product ID (append with "=" for spares)	Description
C9400-SSD-960GB	Cisco Catalyst 9400 Series 960GB M2 SATA memory
AC Power Supply Modules	
C9400-PWR-2100AC	Cisco Catalyst 9400 Series 2100W AC Power Supply
C9400-PWR-3200AC	Cisco Catalyst 9400 Series 3200W AC Power Supply
DC Power Supply Modules	
C9400-PWR-3200DC	Cisco Catalyst 9400 Series 3200W DC Power Supply

[1] M.2 Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) Module

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 9400 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.8	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.7	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.6	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.5b	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.4	2.6	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.2	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4 → **Downloads**.
Gibraltar 16.10.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.8	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**

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[2]	512 MB[3]	256	1280 x 800 or higher	Small

[2] We recommend 1 GHz
[3] 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 and CPLD Versions

The following table provides ROMMON and CPLD version information for the Cisco Catalyst 9400 Series Supervisor Modules. For ROMMON and CPLD 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 (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	CPLD Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)
Gibraltar 16.12.7	16.12.2r	19032905
Gibraltar 16.12.6	16.12.2r	19032905
Gibraltar 16.12.5	16.12.2r	19032905
Gibraltar 16.12.4	16.12.2r	19032905
Gibraltar 16.12.3	16.12.2r	19032905
Gibraltar 16.12.2	16.12.1r	19032905
Gibraltar 16.12.1c	16.12.1r	19032905
Gibraltar 16.11.1	16.10.2r	17101705
Gibraltar 16.10.1	16.6.2r	17101705
Fuji 16.9.x	16.6.2r[FC1]	17101705
Fuji 16.8.1a	16.6.2r	17101705
Everest 16.6.x	16.6.2r[FC1]	17101705

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.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05b.SP
Cisco IOS XE Gibraltar 16.12.5	CAT9K_IOSXE	cat9k_iosxe.16.12.05.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05.SPA
Cisco IOS XE Gibraltar 16.12.4	CAT9K_IOSXE	cat9k_iosxe.16.12.04.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.04.SPA
Cisco IOS XE Gibraltar 16.12.3a	CAT9K_IOSXE	cat9k_iosxe.16.12.03a.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03a.SP
Cisco IOS XE Gibraltar 16.12.3	CAT9K_IOSXE	cat9k_iosxe.16.12.03.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03.SPA
Cisco IOS XE Gibraltar 16.12.2	CAT9K_IOSXE	cat9k_iosxe.16.12.02.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.02.SPA
Cisco IOS XE Gibraltar 16.12.1c	CAT9K_IOSXE	cat9k_iosxe.16.12.01c.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.01c.SP

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.

Note Disconnecting and reconnecting power to a Cisco Catalyst 9400 Series Supervisor 1 Module within a 5-second window, can corrupt the boot SPI.

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) with Cisco StackWise Virtual

Follow these instructions to perform In Service Software Upgrade (ISSU) to Cisco IOS XE Gibraltar 16.12.1 with Cisco StackWise Virtual, in install mode.

Before you begin

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

When upgrading from ...	To...
Cisco IOS XE Fuji 16.9.3 or Cisco IOS XE Fuji 16.9.4	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 36 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.16.12.01.SPA.bin activate issu commit
```

The following sample output displays installation of Cisco IOS XE Gibraltar 16.12.1 software image with ISSU procedure.

```
Switch# install add file tftp:cat9k_iosxe.16.12.01.SPA.bin activate issu commit
install_add_activate_commit: START Thu Jul 21 06:16:32 UTC 2019
Downloading file tftp://172.27.18.5//cat9k_iosxe.16.12.01.SPA.bin

*Jul 21 06:16:34.064: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
 install one-shot ISSU tftp://172.27.18.5//cat9k_iosxe.16.12.01.SPA.binFinished downloading
 file tftp://172.27.18.5//cat9k_iosxe.16.12.01.SPA.bin to flash:cat9k_iosxe.16.12.01.SPA.bin
install_add_activate_commit: Adding ISSU

--- Starting initial file syncing ---
[1]: Copying flash:cat9k_iosxe.16.12.01.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

```
install_add_activate_commit: Activating ISSU

NOTE: Going to start Oneshot ISSU install process

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


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


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

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

*Jul 21 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jul 21 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jul 21 06:24:16.466: %HMANRP-5-CHASSIS_DOWN_EVENT: Chassis 2 gone DOWN!
*Jul 21 06:24:16.497: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Jul 21 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Jul 21 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Jul 21 06:24:16.674: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Jul 21 06:24:16.679: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected switch 2 is no longer
 standby
*Jul 21 06:24:16.416: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1 R0/0: nif_mgr: Port 1 on front
side stack link 0 is DOWN.
*Jul 21 06:24:16.416: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 1 R0/0: nif_mgr: Port 1 on
 front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Jul 21 06:24:16.416: %NIF_MGR-6-STACK_LINK_DOWN: Switch 1 R0/0: nif_mgr: Front side stack
 link 0 is DOWN.
*Jul 21 06:24:16.416: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port
1 on Switch 1 is down

<output truncated>

*Jul 21 06:29:36.393: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Jul 21 06:29:36.392: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has
been elected STANDBY.
*Jul 21 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))
*Jul 21 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Jul 21 06:29:42.257: %REDUNDANCY-3-IPC: IOS versions do not match.
*Jul 21 06:30:24.323: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeededFinished
wait for Standby to reach terminal redundancy state


*Jul 21 06:30:25.325: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
```

```
STAGE 3: Installing software on Active
================================================
--- Starting install_active ---
Performing install_active on Chassis 1

<output truncated>

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


STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_add_activate_commit  Thu Jul 21 23:06:45 UTC 2019
Jul 21 23:06:45.731: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot ISSU flash:cat9k_iosxe.16.12.01.SPA.bin
Jul 21 23:06:47.509: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 21 23:06:48.776: %PM

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Fri 08/17/2018 10:48:42.68 by rel

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

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


Jul 21 23:08:30.238: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:

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



Switch console is now available


Press RETURN to get started.




Jul 21 23:14:17.080: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit
Jul 21 23:15:48.445: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit ISSU
```

Step 3 **show version**

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

The following sample output of the **show version** command displays the Cisco IOS XE 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 (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

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

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

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

No ISSU operation is in progress

Switch#
```

Step 5 **exit**

Exits privileged EXEC mode and returns to user EXEC mode.

Upgrading with In Service Software Upgrade (ISSU) in Dual Supervisor Module Configuration

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

Before you begin

ISSU from Cisco IOS XE Gibraltar 16.12.1c to any release requires installation of Software Maintenance Upgrade (SMU) packages. ISSU from Cisco IOS XE Gibraltar 16.12.2 and later does not require installation of SMU packages.

Install the following SMU packages before performing ISSU.

Scenario	File Name (Hot Patch)
Cisco IOS XE Fuji 16.9.1 to any ISSU supported release	cat9k_iosxe.16.09.01.CSCvs66914.SPA.smu.bin
Cisco IOS XE Fuji 16.9.2 to any ISSU supported release	cat9k_iosxe.16.09.02.CSCvs66914.SPA.smu.bin
Cisco IOS XE Fuji 16.9.3 to any ISSU supported release	cat9k_iosxe.16.09.03.CSCvs66914.SPA.smu.bin
Cisco IOS XE Fuji 16.9.4 to any ISSU supported release	cat9k_iosxe.16.09.04.CSCvs66914.SPA.smu.bin
Cisco IOS XE Gibraltar 16.12.1c to any ISSU supported release	cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin

Note Downgrade with ISSU is not supported. To downgrade, follow the instructions in the Downgrading in Install Mode, on page 36 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 show redundancy

Use this command to display redundancy facility information.

```
Switch# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 7 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
               Maintenance Mode = Disabled
                 Communications = Up

Current Processor Information :
-------------------------------
                Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 7 minutes
                 Image Version = Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software
 (CAT9K_IOSXE), Version 16.12.1c, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Sun 25-Aug-19 10:19 by mcpre
                           BOOT = bootflash:packages.conf;
                    CONFIG_FILE =
        Configuration register = 0x102

Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 5 minutes
                 Image Version = Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software
 (CAT9K_IOSXE), Version 16.12.1c, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Sun 25-Aug-19 10:19 by mcpre
                           BOOT = bootflash:packages.conf;
```

```
                    CONFIG_FILE =
          Configuration register = 0x102
```

Step 3 **show issu state** [*detail*]

Use this command to verify that no other ISSU process is in progress.

```
Switch# show issu state detail
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

Current ISSU Status: Enabled
Previous ISSU Operation: Successful
========================================================
System Check                          Status
--------------------------------------------------------
Platform ISSU Support                 Yes
Standby Online                        Yes
Autoboot Enabled                      Yes
SSO Mode                              Yes
Install Boot                          Yes
Valid Boot Media                      Yes
========================================================
No ISSU operation is in progress
```

Step 4 **install add file activate commit**

Use the commands below to install the SMU packages.

install add file tftp:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin activate commit

The following sample output displays installation of the CSCvs66914 SMU package.

```
Switch# install add file tftp:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin activate commit
install_add: START Wed Feb 19 20:11:34 UTC 2020
Downloading file tftp:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin
Finished downloading file tftp:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin to
bootflash:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Copying image file: bootflash:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin to standby
Info: Finished copying bootflash:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin to standby
Finished initial file syncing


*Feb 19 20:11:35.545: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 add tftp:/cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin--- Starting SMU Add operation ---
Performing SMU_ADD on Active/Standby
  [R0] SMU_ADD package(s) on R0
  [R0] Finished SMU_ADD on R0
  [R1] SMU_ADD package(s) on R1
  [R1] Finished SMU_ADD on R1
Checking status of SMU_ADD on [R0 R1]
SMU_ADD: Passed on [R0 R1]
Finished SMU Add operation

SUCCESS: install_add  Wed Feb 19 20:11:49 UTC 2020

Switch#
```

```
*Feb 19 20:11:50.094: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU bootflash:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin
```

Step 5 **show install summary**

Use this command to verify if the SMU packages are installed properly.

The following sample output displays that the CSCvs66914 SMU package has been installed on the switch.

```
Switch# show install summary
[ R0 R1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   I    bootflash:cat9k_iosxe.16.12.01c.CSCvs66914.SPA.smu.bin
IMG   C    16.12.1c.0.8

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Step 6 **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.

The following sample output displays the installation of the Cisco IOS XE Gibraltar 16.12.2 software image with ISSU procedure.

```
Switch# install add file tftp:cat9k_iosxe.16.12.02.SPA.bin  activate issu commit
install_add_activate_commit: START Wed Feb 19 20:14:29 UTC 2020
Downloading file tftp:/cat9k_iosxe.16.12.02.SPA.bin

*Feb 19 20:14:30.451: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 one-shot ISSU tftp:cat9k_iosxe.16.12.02.SPA.bin
*Feb 19 20:18:16.509: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded
 [free space is 1918380 kB] - Please clean up files on bootflash.Finished downloading file
 tftp:cat9k_iosxe.16.12.02.SPA.bin to bootflash:cat9k_iosxe.16.12.02.SPA.bin
install_add_activate_commit: Adding ISSU
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Copying image file: bootflash:cat9k_iosxe.16.12.02.SPA.bin to standby
Info: Finished copying bootflash:cat9k_iosxe.16.12.02.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

install_add_activate_commit: Activating ISSU

NOTE: Going to start Oneshot ISSU install process

STAGE 0: System Level Sanity Check
================================================
--- Verifying install_issu supported ---
```

```
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
--- Verifying Platform specific ISSU admission criteria ---
Finished Initial System Level Sanity Check


STAGE 1: Installing software on Standby
================================================
--- Starting install_remote ---
Performing install_remote on remote RP/Bay
--- Starting install local lock acquisition on R1 ---
Finished install local lock acquisition on R1

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found cat9k-cc_srdriver.16.12.02.SPA.pkg
  Found cat9k-espbase.16.12.02.SPA.pkg
  Found cat9k-guestshell.16.12.02.SPA.pkg
  Found cat9k-rpbase.16.12.02.SPA.pkg
  Found cat9k-rpboot.16.12.02.SPA.pkg
  Found cat9k-sipbase.16.12.02.SPA.pkg
  Found cat9k-sipspa.16.12.02.SPA.pkg
  Found cat9k-srdriver.16.12.02.SPA.pkg
  Found cat9k-webui.16.12.02.SPA.pkg
  Found cat9k-wlc.16.12.02.SPA.pkg

<outputt truncated>

--- Starting list of software package changes ---
Old files list:
  Removed cat9k-cc_srdriver.16.12.01c.SPA.pkg
  Removed cat9k-espbase.16.12.01c.SPA.pkg
  Removed cat9k-guestshell.16.12.01c.SPA.pkg
  Removed cat9k-rpbase.16.12.01c.SPA.pkg
  Removed cat9k-rpboot.16.12.01c.SPA.pkg
  Removed cat9k-sipbase.16.12.01c.SPA.pkg
  Removed cat9k-sipspa.16.12.01c.SPA.pkg
  Removed cat9k-srdriver.16.12.01c.SPA.pkg
  Removed cat9k-webui.16.12.01c.SPA.pkg
  Removed cat9k-wlc.16.12.01c.SPA.pkg
New files list:
  Added cat9k-cc_srdriver.16.12.02.SPA.pkg
  Added cat9k-espbase.16.12.02.SPA.pkg
  Added cat9k-guestshell.16.12.02.SPA.pkg
  Added cat9k-rpbase.16.12.02.SPA.pkg
  Added cat9k-rpboot.16.12.02.SPA.pkg
  Added cat9k-sipbase.16.12.02.SPA.pkg
  Added cat9k-sipspa.16.12.02.SPA.pkg
  Added cat9k-srdriver.16.12.02.SPA.pkg
  Added cat9k-webui.16.12.02.SPA.pkg
  Added cat9k-wlc.16.12.02.SPA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
```

```
Committing provisioning file
Finished commit of software changes

SUCCESS: Software provisioned.  New software will load on reboot.
  [R1] install_remote package(s) on R1
  WARNING: Found 51 disjoint TDL objects.
  [R1] Finished install_remote on R1
install_remote: Passed on [R1]
Finished install_remote


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

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

*Feb 19 20:23:16.492: %IOSXE_OIR-6-OFFLINECARD: Card (rp) offline in slot R1
*Feb 19 20:23:16.504: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Feb 19 20:23:16.563: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Feb 19 20:23:16.563: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Feb 19 20:23:16.563: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Feb 19 20:23:17.503: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Feb 19 20:23:17.512: %IOSXE_REDUNDANCY-6-PEER: Active detected switch -1 as standby.
*Feb 19 20:23:17.503: %CMRP-3-RP_RESET: R1/0: cmand: RP is resetting : remote RP requested
 reset of this RP
*Feb 19 20:23:19.508: %CMRP-6-RP_SB_RELOAD_REQ: R0/0: cmand: Reloading Standby RP: initiated
 by RF reload message
*Feb 19 20:26:21.756: %IOSXE-3-PLATFORM: R1/0: kernel: dplr_intrpt: Entered
dplr_intrpt_module_init dplr_intrpt 1
*Feb 19 20:27:59.469: %IOSXE_OIR-6-ONLINECARD: Card (rp) online in slot R1
*Feb 19 20:28:07.064: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))

*Feb 19 20:28:07.065: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Feb 19 20:28:09.895: %REDUNDANCY-3-IPC: IOS versions do not match.

*Feb 19 20:28:09.952: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Feb 19 20:29:22.973: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Feb 19 20:29:24.049: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)Finished
wait for Standby to reach terminal redundancy state


STAGE 3: Installing software on Active
================================================
--- Starting install_active ---
Performing install_active on active RP/Bay
--- Starting install local lock acquisition on R0 ---
Finished install local lock acquisition on R0

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found cat9k-cc_srdriver.16.12.02.SPA.pkg
```

```
  Found cat9k-espbase.16.12.02.SPA.pkg
  Found cat9k-guestshell.16.12.02.SPA.pkg
  Found cat9k-rpbase.16.12.02.SPA.pkg
  Found cat9k-rpboot.16.12.02.SPA.pkg
  Found cat9k-sipbase.16.12.02.SPA.pkg
  Found cat9k-sipspa.16.12.02.SPA.pkg
  Found cat9k-srdriver.16.12.02.SPA.pkg
  Found cat9k-webui.16.12.02.SPA.pkg
  Found cat9k-wlc.16.12.02.SPA.pkg
Verifying image file locations

<output truncated>

--- Starting list of software package changes ---
Old files list:
  Removed cat9k-cc_srdriver.16.12.01c.SPA.pkg
  Removed cat9k-espbase.16.12.01c.SPA.pkg
  Removed cat9k-guestshell.16.12.01c.SPA.pkg
  Removed cat9k-rpbase.16.12.01c.SPA.pkg
  Removed cat9k-rpboot.16.12.01c.SPA.pkg
  Removed cat9k-sipbase.16.12.01c.SPA.pkg
  Removed cat9k-sipspa.16.12.01c.SPA.pkg
  Removed cat9k-srdriver.16.12.01c.SPA.pkg
  Removed cat9k-webui.16.12.01c.SPA.pkg
  Removed cat9k-wlc.16.12.01c.SPA.pkg
New files list:
  Added cat9k-cc_srdriver.16.12.02.SPA.pkg
  Added cat9k-espbase.16.12.02.SPA.pkg
  Added cat9k-guestshell.16.12.02.SPA.pkg
  Added cat9k-rpbase.16.12.02.SPA.pkg
  Added cat9k-rpboot.16.12.02.SPA.pkg
  Added cat9k-sipbase.16.12.02.SPA.pkg
  Added cat9k-sipspa.16.12.02.SPA.pkg
  Added cat9k-srdriver.16.12.02.SPA.pkg
  Added cat9k-webui.16.12.02.SPA.pkg
  Added cat9k-wlc.16.12.02.SPA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

SUCCESS: Software provisioned.  New software will load on reboot.
  [R0] install_active package(s) on R0
  [R0] Finished install_active on R0
install_active: Passed on [R0]
Finished install_active


STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
 New software will load after reboot process is completed
SUCCESS: install_add_activate_commit  Wed Feb 19 20:30:19 UTC 2020

<output truncated>

*Feb 19 20:33:28.428: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Feb 19 20:33:31.462: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Feb 19 20:34:42.327: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
```

```
*Feb 19 20:34:43.454: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Feb 19 20:35:33.623: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 commit%IOSXEBOOT-4-ISSU_ONE_SHOT: (rp/1): ISSU finished successfully

*Feb 19 20:35:35.021: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit ISSU
Switch>en
```

Step 7 **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:

```
Cisco IOS XE Software, Version 16.12.02
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.12.02,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 19-Nov-19 10:04 by mcpre
```

Step 8 **show issu state** [*detail*]

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

The following is a sample output of **show issu state detail** after installation of the software image with ISSU.

```
Switch# show issu state detail
--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting installation state synchronization ---
Finished installation state synchronization

Current ISSU Status: Enabled
Previous ISSU Operation: Successful
=====================================================
System Check                       Status
-----------------------------------------------------
Platform ISSU Support              Yes
Standby Online                     Yes
Autoboot Enabled                   Yes
SSO Mode                           Yes
Install Boot                       Yes
Valid Boot Media                   Yes
=====================================================
No ISSU operation is in progress
```

Step 9 **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 via **boot flash:packages.conf**.

Before you begin

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

When upgrading from ...	Permitted Supervisor Setup (Applies to the release you are upgrading from)	First upgrade to...	To upgrade to ...
Cisco IOS XE Everest 16.6.1[4]	Upgrade a single supervisor, and complete the boot loader and CPLD upgrade. After completing the first supervisor upgrade, remove and swap in the second supervisor. After both supervisors are upgraded, they can be inserted and booted in a high availability setup. **Note** Do not simultaneously upgrade dual supervisors from Cisco IOS XE Everest 16.6.1 to a later release. Doing so may cause hardware damage.	Cisco IOS XE Everest 16.6.3 Follow the upgrade steps as in the Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Everest 16.6.x → Upgrading the Switch Software → Upgrading in Install Mode	Cisco IOS XE Gibraltar 16.12.1c
Cisco IOS XE Everest 16.6.2 and later releases	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously upgraded.	Not applicable	

[4] When upgrading from Cisco IOS XE Everest 16.6.1 to a later release, the upgrade may take a long time, and the system will reset three times due to rommon and complex programmable logic device (CPLD) upgrade. Stateful switchover is supported from Cisco IOS XE Everest 16.6.2

Caution

- Do not power cycle your switch during an upgrade.
- Do not disconnect power or remove the supervisor module during an upgrade.
- 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 OIR of a switching module (linecard) when the switch is booting up.

The sample output in this section displays upgrade from Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1c using **install** commands.

Procedure

Step 1 Clean Up

a) **install remove inactive**

Use this command to clean up old 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 14:14:40 PDT 2019
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.06.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[R0]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.16.06.03.SPA.pkg
/flash/cat9k-rpbase.16.06.03.SPA.pkg
/flash/cat9k-rpboot.16.06.03.SPA.pkg
/flash/cat9k-sipbase.16.06.03.SPA.pkg
/flash/cat9k-sipspa.16.06.03.SPA.pkg
/flash/cat9k-srdriver.16.06.03.SPA.pkg
/flash/cat9k-webui.16.06.03.SPA.pkg
/flash/cat9k_1.bin
/flash/cat9k_1.conf
/flash/cat9k_2.1.conf
/flash/cat9k_2.bin
/flash/cat9k_2.conf
/flash/cat9k_iosxe.16.06.03.SPA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Deleting file
Deleting file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k_1.bin ... done.
Deleting file flash:cat9k_1.conf ... done.
Deleting file flash:cat9k_2.1.conf ... done.
Deleting file flash:cat9k_2.bin ... done.
Deleting file flash:cat9k_2.conf ... done.
Deleting file flash:cat9k_iosxe.16.06.03.SPA.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Mon Jul 22 14:16:29 PDT 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// 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 22 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 to flash. 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 Mon Jul 22 22:49:41 UTC 2019

*Jul 22 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 22 22:49:42 install_engine.sh:

 %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.12.01.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE

/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 requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

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

```
Commit: Passed on [1]
Finished Commit

Install will reload the system now!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
/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
Mon Jul 22 22:53:58 UTC 2019
Switch#
```

Note Old files listed in the logs will not be removed from flash.

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:

Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.06.03.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.06.03.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.06.03.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.06.03.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.06.03.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.06.03.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.06.03.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.06.03.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.06.03.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.06.03.SPA.pkg

491524 -rw- 25711568  Jul 22 2019 11:49:33 -07:00  cat9k-cc_srdriver.16.12.01.SPA.pkg
491525 -rw- 78484428  Jul 22 2019 11:49:35 -07:00  cat9k-espbase.16.12.01.SPA.pkg
491526 -rw- 1598412   Jul 22 2019 11:49:35 -07:00  cat9k-guestshell.16.12.01.SPA.pkg
491527 -rw- 404153288 Jul 22 2019 11:49:47 -07:00  cat9k-rpbase.16.12.01.SPA.pkg
491533 -rw- 31657374  Jul 22 2019 11:50:09 -07:00  cat9k-rpboot.16.12.01.SPA.pkg
491528 -rw- 27681740  Jul 22 2019 11:49:48 -07:00  cat9k-sipbase.16.12.01.SPA.pkg
491529 -rw- 52224968  Jul 22 2019 11:49:49 -07:00  cat9k-sipspa.16.12.01.SPA.pkg
491530 -rw- 31130572  Jul 22 2019 11:49:50 -07:00  cat9k-srdriver.16.12.01.SPA.pkg
491531 -rw- 14783432  Jul 22 2019 11:49:51 -07:00  cat9k-webui.16.12.01.SPA.pkg
491532 -rw- 9160      Jul 22 2019 11:49:51 -07:00  cat9k-wlc.16.12.01.SPA.pkg

11353194496 bytes total (9544245248 bytes free)
Switch#
```

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 copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf
```

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

434197 -rw- 7406 Jul 22 2018 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 22 2018 10:58:08 -07:00 cat9k_iosxe.16.12.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

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 16.12.1c 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
16.12.1c, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 30-Jul-19 10:48 by mcpre
```

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 ...	Permitted Supervisor Setup (Applies to the release you are downgrading from)	To ...
Cisco IOS XE Gibraltar 16.12.1c	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously downgraded. **Note** Do not perform an Online Removal and Replacement (OIR) of either supervisor module during the process.	Cisco IOS XE Gibraltar 16.11.x or earlier releases.

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.12.1c to Cisco IOS XE Everest 16.6.2, using **install** commands.

Important New hardware modules (supervisors or line card modules) 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 old 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 14:14:40 PDT 2019
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.12.01.SPA.pkg
```

```
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[R0]:
/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.pkg
/flash/cat9k_1.bin
/flash/cat9k_1.conf
/flash/cat9k_2.1.conf
/flash/cat9k_2.bin
/flash/cat9k_2.conf
/flash/cat9k_iosxe.16.09.01.SSA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
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_1.bin ... done.
Deleting file flash:cat9k_1.conf ... done.
Deleting file flash:cat9k_2.1.conf ... done.
Deleting file flash:cat9k_2.bin ... done.
Deleting file flash:cat9k_2.conf ... done.
Deleting file flash:cat9k_iosxe.16.10.01.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Mon Jul 22 14:16:29 PDT 2018
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.16.06.02.SPA.bin flash:
```

```
Destination filename [cat9k_iosxe.16.06.02.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.02.SPA.bin...
Loading /cat9k_iosxe.16.06.02.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 Mon Jul 22 2018 13:35:16 -07:00 cat9k_iosxe.16.06.02.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

- **install add file activate commit**
- **install rollback to committed**

The following example displays the installation of the `cat9k_iosxe.16.06.02.SPA.bin` software image to flash, to downgrade the switch 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:
Switch# install add file flash:cat9k_iosxe.16.06.02.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 22 22:49:41 UTC 2019

*Jul 22 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 22 22:49:42 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.02.SPA.bininstall_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.02.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE

/flash/cat9k-webui.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.02.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
```

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

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

Install will reload the system now!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
/flash/cat9k-webui.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-guestshell.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.02.SPA.pkg
Fri Jul 22 22:53:58 UTC 2019
Switch#
```

The following example displays sample output when downgrading the switch by using the **install rollback to committed** command.

Important You use the **install rollback to committed** command for downgrading, only if the version you want to downgrade to, is committed.

```
Switch# install rollback to committed

install_rollback: START Mon Jul 22 14:24:56 UTC 2019

This operation requires a reload of the system. Do you want to proceed? [y/n]
*Jul 22 14:24:57.555: %IOSXE-5-PLATFORM: R0/0: Jul 22 14:24:57 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install rollbacky
--- Starting Rollback ---
Performing Rollback on Active/Standby

WARNING: Found 55 disjoint TDL objects.
[R0] Rollback package(s) on R0
--- Starting rollback impact ---

Changes that are part of this rollback
Current : rp 0 0 rp_boot cat9k-rpboot.16.12.01.SPA.pkg
Current : rp 1 0 rp_boot cat9k-rpboot.16.12.01.SPA.pkg
Replacement: rp 0 0 rp_boot cat9k-rpboot.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_boot cat9k-rpboot.16.06.02.SPA.pkg
Current : cc 0  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 0  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 0  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 1  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 1  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 1  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 10 0 cc cat9k-sipbase.16.12.01.SPA.pkg
```

```
Current : cc 10 0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 10 0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 2  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 2  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 2  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 3  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 3  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 3  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 4  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 4  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 4  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 5  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 5  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 5  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 6  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 6  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 6  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 7  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 7  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 7  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 8  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 8  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 8  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : cc 9  0 cc_srdriver cat9k-cc_srdriver.16.12.01.SPA.pkg
Current : cc 9  0 cc cat9k-sipbase.16.12.01.SPA.pkg
Current : cc 9  0 cc_spa cat9k-sipspa.16.12.01.SPA.pkg
Current : fp 0  0 fp cat9k-espbase.16.12.01.SPA.pkg
Current : fp 1  0 fp cat9k-espbase.16.12.01.SPA.pkg
Current : rp 0  0 guestshell cat9k-guestshell.16.12.01.SPA.pkg
Current : rp 0  0 rp_base cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 0  0 rp_daemons cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 0  0 rp_iosd cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 0  0 rp_security cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 0  0 rp_webui cat9k-webui.16.12.01.SPA.pkg
Current : rp 0  0 rp_wlc cat9k-wlc.16.12.01.SPA.pkg
Current : rp 0  0 srdriver cat9k-srdriver.16.12.01.SPA.pkg
Current : rp 1  0 guestshell cat9k-guestshell.16.12.01.SPA.pkg
Current : rp 1  0 rp_base cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 1  0 rp_daemons cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 1  0 rp_iosd cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 1  0 rp_security cat9k-rpbase.16.12.01.SPA.pkg
Current : rp 1  0 rp_webui cat9k-webui.16.12.01.SPA.pkg
Current : rp 1  0 rp_wlc cat9k-wlc.16.12.01.SPA.pkg
Current : rp 1  0 srdriver cat9k-srdriver.16.12.01.SPA.pkg
Replacement: cc 0  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 0  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 0  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 1  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 1  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 1  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 10 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 10 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 10 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 2  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 2  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 2  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 3  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 3  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 3  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 4  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 4  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 4  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 5  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 5  0 cc cat9k-sipbase.16.06.02.SPA.pkg
```

```
Replacement: cc 5  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 6  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 6  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 6  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 7  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 7  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 7  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 8  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 8  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 8  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 9  0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 9  0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 9  0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: fp 0  0 fp cat9k-espbase.16.06.02.SPA.pkg
Replacement: fp 1  0 fp cat9k-espbase.16.06.02.SPA.pkg
Replacement: rp 0  0 guestshell cat9k-guestshell.16.06.02.SPA.pkg
Replacement: rp 0  0 rp_base cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0  0 rp_daemons cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0  0 rp_iosd cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0  0 rp_security cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0  0 rp_webui cat9k-webui.16.06.02.SPA.pkg
Replacement: rp 0  0 srdriver cat9k-srdriver.16.06.02.SPA.pkg
Replacement: rp 1  0 guestshell cat9k-guestshell.16.06.02.SPA.pkg
Replacement: rp 1  0 rp_base cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1  0 rp_daemons cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1  0 rp_iosd cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1  0 rp_security cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1  0 rp_webui cat9k-webui.16.06.02.SPA.pkg
Replacement: rp 1  0 srdriver cat9k-srdriver.16.06.02.SPA.pkg

Finished rollback impact
[R0] Finished Rollback on R0
Checking status of Rollback on [R0]
Rollback: Passed on [R0]
Finished Rollback

Install will reload the system now!
SUCCESS: install_rollback Mon Jul 22 14:26:35 UTC 2019

Switch#
*Mar 06 14:26:35.880: %IOSXE-5-PLATFORM: R0/0: Mar 06 14:26:35 install_engine.sh:
%INSTALL-5-INSTALL_COMPLETED_INFO: Completed install rollback PACKAGE
*Mar 06 14:26:37.740: %IOSXE_OIR-6-REMCARD: Card (rp) removed from slot R1
*Mar 06 14:26:39.253: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in slot R1Nov 2 14:26:5

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Mon 07/22/2019 10:19:23.77 by rel

Current image running:
Primary Rommon Image

Last reset cause: SoftwareResetTrig
C9400-SUP-1 platform with 16777216 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt] 0
attempting to boot from [bootflash:packages.conf]

Located file packages.conf
#
################################################################################################################################
```

```
Warning: ignoring ROMMON var "BOOT_PARAM"
Warning: ignoring ROMMON var "USER_BOOT_PARAM"

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.2,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 22-Jul-19 05:51 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco C9410R (X86) processor (revision V00) with 868521K/6147K bytes of memory.
Processor board ID FXS2118Q1GM
312 Gigabit Ethernet interfaces
40 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
15958516K bytes of physical memory.
11161600K bytes of Bootflash at bootflash:.
1638400K bytes of Crash Files at crashinfo:.
0K bytes of WebUI ODM Files at webui:.

%INIT: waited 0 seconds for NVRAM to be available

Press RETURN to get started!
```

Step 4 Reload

a) **boot flash:**

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

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

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

b) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Everest 16.6.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Tue 10-Jul-18 06:38 by mcpre
<output truncated>
```

Upgrading the Complex Programmable Logic Device Version

CPLD version upgrade process must be completed after upgrading the software image.

Upgrading the CPLD Version: High Availability Setup

Beginning in the privileged EXEC mode, complete the following steps:

Before you begin

When performing the CPLD version upgrade as shown, the **show platform** command can be used to confirm the CPLD version after the upgrade. This command output shows the CPLD version on all modules. However, the CPLD upgrade only applies to the supervisors, not the line cards. The line cards CPLD version is a cosmetic display. After the upgrade is completed in a high availability setup, the supervisors will be upgraded, but the line cards will still show the old CPLD version. The version mismatch between the supervisors and line cards is expected until a chassis reload.

Procedure

Step 1 Upgrade the CPLD Version of the standby supervisor module

Enter the following commands on the active supervisor:

a) `Device# configure terminal`
b) `Device(config)# service internal`
c) `Device(config)# exit`
d) `Device# upgrade hw-programmable cpld filename bootflash: rp standby`

The standby supervisor module reloads automatically and the upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Wait until the standby supervisor module boots up and the SSO has formed (HOT) before you proceed to the next step; this takes approximately 17 minutes.

Step 2 Perform a switch over

a) `Device# redundancy force-switchover`

This causes the standby supervisor (on which you have completed the CPLD upgrade in Step 1) to become the active supervisor module

Step 3 Upgrade the CPLD Version of the new standby supervisor module

Repeat Step 1 and all its substeps.

Note Do not operate an HA system with mismatched FPGA versions. FPGA version should be upgraded on both the supervisors one at a time.

Upgrading the CPLD Version: Cisco StackWise Virtual Setup

Beginning in the privileged EXEC mode, complete the following steps:

Procedure

Step 1 Upgrade the CPLD version of the standby supervisor module

Enter the following commands on the active supervisor:

a) `Device# configure terminal`
b) `Device(config)# service internal`
c) `Device(config)# exit`
d) `Device# upgrade hw-programmable cpld filename bootflash: rp standby`

Step 2 Reload the standby supervisor module

a) `Device# redundancy reload peer`

The upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Wait until the standby supervisor module boots up and the SSO has formed (HOT) before you proceed to the next step; this takes approximately 17 minutes.

Step 3 Perform a switch over

a) `Device# redundancy force-switchover`

This causes the standby supervisor (on which you have completed the CPLD upgrade in step 1) to become the active supervisor module

Step 4 Upgrade the CPLD version of the new standby supervisor module

Perfom Steps 1 and 2, including all substeps, on the new standby supervisor module

Upgrading the CPLD Version: Single Supervisor Module Setup

Beginning in the privileged EXEC mode, complete the following steps:

Procedure

Upgrade the CPLD version of the active supervisor module

Enter the following commands on the active supervisor:

a) `Device# configure terminal`
b) `Device(config)# service internal`
c) `Device(config)# exit`
d) `Device# upgrade hw-programmable cpld filename bootflash: rp active`

The supervisor module reloads automatically and the upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Example: CPLD Upgrade in a High Availability Setup

The sample output here shows the CPLD upgrade process in a High Availability setup:

1. Boot Cisco IOS XE Gibraltar 16.12.1; the bootloader upgrades automatically:

```
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): boot loader upgrade successful
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): Reloading the Supervisor to enable the New
BOOTLOADER

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Mon 04/15/2019 10:19:23.77 by rel

Current ROMMON image : Primary
Last reset cause     : SoftwareResetTrig
C9400-SUP-1XL-Y platform with 16777216 Kbytes of main memory

<output truncated>
```

2. Upgrade CPLD

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service internal
Device(config)# exit
Device#
**Feb 27 12:49:27.446 PST: %SYS-5-CONFIG_I: Configured from console by console
```

```
Device# upgrade hw-programmable cpld filename bootflash: RP Standby
Firmware upgrade will require the standby supervisor to reload. Do you want to
proceed?(y/n) y

*Feb 27 22:22:22.267: %PARSER-5-HIDDEN: Warning!!! ' upgrade hw-programmable cpld filename
 bootflash:  RP standby ' is a hidden command. Use of this command is not
recommended/supported and will be removed in future.
*Feb 27 22:23:00.059: %IOSXE_OIR-6-REMCARD: Card (rp) removed from slot R1
*Feb 27 22:23:00.063: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Feb 27 22:23:00.149: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
*Feb 27 22:23:00.149: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Feb 27 22:23:00.149: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Feb 27 22:23:01.148: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Feb 27 22:23:01.158: %IOSXE_REDUNDANCY-6-PEER: Active detected switch -1 as standby.
*Feb 27 22:23:01.636: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 6/0, interfaces
disabled
*Feb 27 22:23:01.646: %SPA_OIR-6-OFFLINECARD: SPA (C9400-SUP-1) offline in subslot 6/0
*Feb 27 22:23:01.670: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in slot R1
```

The supervisor module reloads and the upgrade takes place in ROMMON mode. The following is sample output from a standby supervisor during the course of a CPLD upgrade

```
Initializing Hardware...

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Mon 04/15/2019 10:19:23.77 by rel

Current ROMMON image : Primary
Last reset cause     : PowerOn
C9400-SUP-1 platform with 16777216 Kbytes of main memory

Starting System FPGA Upgrade .....

Programming SPI Primary image is completed.

Authenticating SPI Primary image .....
IO FPGA image is authenticated successfully.

Programming Header .....
FPGA HDR file size: 12
Image page count:   1
Verifying programmed header .....
Verifying programmed header .....
Programmed header is verified successfully.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Power Cycle is needed to complete System firmware upgrade.
It takes ~7 mins to upgrade firmware after power cycle starts. Perform the FPGA upgrade
 for the standby supervisor board (using the IOS CLI from the active supervisor).
“upgrade hw-programmable cpld filename bootflash: RP Standby”
The Standby supervisor will get reloaded automatically. FPGA upgrade will take place in
 Rommon context.
During the FPGA upgrade, the Supervisor will get powered cycle, and remain inactive for
 approximate 5 minutes.
b.       Once the standby boots up completely (form

DO NOT DISRUPT AFTER POWER CYCLE UNTIL ROMMON PROMPT APPEARS.
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Power Cycling the Supervisor board now !
Initializing Hardware...

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Mon 04/15/2019 10:19:23.77 by rel

rommon >
```

Check the version in ROMMON mode:

```
rommon >version -v

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Mon 04/15/2019 10:19:23.77 by rel

Current ROMMON image : Primary
Last reset cause     : SoftwareResetTrig
C9400-SUP-1XL-Y platform with 16777216 Kbytes of main memory

Fpga Version: 0x19032905
System Integrity Status: 134ABCE 6A40 6A48
```

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 9400 Series Switches fall under these base or add-on license levels.

Base Licenses

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

Add-On Licenses

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

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

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

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Term—for a license level, and for a three, five, or seven year period.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 1: Permitted Combinations

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

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

- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload. This applies only to *Smart Licensing*. The notion of evaluation licenses does not apply to *Smart Licensing Using Policy*.

Cisco Smart Licensing

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

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

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

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

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

Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device that is running Cisco IOS XE Fuji 16.9.1 or later releases. 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

Starting from Cisco IOS XE Fuji 16.9.1, 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*

How Upgrading or Downgrading Software Affects Smart Licensing

Starting from Cisco IOS XE Fuji 16.9.1, Smart Licensing is the default and only license management solution; all licenses are managed as Smart Licenses.

Important Starting from Cisco IOS XE Fuji 16.9.1, the Right-To-Use (RTU) licensing mode is deprecated, and the associated **license right-to-use** command is no longer available on the CLI.

Note how upgrading to a release that supports Smart Licensing or moving to a release that does not support Smart Licensing affects licenses on a device:

- **When you upgrade from an earlier release to one that supports Smart Licensing**—all existing licenses remain in evaluation mode until registered in Cisco Smart Software Manager. After registration, they are made available in your Smart Account.

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

- **When you downgrade to a release where Smart Licensing is not supported**—all smart licenses on the device are converted to traditional licenses and all smart licensing information on the device is removed.

Scaling Guidelines

For information about feature scaling guidelines, see these datasheets for Cisco Catalyst 9400 Series Switches:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-sup-eng-data-sheet-cte-en.html

Limitations and Restrictions

- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Flexible NetFlow limitations

- You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
- You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.
- You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

- Hardware limitations—When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotation, the link does not come up.
- Interoperability limitations—When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.
- In-Service Software Upgrade (ISSU)
  - ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.10.x or to Cisco IOS XE Gibraltar 16.11.x is not supported. This applies to both a single and dual supervisor module setup.
  - While performing ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x, if **interface-id snmp-if-index**command is not configured with OSPFv3, packet loss can occur. Configure the **interface-id snmp-if-index** command either during the maintenance window or after isolating the device (by using maintenance mode feature) from the network before doing the 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.
- No service password recovery—With ROMMON versions R16.6.1r and R16.6.2r, the 'no service password-recovery' feature is not available.
- 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.
  - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.
- Redundancy—The supervisor module (hardware) supports redundancy. Software redundancy is supported starting with Cisco IOS XE Everest 16.6.2. However, the associated route processor redundancy (RPR) feature is not supported.

Before performing a switchover, use the **show redundancy**, **show platform**, and **show platform software iomd redundancy** commands to ensure that both the SSOs have formed and that the IOMD process is completed.

In the following sample output for the **show redundancy**, note that both the SSOs have formed.

```
Switch# show redundancy
Redundant System Information :
------------------------------
Available system uptime = 3 hours, 30 minutes
Switchovers system experienced = 2
Standby failures = 0
Last switchover reason = active unit removed

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
------------------------------
Active Location = slot 3
Current Software state = ACTIVE
Uptime in current state = 2 hours, 57 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

Peer Processor Information :
----------------------------
Standby Location = slot 4
Current Software state = STANDBY HOT
Uptime in current state = 2 hours, 47 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822
```

In the following sample output for the **show platform** command, note that both SSOs have formed and the `HA_STATE` field is `ready`.

```
Switch# show platform
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Local RF state = ACTIVE
Peer RF state = STANDBY HOT

slot  PSM STATE   SPA INTF   HA_STATE HA_ACTIVE
   1     ready   started     ready    00:01:16
   2     ready   started     ready    00:01:22
   3     ready   started     ready    00:01:27 ***active RP
   4     ready   started     ready    00:01:27
<output truncated>
```

In the following sample output for the **show platform software iomd redundancy** command, note that the `State` for all the linecards and supervisor modules is `ok`. This indicates that the IOMD processes are completed.

```
Switch# show platform software iomd redundancy
Chassis type: C9407R

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
1         C9400-LC-24XS       ok                    3d09h
2         C9400-LC-48U        ok                    3d09h
R0        C9400-SUP-1         ok, active            3d09h
R1        C9400-SUP-1         ok, standby           3d09h
P1        C9400-PWR-3200AC    ok                    3d08h
P2        C9400-PWR-3200AC    ok                    3d08h
P17       C9407-FAN           ok                    3d08h
<output truncated>
```

- With bootloader version 16.6.2r, you cannot access the M.2 SATA SSD drive at the ROMMON prompt (`rommon>` **`dir disk0`**). The system displays an error message indicating that the corresponding file system protocol is not found on the device. The only way to access the drive when on bootloader version 16.6.2r, is through the Cisco IOS prompt, after boot up.
- 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.
- Uplink Symmetry—When a redundant supervisor module is inserted, we recommend that you have symmetric uplinks, to minimize packet loss during a switchover.

  Uplinks are said to be in symmetry when the same interface on both supervisor modules have the same type of transceiver module. For example, a TenGigabitEthernet interface with no transceiver installed operates at a default 10G mode; if the matching interface of the other supervisor has a 10G transceiver, then they are in symmetry. Symmetry provides the best SWO packet loss and user experience.

  Asymmetric uplinks have at least one or more pairs of interfaces in one supervisor not matching the transceiver speed of the other supervisor.
- 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.

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
CSCvr74931	Multicast processing takes longer time in port-channel unbundle

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

Identifier	Description
CSCwa39351	C9400-LC-48S or C9400-LC-24S line card can reboot when inserting an SFP

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

Identifier	Description
CSCvv27849	Cat 9K & 3K: Unexpected reload caused by the FED process.

Identifier	Description
CSCvx94722	Radius protocol generate jumbo frames for dot1x packets
CSCvy19160	C9400 switch may reload with Last reload reason: RP-CPU
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

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
CSCvv57251	random ports remain in down, down state after randomly bouncing and changing VLAN
CSCvw02235	DAD link on C9400-LC-48T does not bring up after reload
CSCvw63161	ZTP failing with error in creating downloaded_script.py
CSCvt60188	Authentication Config Removal leads to standby reload

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.
CSCvr67651	show beacon output is missing fantray beacon status for switch 1 and shows incorrectly for switch 2
CSCvr82708	Device crash when upgrading via ISSU
CSCvr86162	Output of crepSegmentComplete is incorrect for the switches with single Edge port

Identifier	Description
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs59282	PnP over 40gig uplink doesn't work with dual SUP
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
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
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)
CSCvt23445	Cat9400 - Some 3rd-Party phones do not bring up the interface with 'no mdix auto' configured.
CSCvt27570	interface with 100FX SFP stuck in up-state
CSCvt30243	connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt39133	OID cswDistrStackPhyPortInfo triggers memory leak
CSCvt61769	ISSU upgrade: ISSU fails after stage 2, Standby SUP goes into ROMMON
CSCvt65043	PSU Operating State changes to combined when "power budget mode single-sup" is enabled
CSCvt72427	Cat3k/9k Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan
CSCvt74856	C9407R Operating Redundancy mode shown as SSO after standby SUP fullly booting up.
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvt99199	MACSEC issue in SDA deployment
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
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
CSCvp51129	9400: Macsec: replay protection window-size is shown as 0 though configured with some size
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvq24181	Crash/Unresponsiveness after TDR test is set through SNMP
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvq91675	The active and the standby Sup crashes due to ccmc crash when upgraded to 16.12.1.
CSCvr23358	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr38087	Diagnostics errors after the Line Card OIR on C9400
CSCvr59959	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr63642	To address sync done message missing after LC OIR and switchover resulting in HMS timeout
CSCvr75014	MAB Client will reauthenticate during an ISSU from 16.9.4 to 16.12.2
CSCvr79474	HW-faulty not present in OID list for cefcModuleOperStatus object MIB:CISCO-ENTITY-FRU-CONTROL-MIB
CSCvr82402	SNMP timeout when querying entSensorValueEntry
CSCvr86223	c9400 Not able to configure power redundancy mode in SVL
CSCvr88026	C9407R Power setting, default to combine after reload
CSCvr88090	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction
CSCvr90237	Mulitple issues seen if we do SSO with MKA MACsec on Sup ports.

Identifier	Description
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
CSCvs01943	"login authentication VTY_authen" is missing on "line vty 0 4" only
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.
CSCvs30569	cmand crash after removal fantray
CSCvs35355	cmcc crash following oir events
CSCvs36803	When port security applied mac address not learned on hardware
CSCvs42476	Crash during authentication failure of client
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
CSCvo36359	Enable TestUnusedPortLoopback.

Identifier	Description
CSCvp37771	Mgig - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones
CSCvp62101	~3sec Traffic Loss on Uplink Port Channel After Active SUP removal
CSCvp66193	IOSd Crash within "DHCPD Receive" process
CSCvp70112	EnvMon trap not received after Power Supply and FAN OIR
CSCvp95156	Memory leak in linux_iosd when polling mabClientIndexTest mib.
CSCvq05337	| v169_3_hemit_es_throttle ES image || EGR_INVALID_REWRITE counter increasing in mVPN setup
CSCvq22224	// evpn/vxlan // dhcp relay not working over l3vni
CSCvq29115	Failed to get Board ID shown if stack member boots up
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq30464	CAT9400: MTU config not getting applied to inactive ports becoming active
CSCvq35631	Switch crashed due to HTTP Core
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq44397	ospf down upon switchover with aggressive timers "hello-interval 1" and "dead-interval 4"
CSCvq50632	SUP uplinks and/or slot 7 or slot 8 stop passing traffic or fail POST upon SUP failover
CSCvq50846	ip verify source mac-check prevents device tracking from getting arp probe reply
CSCvq58991	Diagnostic test of TestPortTxMonitoring is failing for DAD links
CSCvq68337	switch not forward packet when active route down
CSCvq72181	Seeing 100% CPU with FED on switch SVL setup
CSCvq72713	Switch can't forwarding traffic follow the rule of EIGRP unequal cost load-balancing
CSCvq82313	Switch sif_mgr process crash.
CSCvq89352	missing system_report when crashed - revisit fix of CSCvq26295
CSCvq94294	Multicast memory leak seen when we have a scale setup
CSCvq94738	The COPP configuration back to the default After rebooting the device
CSCvr03905	Memory Leak on FED due to IPv6 Source Guard
CSCvr29921	Inserting 1Gige SFP (GLC-SX-MMD or SFP GE-T) to SUP port causes another port to link flap.

Identifier	Description
CSCvr43959	C9400 ISSU to 16.9.4 or 16.12.1c With Port Security Enabled Causes Traffic Loss
CSCvr51939	Inactive Interfaces Incorrectly Holding Buffers, causing output drops on switch SUP active ports.
CSCvr70470	sessmgrd crash with "clear dot1x mac" command
CSCvr71158	Commands returning invalid PRC error message
CSCvr80063	Memory leak due to bcm54185-debug-slot4 on C9404R version 16.9.4

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1c

Identifier	Description
CSCvq91675	The active and the standby Sup crashes due to ccmc crash when upgraded to 16.12.1.

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
CSCvn65834	Packet drops on mgig ports due to link negotiation issue
CSCvn77683	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvn83940	Cat9k TFTP copy failed with Port Security enabled
CSCvn99610	'speed nonegotiate' config disappears after reload - C9400-LC-24S
CSCvo08436	C9400 - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones
CSCvo15594	Hardware MAC address programming issue for remote client catalyst 9300
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
CSCvo33809	9400: Input QoS policy may not get installed in Hardware
CSCvo33983	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo41632	C9400-LC-48U goes to faulty status when specific MAC ACL is applied on interfaces

Identifier	Description
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
CSCvo61106	System report not created for stack_mgr crashes on Cat 9500
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 9400 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html

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

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.