Release Notes for Cisco Catalyst 3850 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2025-10-21

Release Notes for Cisco Catalyst 3850 Series Switches, Cisco IOS XE Gibraltar 16.12.x

Introduction

Cisco Catalyst 3850 Series Switches are the next generation of enterprise class stackable access layer switches, with the new and improved 480-Gbps StackWise-480 and Cisco StackPower. Security and application visibility and control are natively built into the switch.

Cisco Catalyst 3850 Series Switches also support full IEEE 802.3 at Power over Ethernet Plus (PoE+), modular and field replaceable network modules, redundant fans, and power supplies. Cisco Catalyst 3650 Series Switches enhance productivity by enabling applications such as IP telephony and video for a true borderless network experience.

Cisco IOS XE represents the continuing evolution of the preeminent Cisco IOS operating system. The Cisco IOS XE architecture and well-defined set of APIs extend the Cisco IOS software to improve portability across platforms and extensibility outside the Cisco IOS environment. The Cisco IOS XE software retains the same look and feel of the Cisco IOS software, while providing enhanced future-proofing and improved functionality.

Whats New in Cisco IOS XE Gibraltar 16.12.14

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 16.12.13

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 16.12.12

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 16.12.11

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 16.12.10a

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

Whats New in Cisco IOS XE Gibraltar 16.12.10

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 16.12.9

Hardware Features in Cisco IOS XE Gibraltar 16.12.9

None.

Software Features in Cisco IOS XE Fuji 16.12.9

Feature Name	Description
Secure Data Wipe	Introduces support for performing factory reset by using the keywo **secure** in the **factory-reset** command. This option performs data sanitisation and securely resets the device.

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

Hardware Features in Cisco IOS XE Gibraltar 16.12.6

There are no new hardware features in this release.

Software Features in Cisco IOS XE Gibraltar 16.12.6

Feature Name	Description, Documentation Link, and License Level Information
License Status Change for Evaluation and Expired Evaluation Licenses	To ensure audit compliance for all your licenses, starting with Cisco IOS XE Gibraltar 16.12.6, a device that is not connected to CSSM will see a change in the license status field, only for evaluation and expired evaluation licenses. What was displayed as `EVAL MODE` (evaluation license) and `EVAL EXPIRED` (expired evaluation license) prior to Cisco IOS XE Gibraltar 16.12.6, is displayed as `IN-USE` starting from Cisco IOS XE Gibraltar 16.12.6. This change in the license status is effective only under the following conditions: • The device was using an evaluation license or an expired evaluation license *prior* to Cisco IOS XE Gibraltar 16.12.6. • The device is *not* connected to CSSM. • The device is now running Cisco IOS XE Gibraltar 16.12.6 or a later release. **Note** • If a device is connected to CSSM, there will be no change in the license status field. • If a device is not connected to CSSM, but is registered with an Specific License Reservation (SLR) authorization code, there will be no change in the license status field. See System Management → Configuring Smart Licensing, section *License Status Change for Evaluation and Expired Evaluation Licenses*. See also Specific License Reservation, section *License Status Change for Evaluation and Expired Evaluation Licenses*. (A license level does not apply)

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

Whats New in Cisco IOS XE Gibraltar 16.12.1

Hardware Features in Cisco IOS XE Gibraltar 16.12.1

None.

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.
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). (IP Base and IP Services)

Feature Name	Description, Documentation Link, and License Level Information
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+. (LAN Base, IP Base, and, IP Services)
IEEE 1588v2, Precision Time Protocol (PTP) support	Introduces PTP support on native Layer 3 ports. See Layer 2 → Configuring Precision Time Protocol (PTP). (IP Base and IP Services)
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. (LAN Base, IP Base, and IP Services)
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 (IP Services)

Feature Name	Description, Documentation Link, and License Level Information
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 (IP Services)
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 (IP Base and IP Services)
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 (LAN Base, IP Base and, IP Services)
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 (IP Services)

Feature Name	Description, Documentation Link, and License Level Information
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: PIM Accept Register • IPv6: Routable Address Hello Option • IPv6: PIM Source-Specific Multicast (SSM) • IPv6: PIM Sparse Mode • IPv6: Scoped Boundary • IPv6: PIMv6 Anycast RP solution (IP Base and IP Services)
IPv6: PBR Recursive Next-Hop	IPv6 support is introduced for PBR Recursive Next-Hop option. (LAN Base, IP Base and, IP Services)
IPv6-based Posture Validation	IPv6 support is introduced for Posture Validation. (LAN Base, IP Base and, IP Services)
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 (LAN Base, IP Base and, IP Services)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: Services	IPv6 support is introduced for AAAA DNS Lookups over an IPv6 Transport. (LAN Base, IP Base and, IP Services)
IPv6: Time-Based Access Lists Using Time Ranges	IPv6 support is introduced for Time-Based Access Lists using time ranges. (LAN Base, IP Base and, IP Services)
IPv6: Triggered RIP	IPv6 support is introduced for Triggered Extensions to RIP.
Programmability • NETCONF-YANG SSH Server Support • OpenFlow • YANG Data Models	The following programmability features are introduced in this release: • 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—Enables integration with open source Faucet SDN Controllers to automate management of layer 2 switching, VLANs, ACLs, and layer 3 routing. • 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. (LAN Base, IP Base, and IP Services)
Stack troubleshooting optimization	The output of the **show tech-support stack** command has been enhanced to include more stack-related information. (A license level does not apply)

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
- Unsupported Features
- Complete List of Supported Features
- Accessing Hidden Commands
- Default Behaviour, on page 11

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

- 802.1x Configurable username and password for MAC Authentication Bypass (MAB)
- Cisco Group Management Protocol (CGMP)
- Cisco Plug-In for OpenFlow (OpenFlow 1.0 and 1.3) is available in Cisco IOS XE Release 3.7.3E, but is not supported in later releases.
- Cisco TrustSec 802.1x
- Cisco TrustSec critical authentication
- Cisco Networking Services (CNS) configuration agent
- Converged Access (CA) is not supported beyond Cisco IOS XE Denali 16.3.x.

  On the Cisco Catalyst 3850 Series Switches, CA is supported in the Cisco IOS XE Denali 16.3.x software release, which has extended support for 40 months.

- Command Switch Redundancy
- Device classifier for Auto Smartports (ASP)
- Dynamic Host Configuration Protocol (DHCP) snooping ASCII circuit ID
- DHCP version 6 (DHCPv6) relay source configuration
- Distance Vector Multicast Routing Protocol (DVMRP) tunneling
- Dynamic access ports
- Fallback bridging for non-IP traffic

- IEEE 802.1X-2010 with 802.1AE support
- Improvements in QoS policing rates
- Ingress Strict Priority Queuing (Expedite)
- IPsec
- IP-in-IP (IPIP) Tunneling
- IPsec VPN
- IP SLA Media Operation
- IPv6 support for Internet Key Exchange (IKE) versoin 2 / IP Security (IPSec) version 3
- IPv6 ready logo phase II - host
- IPv6 static route support on LAN Base images
- IPv6 strict host mode
- Layer 2 tunneling protocol enhancements
- Link-state tracking
- Mesh, FlexConnect, and OfficeExtend access point deployment
- Medianet
- MSE 8.x is not supported with Cisco IOS XE Denali 16.x.x.
- Passive monitoring
- Per VLAN policer
- Performance Monitor (Phase 1)
- Port security on EtherChannels
- Pragmatic General Multicast (PGM)
- RFC 4292 IP-FORWARD-MIB (IPv6 only)
- RFC 4293 IP-MIB (IPv6 only)
- RFC5460 DHCPv6 Bulk leasequery
- Trust boundary configuration
- UniDirectional Link Routing (UDLR)
- VLAN access control lists (VACL) logging of access denied
- Virtual Routing and Forwarding (VRF)-Aware web authentication
- Web-Based Authentication without SVI
- Weighted Random Early Detection (WRED)

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 3850 Series Switches—Model Numbers

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48T-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24P-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48P-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48F-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24U-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-48U-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-12X48U-L	LAN Base	Cisco Catalyst 3850 Stackable 12 100M/1G/2.5G/5G/10G and 36 1G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-L	LAN Base	Cisco Catalyst 3850 Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-24T-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set

Switch Model	Cisco IOS Image	Description
WS-C3850-48T-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply, 1 RU.
WS-C3850-24U-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-48U-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-24PW-S	IP Base	Cisco Catalyst 3850 24-port PoE IP Base with 5-access point license
WS-C3850-48PW-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base with 5-access point license
WS-C3850-12S-S	IP Base	Cisco Catalyst 3850 12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-S	IP Base	Cisco Catalyst 3850 24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-S	IP Base	Cisco Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply
WS-C3850-16XS-S	IP Base	Cisco Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.
WS-C3850-24XS-S	IP Base	Cisco Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.

Switch Model	Cisco IOS Image	Description
WS-C3850-32XS-S	IP Base	Cisco Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.
WS-C3850-48XS-S	IP Base	Standalone Cisco Catalyst 3850 Switch, that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC front-to-back power supply. 1 RU.
WS-C3850-48XS-F-S	IP Base	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC back-to-front power supply. 1 RU.
WS-C3850-12X48U-S	IP Base	Cisco Catalyst 3850 Stackable 12 100M/1G/2.5G/5G/10G and 36 1 G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-S	IP Base	Cisco Catalyst 3850 Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-24T-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-48T-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-24P-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48P-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48F-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set
WS-C3850-24U-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply

Switch Model	Cisco IOS Image	Description
WS-C3850-48U-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
WS-C3850-12S-E	IP Services	Cisco Catalyst 3850 12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-E	IP Services	Cisco Catalyst 3850 24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-E	IP Services	Cisco Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 -W power supply
WS-C3850-16XS-E	IP Services	Cisco Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.
WS-C3850-24XS-E	IP Services	Cisco Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply
WS-C3850-32XS-E	IP Services	Cisco Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-E switch
WS-C3850-12X48U-E	IP Services	Cisco Catalyst 3850 Stackable 12 100M/1G/2.5G/5G/10G and 36 1 G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-E	IP Services	Cisco Catalyst 3850 Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-48XS-E	IP Services	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750 WAC front-to-back power supply. 1 RU.
WS-C3850-48XS-F-E	IP Services	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC back-to-front power supply. 1 RU.

Network Modules

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

Network Module	Description
C3850-NM-4-1G	This module has four 1 G SFP module slots. Any combination of standa supported. SFP+ modules are not supported. If you insert an SFP+ module in the 1G network module, the SFP+ mod and the switch logs an error message. Note the supported switch models: • WS-C3850-24T/P/U • WS-C3850-48T/F/P/U • WS-C3850-12X48U • WS-C3850-24XU • WS-C3850-12S • WS-C3850-24S
C3850-NM-2-10G	This module has four slots: Two slots (left side) support only 1 G SFP modules and two slots (right G SFP or 10 G SFP modules. Note the supported switch models • WS-C3850-24T/P/U • WS-C3850-48T/F/P/U • WS-C3850-12X48U • WS-C3850-24XU • WS-C3850-12S • WS-C3850-24S
C3850-NM-4-10G	This module has four 10 G slots or four 1 G slots. Note the supported switch models • WS-C3850-48T/F/P/U • WS-C3850-12X48U • WS-C3850-24XU • WS-C3850-12XS • WS-C3850-24XS

Network Module	Description
C3850-NM-8-10G	This module has eight 10 G slots with an SFP+ port in each slot. Ea 10 G connection Note the supported switch models • WS-C3850-12X48U • WS-C3850-24XU • WS-C3850-24XS
C3850-NM-2-40G	This module has two 40 G slots with a QSFP+ connector in each slo • WS-C3850-12X48U • WS-C3850-24XU • WS-C3850-24XS

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.

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Gibraltar 16.12.14	Not applicable	Not applicable	Not applicable	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 16.12.13	Not applicable	Not applicable	Not applicable	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 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Gibraltar 16.12.12	Not applicable	Not applicable	Not applicable	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 16.12.11	Not applicable	Not applicable	Not applicable	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 16.12.10a	Not applicable	Not applicable	Not applicable	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 16.12.10	Not applicable	Not applicable	Not applicable	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 16.12.9	Not applicable	Not applicable	Not applicable	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 16.12.8	Not applicable	Not applicable	Not applicable	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 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Gibraltar 16.12.7	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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 16.12.5b	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Gibraltar 16.12.3	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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**.
Fuji 16.9.8	Not applicable	Not applicable	Not applicable	2.3 Patch 1 2.4 Patch 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	Not applicable	Not applicable	Not applicable	2.3 Patch 1 2.4 Patch 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	Not applicable	Not applicable	Not applicable	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 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Fuji 16.9.5	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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	Not applicable	Not applicable	Not applicable	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 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Everest 16.6.4	Not applicable	Not applicable	Not applicable	2.2 2.3	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack See Cisco Prime Infrastructure 3.1→ **Downloads**.
Everest 16.6.3	Not applicable	Not applicable	Not applicable	2.2 2.3	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack See Cisco Prime Infrastructure 3.1→ **Downloads**.
Everest 16.6.2	Not applicable	Not applicable	Not applicable	2.2 2.3	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack See Cisco Prime Infrastructure 3.1→ **Downloads**.
Everest 16.6.1	Not applicable	Not applicable	Not applicable	2.2	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack See Cisco Prime Infrastructure 3.1→ **Downloads**.
Everest 16.5.1a	Not applicable	Not applicable	Not applicable	2.1 Patch 3	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack See Prime Infrastructure 3.1→ **Downloads**.

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.3.6	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.2 Patch 2(wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7 + PI 3.1 latest device pack 16 (Wired). PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7 + PI 3.1 latest device pack 14 (Wireless). See Cisco Prime Infrastructure 3.1→ **Downloads**.
Denali 16.3.5b	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.2 Patch 2(wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1.5 + PI 3.1.5 update 1 + PI 3.1 latest device pack (Wired) PI 3.1 + PI 3.1 maintenance release 7+ PI 3.1 latest device pack (Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.
Denali 16.3.5	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.2 Patch 2(wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1.5 + PI 3.1.5 update 1 + PI 3.1 latest device pack (Wired) PI 3.1 + PI 3.1 maintenance release 7+ PI 3.1 latest device pack (Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.3.3	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.1 Patch 1 (Wired and Wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1.5 + PI 3.1.5 update 1 + PI 3.1 latest device pack (Wired) PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack (Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.
Denali 16.3.2	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.1 Patch 1 (Wired and Wireless)	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack (Wired and Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.
Denali 16.3.1	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.0 Patch 3 1.4 Patch 7 1.3 Patch 6 (Wired and Wireless)	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack (Wired and Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.
Denali 16.2.2	03.07.02E 03.06.03E	8.1.0, 8.2.0	CMX 10.2.2	1.3 Patch 5 (Wired and Wireless)	5.3 5.4	3.1.0 + Device Pack 1 (Wired and Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.
Denali 16.2.1	03.07.03E 03.06.03E	8.1.0 8.2.0	CMX 10.2.2	1.3 Patch 5 (Wired and Wireless)	5.3 5.4	3.1.0 (Wired) 3.1.0, 3.0.2[1] + Device Pack 4 + PI 3.0 Technology Pack (Wireless) See Cisco Prime Infrastructure 3.1→ **Downloads**.

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.1.3	03.07.02E 03.06.03E	8.1.0	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + Device Pack 5+ PI 3.0 Technology Pack See Cisco Prime Infrastructure 3.0 → **Downloads**
Denali 16.1.2	03.07.02E 03.06.03E	8.1.0	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + Device Pack 4 + PI 3.0 Technology Pack See Cisco Prime Infrastructure 3.0 → **Downloads**
Denali 16.1.1	03.07.02E 03.06.03E	8.1.0	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + PI 3.0 Device Pack 2 + PI 3.0 Technology Pack See Cisco Prime Infrastructure 3.0 → **Downloads**.
03.07.03E 03.07.02E 03.07.01E 03.07.00E	03.07.03E 03.07.02E 03.07.01E 03.07.00E	8.0 8.0 8.0 7.6	8.0[3]	1.3	5.2 5.3	2.2 See Cisco Prime Infrastructure 2.2 → **Downloads**.
03.06.04E 03.06.03E 03.06.02aE 03.06.01E 03.06.00E	03.06.04E 03.06.02aE 03.06.01E 03.06.00E	8.0 8.0 - 7.6	8.0	1.3 1.2	5.2 5.3	2.2 2.2, 2.1.2, or 2.1.1 if MSE is also deployed[4] 2.1.0 if MSE is not deployed See Cisco Prime Infrastructure 2.2 → **Downloads** and Cisco Prime Infrastructure 2.1 → **Downloads**
03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	7.6[5] 7.5	7.5	1.2	5.2, 5.3	2.0 See Cisco Prime Infrastructure 2.0 → **Downloads**

[1] The Cisco IOS XE Denali 16.2.1 features are not available with 3.0.2, but 3.0.2 is compatible with Cisco IOS XE Denali 16.2.1

[2] Cisco 5700 (with Cisco IOS XE Release 03.06.03E/Cisco IOS XE Release 03.07.02E) inter-operates as a Peer MC with Catalyst 3850 running Cisco IOS XE Denali 16.1.1
[3] Because of SHA-2 certificate implementation, MSE 7.6 is not compatible with Cisco IOS XE Release 3.6E and later. Therefore, we recommend that you upgrade to MSE 8.0.
[4] If MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.
[5] Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.
[6] Prime Infrastructure 2.0 enables you to manage Cisco WLC 7.5.102.0 with the features of Cisco WLC 7.4.110.0 and earlier releases. Prime Infrastructure 2.0 does not support any features of Cisco WLC 7.5.102.0 including the new AP platforms.

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[7]	512 MB[8]	256	1280 x 800 or higher	Small

[7] We recommend 1 GHz
[8] 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)

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 16.12.14	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.
Cisco IOS XE Gibraltar 16.12.13	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.
Cisco IOS XE Gibraltar 16.12.12	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.
Cisco IOS XE Gibraltar 16.12.11	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.
Cisco IOS XE Gibraltar 16.12.10a	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.
Cisco IOS XE Gibraltar 16.12.10	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.
Cisco IOS XE Gibraltar 16.12.9	Universal	cat3k_caa-universalk9.16.1
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.12.8	Universal	cat3k_caa-universalk9.16.12.08
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.7	Universal	cat3k_caa-universalk9.16.12.07
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.6	Universal	cat3k_caa-universalk9.16.12.06
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.5b	Universal	cat3k_caa-universalk9.16.12.05
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.5	Universal	cat3k_caa-universalk9.16.12.05
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.4	Universal	cat3k_caa-universalk9.16.12.04
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.3a	Universal	cat3k_caa-universalk9.16.12.03
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.3	Universal	cat3k_caa-universalk9.16.12.03
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.
Cisco IOS XE Gibraltar 16.12.1	Universal	cat3k_caa-universalk9.16.12.01
	Universal without Datagram Transport Layer Service (DTLS)	cat3k_caa-universalk9ldpe.16.

Automatic Boot Loader Upgrade

When you upgrade from any prior Cisco IOS XE 3.x.xE release to a Cisco IOS XE Denali 16.x.x, or Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to a Cisco IOS XE Release 3.x.xE, your boot loader will not be downgraded. The updated boot loader supports all previous releases.

For subsequent Cisco IOS XE Denali 16.x.x, or Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x, or Cisco IOS XE Gibraltar 16.x.x releases, if there is a new bootloader in the release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.



Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Gibraltar 16.12.9 or Cisco IOS XE Gibraltar 16.12.10 or Cisco IOS XE Gibraltar 16.12.10a or Cisco IOS XE Gibraltar 16.12.11 or Cisco IOS XE Gibraltar 16.12.12 or Cisco IOS XE Gibraltar 16.12.13 or Cisco IOS XE Gibraltar 16.12.14 the first time	The boot loader may be upgraded to version 6.08. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 6.08, RELEASE SOFTWARE (P)`
	If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Gibraltar 16.12.9 or Cisco IOS XE Gibraltar 16.12.10 or Cisco IOS XE Gibraltar 16.12.10a or Cisco IOS XE Gibraltar 16.12.11 or Cisco IOS XE Gibraltar 16.12.12 or Cisco IOS XE Gibraltar 16.12.13 or Cisco IOS XE Gibraltar 16.12.14, you will see the following on the console:
	`%IOSXEBOOT-Tue-###: (rp/0): Mar 11 01:07:23 Universal 2020 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING 4`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4`

If you boot Cisco IOS XE Gibraltar 16.12.7 or Cisco IOS XE Gibraltar 16.12.8 the first time	The boot loader may be upgraded to version 5.08. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 5.08, RELEASE SOFTWARE (P)`
	If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Gibraltar 16.12.7 or Cisco IOS XE Gibraltar 16.12.8, you will see the following on the console:
	`%IOSXEBOOT-Tue-###: (rp/0): Apr 11 01:07:22 Universal 2020 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING 4`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4`

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Gibraltar 16.12.3 or Cisco IOS XE Gibraltar 16.12.3a or Cisco IOS XE Gibraltar 16.12.4 or Cisco IOS XE Gibraltar 16.12.5 or Cisco IOS XE Gibraltar 16.12.5b or Cisco IOS XE Gibraltar 16.12.6 the first time	The boot loader may be upgraded to version 4.78. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.78, RELEASE SOFTWARE (P)`
	If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Gibraltar 16.12.3 or Cisco IOS XE Gibraltar 16.12.3a or Cisco IOS XE Gibraltar 16.12.4 or Cisco IOS XE Gibraltar 16.12.5 or Cisco IOS XE Gibraltar 16.12.6, you will see the following on the console:
	`%IOSXEBOOT-Tue-###: (rp/0): Mar 11 13:07:19 Universal 2020 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING 4`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4`

If you boot Cisco IOS XE Gibraltar 16.12.1 first time	The boot loader may be upgraded to version 4.68. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.68, RELEASE SOFTWARE (P)`
	If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Gibraltar 16.12.1, you will see the following on the console:
	`%IOSXEBOOT-Tue-###: (rp/0): Oct 17 13:07:19 Universal 2017 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING 4`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4`

Automatic Microcode Upgrade

During a Cisco IOS image upgrade or downgrade on a PoE or UPoE switch, microcode is upgraded to reflect applicable feature enhancements and bug fixes. A microcode upgrade occurs only during an image upgrade or downgrade, on PoE or UPoE switches. It does not occur during switch reloads or on non-PoE switches.

Depending on the release you are upgrading from, microcode upgrade can occur during the install operation or during bootup:

- If the release you are upgrading *from* does not support microcode updates during the course of installation, microcode is updated during boot up, and an additional 4 minutes (approximately) are required to complete the microcode upgrade, in addition to the normal reload time. Data traffic is not forwarded when microcode is upgraded during bootup.
- When using **install** commands to upgrade, microcode is upgraded during the install operation, and no additional time is required during bootup. Here microcode is updated before the reload that occurs as part of the image upgrade process. Data traffic continues to be forwarded during the upgrade.

Do not restart the switch during the upgrade or downgrade process.

The following console messages are displayed during microcode upgrade:

```
MM [1] MCU version 111 sw ver 105
MM [2] MCU version 111 sw ver 105
```

```
Front-end Microcode IMG MGR: found 4 microcode images for 1 device.
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_0 update needed: no
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_1 update needed: yes
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_2 update needed: yes
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_3 update needed: no

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0], index=0 ...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0], index=1 ...395790 bytes.
Front-end Microcode IMG MGR: Programming device 0...rwRrrrrrrw..
0%.....................................................................
10%.....................................................................
20%.....................................................................
30%.....................................................................
40%.....................................................................
50%.....................................................................
60%.....................................................................
70%.....................................................................
80%.....................................................................
90%.....................................................................
100%
Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...25186 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%....100%wRr!
Front-end Microcode IMG MGR: Microcode programming complete for device 0.
Front-end Microcode IMG MGR: Preparing to program device[0], index=3 ...86370 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 242 seconds
```

Software Installation Commands

This table of commands is supported in the Cisco IOS XE Release 3.x.xE release train.	
`Device# software`	
auto-upgrade	Initiates auto upgrade for switches running incompatible software
clean	Cleans unused package files from local media
commit	Commits the provisioned software and cancels the automatic rollback timer
expand	Expands a software bundle to local storage, default location is where the bundle currently resides
install	Installs software
rollback	Rolls back the committed software

This table of commands is supported starting from Cisco IOS XE Denali 16.x.x	
`Device# request platform software package ?`	
clean	Cleans unnecessary package files from media
copy	Copies package to media

This table of commands is supported starting from Cisco IOS XE Denali 16.x.x	
describe	Describes package content
expand	Expands all-in-one package to media
install	Installs the package
uninstall	Uninstalls the package
verify	Verifies In Service Software Upgrade (ISSU) software package compatibility

This table of commands is supported starting from Cisco IOS XE Fuji 16.8.1a	
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 from Cisco IOS XE Gibraltar 16.12.1 in Install Mode, on page 66 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:cat3k_caa-universalk9.16.12.01.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 from Cisco IOS XE Release 3.x.xE in Install Mode

Follow these instructions to upgrade from Cisco IOS XE Release 3.x.xE in install mode:

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Any Cisco IOS XE Release 3.x.xE	Only **software** commands	Cisco IOS XE Gibraltar 16.x.x or Cisco IOS XE Fuji 16.x.x or Cisco IOS XE Everest 16.x.x or Cisco IOS XE Denali 16.x.x

The sample output shows upgrade from Cisco IOS XE Release 3.7.3E to Cisco IOS XE Gibraltar 16.12.1 in install mode.

Procedure

Step 1 Copy new image to stack

When you expand the image, if you point to the source image on your TFTP server, you can skip this section and go to Step 2: Software install image to flash

a) **show run | i tftp**

Use this command to make sure your tftp server is reachable from IOS via GigabitEthernet0/0.

```
Switch# show run | i tftp
ip tftp source-interface GigabitEthernet0/0
ip tftp blocksize 8192
Switch#
Switch# show run | i ip route vrf
ip route vrf Mgmt-vrf 5.0.0.0 255.0.0.0 5.30.0.1
Switch#
Switch# show run int GigabitEthernet0/0
```

```
Building configuration...

Current configuration : 115 bytes
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
ip address 5.30.12.121 255.255.0.0
negotiation auto
end
Switch#
Switch# ping vrf Mgmt-vrf ip 5.28.11.250
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.28.11.250, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

b) **copy tftp: flash:**

Use this command to copy the image from your tftp server to flash.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin flash:
cat3k_caa-universalk9.16.12.01.SPA.bin
Destination filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin...
Loading cat3k_caa-universalk9.16.12.01.SPA.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 373203016 bytes]

373203016 bytes copied in 80.662 secs (4626927 bytes/sec)
Switch#
```

c) **dir flash:**

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

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

32339 -rw- 373217171 Wed Jul 2019 13:52:53 -07:00 cat3k_caa-universalk9.16.12.01.SPA.bin

1562509312 bytes total (731021312 bytes free)
Switch#
```

Step 2 Software install image to flash

a) **software install file**

Use this command with the **new** and **force** options, to expand 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# software install file flash:cat3k_caa-universalk9.16.12.01.SPA.bin new force
Preparing install operation ...
[1]: Copying software from active switch 1 to switches 2,3,4
[1]: Finished copying software to switches 2,3,4
[1 2 3 4]: Starting install operation
[1 2 3 4]: Expanding bundle flash:cat3k_caa-universalk9.16.12.01.SPA.bin
[1 2 3 4]: Copying package files
[1 2 3 4]: Package files copied
[1 2 3 4]: Finished expanding bundle flash:cat3k_caa-universalk9.16.12.01.SPA.bin
[1 2 3 4]: Verifying and copying expanded package files to flash:
[1 2 3 4]: Verified and copied expanded package files to flash:
```

```
[1 2 3 4]: Starting compatibility checks
[1 2 3 4]: Bypassing peer package compatibility checks due to 'force' command option
[1 2 3 4]: Finished compatibility checks
[1 2 3 4]: Starting application pre-installation processing
[1 2 3 4]: Finished application pre-installation processing
[1]: Old files list:
Removed cat3k_caa-base.SPA.03.07.03E.pkg
Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
Removed cat3k_caa-infra.SPA.03.07.03E.pkg
Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
Removed cat3k_caa-platform.SPA.03.07.03E.pkg
Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[2]: Old files list:
Removed cat3k_caa-base.SPA.03.07.03E.pkg
Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
Removed cat3k_caa-infra.SPA.03.07.03E.pkg
Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
Removed cat3k_caa-platform.SPA.03.07.03E.pkg
Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[3]: Old files list:
Removed cat3k_caa-base.SPA.03.07.03E.pkg
Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
Removed cat3k_caa-infra.SPA.03.07.03E.pkg
Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
Removed cat3k_caa-platform.SPA.03.07.03E.pkg
Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[4]: Old files list:
Removed cat3k_caa-base.SPA.03.07.03E.pkg
Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
Removed cat3k_caa-infra.SPA.03.07.03E.pkg
Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
Removed cat3k_caa-platform.SPA.03.07.03E.pkg
Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[1]: New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
[2]: New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
[3]: New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
[4]: New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
[1 2 3 4]: Creating pending provisioning file
[1 2 3 4]: Finished installing software. New software will load on reboot.
[1 2 3 4]: Committing provisioning file

[1 2 3 4]: Do you want to proceed with reload? [yes/no]: yes
[1 2 3 4]: Reloading
```

```
Switch#
```

Note
Old files listed in the logs should be removed using the **request platform software package clean switch all** command, after reload.

Step 3 Reload

If you said 'Yes' to the prompt in software install and your switches are configured with auto boot, the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

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

Use this command to manually boot the new image.

Note
When you boot the new image, the boot loader is automatically updated.

```
switch: boot flash:packages.conf
```

b) **show version**

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

```
Switch# show version
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.12.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

c) **delete flash:**

After you have successfully installed the image, you no longer need the .bin image and the file can be deleted from the flash of each switch if it was copied to flash.

```
Switch# delete flash:cat3k_caa-universalk9.16.12.01.SPA.bin
Delete filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Delete flash:/cat3k_caa-universalk9.16.12.01.SPA.bin? [confirm]
Switch#
```

Upgrading from Cisco IOS XE Release 3.x.xE in Bundle Mode

Follow these instructions to upgrade from Cisco IOS XE Release 3.x.xE in bundle mode:

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Any Cisco IOS XE Release 3.x.xE	Only **request platform software** commands	Cisco IOS XE Gibraltar 16.x.x or Cisco IOS XE Fuji 16.x.x or Cisco IOS XE Everest 16.x.x or Cisco IOS XE Denali 16.x.x

The sample output shows upgrade from Cisco IOS XE Release 3.7.3E to Cisco IOS XE Gibraltar 16.12.1

Procedure

Step 1 Copy new image to stack

Note
You cannot boot Cisco IOS XE Gibraltar 16.x.x, Cisco IOS XE Fuji 16.x.x, Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Denali 16.x.x via TFTP for the first time with a Cisco IOS XE 3.x.xE boot loader. The Cisco IOS XE 3.x.xE boot loaders have a limitation, which prevents the booting of an image larger than 400MB via the TFTP server. Since Cisco IOS XE Gibraltar 16.x.x, Cisco IOS XE Fuji 16.x.x, Cisco IOS XE Everest 16.x.x, and Cisco IOS XE Denali 16.x.x images are larger than 400MB, you must boot the image via flash.

a) **show run | i tftp**

Use this command to make sure your tftp server is reachable from IOS via GigabitEthernet0/0.

```
Switch# show run | i tftp
ip tftp source-interface GigabitEthernet0/0
ip tftp blocksize 8192
Switch#
Switch# show run | i ip route vrf
ip route vrf Mgmt-vrf 5.0.0.0 255.0.0.0 5.30.0.1
Switch#
Switch# show run int GigabitEthernet0/0
Building configuration...

Current configuration : 115 bytes
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
ip address 5.30.12.121 255.255.0.0
negotiation auto
end
Switch#
Switch# ping vrf Mgmt-vrf ip 5.28.11.250
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.28.11.250, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

b) **copy tftp: flash:**

Use this command to copy the image from your tftp server to flash.

Note
If you have a stack, you must copy the image to the flash drive of each switch in the stack.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin flash:
cat3k_caa-universalk9.16.12.01.SPA.bin
Destination filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin...
Loading cat3k_caa-universalk9.16.12.01.SPA.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 373203016 bytes]

373203016 bytes copied in 80.662 secs (4626927 bytes/sec)
Switch#
```

c) **dir flash:**

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

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

32339 -rw- 373217171 Mar 06 2018 13:52:53 -07:00 cat3k_caa-universalk9.16.12.01.SPA.bin
1562509312 bytes total (731021312 bytes free)
Switch#
```

Step 2 Edit the boot variable

a) **no boot system**

Use this command to clear the boot variable.

```
Switch(config)# no boot system
```

b) **boot system**

Use this command to edit the boot variable, to point to the new image.

```
Switch(config)# boot system flash:cat3k_caa-universalk9.16.12.01.SPA.bin
```

c) **write memory**

Use this command to save configuration changes.

```
Switch# write memory
```

d) **show boot**

Use this command to display and verify that your boot variable is pointing to the new image.

```
Switch# show boot
---------------------------
Switch 1
---------------------------
Current Boot Variables:
BOOT variable = flash:cat3k_caa-universalk9.16.12.01.SPA.bin;

Boot Variables on next reload:
BOOT variable = flash:cat3k_caa-universalk9.16.12.01.SPA.bin;
Allow Dev Key = yes
Manual Boot = yes
Enable Break = yes
Switch#
```

Step 3 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash**

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

Note
When you boot the new image, the boot loader is automatically updated.

```
switch:boot flash:cat3k_caa-universalk9.16.12.01.SPA.bin
```

c) **show version**

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

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
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 Move from bundle mode to install mode

Ensure you have enough space in flash to expand a new image by cleaning up old installation files. This command will erase your Cisco IOS XE Gibraltar 16.12.1 bin image file, so ensure that you copy it to your Active again.

a) **request platform software package clean switch all**

Use the **switch all** option to clean up all switches in your stack.

```
Switch# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
Running command on switch 2
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
Running command on switch 3
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
Running command on switch 4
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.
The following files will be deleted:
[1]:
```

```
/flash/cat3k_caa-base.SPA.03.07.02E.pkg
/flash/cat3k_caa-drivers.SPA.03.07.02E.pkg
/flash/cat3k_caa-infra.SPA.03.07.02E.pkg
/flash/cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
/flash/cat3k_caa-platform.SPA.03.07.02E.pkg
/flash/cat3k_caa-universalk9.16.12.01.SPA.bin
/flash/cat3k_caa-wcm.SPA.10.3.120.0.pkg
/flash/packages.conf
[2]:
/flash/cat3k_caa-base.SPA.03.07.02E.pkg
/flash/cat3k_caa-drivers.SPA.03.07.02E.pkg
/flash/cat3k_caa-infra.SPA.03.07.02E.pkg
/flash/cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
/flash/cat3k_caa-platform.SPA.03.07.02E.pkg
/flash/cat3k_caa-universalk9.16.12.01.SPA.bin
/flash/cat3k_caa-wcm.SPA.10.3.120.0.pkg
/flash/packages.conf
[3]:
/flash/cat3k_caa-base.SPA.03.07.02E.pkg
/flash/cat3k_caa-drivers.SPA.03.07.02E.pkg
/flash/cat3k_caa-infra.SPA.03.07.02E.pkg
/flash/cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
/flash/cat3k_caa-platform.SPA.03.07.02E.pkg
/flash/cat3k_caa-universalk9.16.12.01.SPA.bin
/flash/cat3k_caa-wcm.SPA.10.3.120.0.pkg
/flash/packages.conf
[4]:
/flash/cat3k_caa-base.SPA.03.07.02E.pkg
/flash/cat3k_caa-drivers.SPA.03.07.02E.pkg
/flash/cat3k_caa-infra.SPA.03.07.02E.pkg
/flash/cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
/flash/cat3k_caa-platform.SPA.03.07.02E.pkg
/flash/cat3k_caa-universalk9.16.12.01.SPA.bin
/flash/cat3k_caa-wcm.SPA.10.3.120.0.pkg
/flash/packages.conf

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat3k_caa-base.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-drivers.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-infra.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg ... done.
Deleting file flash:cat3k_caa-platform.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.12.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-wcm.SPA.10.3.120.0.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat3k_caa-base.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-drivers.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-infra.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg ... done.
Deleting file flash:cat3k_caa-platform.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.12.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-wcm.SPA.10.3.120.0.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat3k_caa-base.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-drivers.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-infra.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg ... done.
Deleting file flash:cat3k_caa-platform.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.12.01.SPA.bin ... done.
```

```
Deleting file flash:cat3k_caa-wcm.SPA.10.3.120.0.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
[4]:
Deleting file flash:cat3k_caa-base.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-drivers.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-infra.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg ... done.
Deleting file flash:cat3k_caa-platform.SPA.03.07.02E.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.12.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-wcm.SPA.10.3.120.0.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
Switch#
```

b) **copy tftp:**

Use this command to copy the image from your tftp server to flash

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin flash:
cat3k_caa-universalk9.16.12.01.SPA.bin
Destination filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin...
Loading cat3k_caa-universalk9.16.12.01.SPA.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 373203016 bytes]

373203016 bytes copied in 80.662 secs (4626927 bytes/sec)
Switch#
```

c) **request platform software package expand**

Use this command to expand the target image to flash and move from bundle mode to install mode. You can point to the source image on your TFTP server or in flash if you have it copied to flash. Use the **switch all** option to upgrade all switches in your stack. Use the **auto-copy** option to copy the .bin image from flash: to all other switches in your stack.

```
Switch# request platform software package expand switch all file
flash:cat3k_caa-universalk9.16.12.01.SPA.bin auto-copy
[1]: Copying flash:cat3k_caa-universalk9.16.12.01.SPA.bin from switch 1 to switch 2 3 4
[2 3 4]: Finished copying to switch 2 3 4
[1 2 3 4]: Expanding file
[1 2 3 4]: Finished expanding all-in-one software package in switch 1 2 3 4
SUCCESS: Finished expanding all-in-one software package.
Switch#
```

Step 5 Edit the boot variable

a) **no boot system**

Use this command to clear the boot variable.

```
Switch(config)# no boot system
```

b) **boot system**

Use this command to edit the boot variable to point to the new image.

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

c) **write memory**

Use this command to save configuration changes.

```
Switch# write memory
```

d) **show boot**

Use this command to display and verify that your boot variable is pointing to the new image.

```
Switch# show boot
----------------------------
Switch 1
----------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes
Switch#
```

Step 6 Reload

a) **reload**

Use this command to to reload the switch.

```
Switch# reload
```

b) **boot flash**

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

Note
When you boot the new image, the boot loader is automatically updated.

```
switch:boot flash:packages.conf
```

c) **show version**

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

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.12.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

Upgrading from Cisco IOS XE Denali 16.x.x in Install Mode

Follow these instructions to upgrade from a Cisco IOS XE Denali 16.x.x release to a later release in install mode. In order to perform a software image upgrade, you must be booted into IOS using **boot flash:packages.conf**.

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Cisco IOS XE Denali 16.x.x or Cisco IOS XE Everest 16.x.x	Only **request platform software** commands.	Cisco IOS XE Gibraltar 16.x.x or Cisco IOS XE Fuji 16.x.x or Cisco IOS XE Everest 16.x.x or Cisco IOS XE Denali 16.x.x

The sample output shows upgrade from Cisco IOS XE Denali 16.3.5 to Cisco IOS XE Gibraltar 16.12.1 in install mode.

Procedure

Step 1 Clean Up

a) **request platform software package clean switch all file flash:**

Use this command to clean up old installation files; this ensures that you have sufficient space in the flash drive, to expand a new image. Use the **switch all** option to clean up all switches in your stack.

```
Switch# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-guestshell.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpbase.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-wcm.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.03.05.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 2
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-guestshell.16.03.05.SPA.pkg
File is in use, will not delete.
```

```
cat3k_caa-rpbase.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-wcm.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.03.05.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 3
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-guestshell.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpbase.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-wcm.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.03.05.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 4
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
packages.conf
File is in use, will not delete.
cat3k_caa-guestshell.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpbase.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-wcm.16.03.05.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.03.05.SPA.pkg
File is in use, will not delete.
packages.conf
done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
```

Step 2 Copy new image to stack

Copy the new image to flash: (If you point to the source image on a TFTP server you can skip this section and go to: Software install image to flash).

a) **copy tftp: flash:**

Use this command to copy the image from the tftp server to flash.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin flash:
cat3k_caa-universalk9.16.12.01.SPA.bin
Destination filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.12.01.SPA.bin...
Loading cat3k_caa-universalk9.16.12.01.SPA.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 373203016 bytes]
```

b) **dir flash:**

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

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

32339 -rw- 373217171 Jul 24 2019 13:52:53 -07:00 cat3k_caa-universalk9.16.12.01.SPA.bin


1562509312 bytes total (731021312 bytes free)
Switch#
```

Step 3 Software install image to flash

a) **request platform software package install**

Use this command to install the target image to flash. Use the **switch all** option to upgrade all switches in your stack. Use the **auto-copy** option to copy the .bin image from flash: to all other switches in your stack

We recommend copying the image to a TFTP server or the flash drive of the active switch. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3, the corresponding flash drive is flash-3: `Switch#` **`request platform software package install switch all file flash-3:cat3k_caa-universalk9.16.12.01.SPA.bin new auto-copy`**

Note
You must use the **new** option when you upgrade from Cisco IOS XE Denali 16.1.x, 16.2.x or 16.3.1 to Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x, or Cisco IOS XE Gibraltar 16.x.x , because there are packaging changes in the different 16.x.x releases.

Note
When you execute the command, the following message is displayed. This is expected and does not affect the upgrade. See CSCux82059: `Unknown package type 21`

```
Switch# request platform software package install switch all file
flash:cat3k_caa-universalk9.16.12.01.SPA.bin new auto-copy
Expanding image file: flash:cat3k_caa-universalk9.16.12.01.SPA.bin
[1]: Copying flash:cat3k_caa-universalk9.16.12.01.SPA.bin from switch 1 to switch 2 3 4
[2 3 4]: Finished copying to switch 2 3 4
[1 2 3 4]: Expanding file
[1 2 3 4]: Finished expanding all-in-one software package in switch 1 2 3 4
SUCCESS: Finished expanding all-in-one software package.
[1 2 3 4]: Performing install
Unknown package type 21
Unknown package type 21
Unknown package type 21
```

```
Unknown package type 21
SUCCESS: install Finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-guestshell.16.03.05.SPA.pkg
Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
Removed cat3k_caa-rpcore.16.03.05.pkg
Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
Removed cat3k_caa-wcm.16.03.05.SPA.pkg
Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-guestshell.16.03.05.SPA.pkg
Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
Removed cat3k_caa-rpcore.16.03.05.pkg
Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
Removed cat3k_caa-wcm.16.03.05.SPA.pkg
Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-guestshell.16.03.05.SPA.pkg
Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
Removed cat3k_caa-rpcore.16.03.05.pkg
Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
Removed cat3k_caa-wcm.16.03.05.SPA.pkg
Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[3]: Finished install successful on switch 3
[4]: install package(s) on switch 4
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-guestshell.16.03.05.SPA.pkg
Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
Removed cat3k_caa-rpcore.16.03.05.pkg
Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
Removed cat3k_caa-wcm.16.03.05.SPA.pkg
```

```
Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
Added cat3k_caa-rpbase.16.12.01.SPA.pkg
Added cat3k_caa-rpcore.16.12.01.SPA.pkg
Added cat3k_caa-srdriver.16.12.01.SPA.pkg
Added cat3k_caa-guestshell.16.12.01.SPA.pkg
Added cat3k_caa-webui.16.12.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[4]: Finished install successful on switch 4
Checking status of install on [1 2 3 4]
[1 2 3 4]: Finished install in switch 1 2 3 4
SUCCESS: Finished install: Success on [1 2 3 4]
Switch#
```

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

b) **dir flash:**

After you have successfully installed the software, use this command to verify that the flash partition has five new .pkg files and one updated packages.conf file. See sample output below:

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

Directory of flash:/

7747  -rw- 281076014 Mar 27 2016 22:15:50 +00:00 cat3k_caa-guestshell.16.03.05.SPA.pkg
7748  -rw- 7197312   Mar 27 2016 22:15:51 +00:00 cat3k_caa-rpbase.16.03.05.SPA.pkg
7749  -rw- 166767220 Mar 27 2016 22:15:51 +00:00 cat3k_caa-rpcore.16.03.05.pkg
7750  -rw- 14631548  Mar 27 2016 22:15:51 +00:00 cat3k_caa-srdriver.16.03.05.SPA.pkg
31000 -rw- 22173354  Mar 27 2016 04:40:38 -07:00 cat3k_caa-wcm.16.03.05.SPA.pkg
30996 -rw- 266177140 Mar 27 2017 04:40:36 -07:00 cat3k_caa-webui.16.03.05.SPA.pkg

30998 -rw- 9067132   Jul 24 2019 04:40:37 -07:00 cat3k_caa-rpbase.16.12.01.SPA.pkg
30999 -rw- 178403952 Jul 24 2019 04:40:38 -07:00 cat3k_caa-rpcore.16.12.01.SPA.pkg
30997 -rw- 13333112  Jul 24 2019 04:40:39 -07:00 cat3k_caa-srdriver.16.12.01.SPA.pkg
30994 -rw- 13333112  Jul 24 2019 04:40:40 -07:00 cat3k_caa-guestshell.16.12.01.SPA.pkg
30994 -rw- 13333112  Jul 24 2019 04:40:41 -07:00 cat3k_caa-webui.16.12.01.SPA.pkg
1621966848 bytes total (132620288 bytes free)


Switch# dir flash:*.conf
Directory of flash:/packages.conf

32342 -rw- 4690 Jul 24 2019 04:40:42 -07:00 packages.conf

1562509312 bytes total (730988544 bytes free)
Switch#
```

c) **dir flash:*.bin**

After you have successfully installed the image, you no longer need the.bin image. If you copied the file to flash, use this command to check if it is still saved in the the flash of each switch.

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

32339 -rw- 373217171 Jul 24 2019 13:52:53 -07:00 cat3k_caa-universalk9.16.12.01.SPA.bin
```

```
1562509312 bytes total (731021312 bytes free)
Switch#
```

d) **delete flash:**

If an image is still saved, use this command to delete it, if not, it has been deleted as part of the install operation and you can skip this step.

```
Switch# delete flash:cat3k_caa-universalk9.16.12.01.SPA.bin
Delete filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Delete flash:/ cat3k_caa-universalk9.16.12.01.SPA.bin? [confirm]
Switch#
```

Step 4 Reload

a) **reload**

Use this command in the privileged EXEC mode to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If the switch is configured with auto boot, then the stack automatically boots up with the new image. If not, you can manually boot flash:packages.conf

```
switch:boot flash:packages.conf
```

c) **show version**

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

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.12.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

Downgrading to Cisco IOS XE 3.x.xE in Bundle Mode

Follow these instructions to downgrade to older Cisco IOS XE Release 3.x.xE releases in bundle mode.

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Denali 16.x.x or Cisco IOS XE Everest 16.x.x	Only **request platform software** commands.	Cisco IOS XE Release 3.x.xE

The sample output shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Release 3.7.2E.

Procedure

Step 1 Copy new image to stack

a) **show run | i tftp**

Use this command to make sure your tftp server is reachable from IOS via GigabitEthernet0/0.

```
Switch# show run | i tftp
ip tftp source-interface GigabitEthernet0/0
ip tftp blocksize 8192
Switch#
Switch# show run | i ip route vrf
ip route vrf Mgmt-vrf 5.0.0.0 255.0.0.0 5.30.0.1
Switch#
Switch# show run int GigabitEthernet0/0
Building configuration...

Current configuration : 115 bytes
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
ip address 5.30.12.121 255.255.0.0
negotiation auto
end
Switch#
Switch# ping vrf Mgmt-vrf ip 5.28.11.250
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.28.11.250, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

b) **copy tftp: flash:**

Use this command to copy the image from your tftp server to flash.

Note
If you have a stack, you must copy the image to the flash drive of each switch in the stack.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin flash:
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Destination filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin...
Loading cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!
!!!!!!!!!!!!!!
[OK - 311154824 bytes]

311154824 bytes copied in 68.781 secs (4523849 bytes/sec)
Switch#
```

c) **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:/
```

```
47718 -rw- 311154824 Jul 24 2019 18:17:21 +00:00
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin

3458338816 bytes total (2468995072 bytes free)
Switch#
```

Step 2 Edit the boot variable

a) **no boot system**

Use this command to clear the boot variable.

```
Switch(config)# no boot system
```

b) **boot system**

Use this command to edit the boot variable, to point to the new image.

```
Switch(config)# boot system flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
```

c) **write memory**

Use this command to save configuration changes.

```
Switch# write memory
```

d) **show boot**

Use this command to display and verify that your boot variable is pointing to the new image.

```
Switch# show boot
----------------------------
Switch 1
----------------------------
Current Boot Variables:
BOOT variable = flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin;

Boot Variables on next reload:
BOOT variable = flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin;
Allow Dev Key = yes
Manual Boot = yes
Enable Break = yes
Switch#
```

Step 3 Reload

a) **reload**

Use this command to reload the switch.

```
switch# reload
```

b) **boot flash**

If your switches are configured with auto boot, the stack will automatically boot up with the new image. If not, you can manually boot flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin

Note

When you downgrade to a Cisco IOS XE Release 3.x.xE image, the boot loader does not automatically downgrade. The new boot loader can support booting bothCisco IOS XE Release 3.x.xE as well as Cisco IOS XE Denali 16.x.x, Cisco IOS XE Everest 16.x.x, Cisco IOS XE Fuji 16.x.x, and Cisco IOS XE Gibraltar 16.x.x releases.

```
switch:boot flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
```

c) **show version**

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

```
Switch# show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 03.07.02E RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 24-Jul-19 23:51 by prod_rel_team
```

Step 4 Move from Cisco IOS XE 3.xE Bundle Mode to Install Mode

a) **software clean file flash:**

Use this command to ensure you have enough space in flash to expand a new image by cleaning up old installation files. This command will erase your Cisco IOS XE Release 3.x.xE bin image file, so ensure that you copy it to your active switch again.

```
Switch# software clean file flash:
Preparing clean operation ...
[1 2 3 4]: Cleaning up unnecessary package files
[1 2 3 4]: Preparing packages list to delete ...
[1]: Files that will be deleted:
cat3k_caa-rpbase.16.12.01.SPA.pkg
cat3k_caa-rpcore.16.12.01.SPA.pkg
cat3k_caa-srdriver.16.12.01.SPA.pkg
cat3k_caa-universalk9.16.12.01.SPA.bin
cat3k_caa-guestshell.16.12.01.SPA.pkg
cat3k_caa-webui.16.12.01.SPA.pkg
packages.conf
[2]: Files that will be deleted:
cat3k_caa-rpbase.16.12.01.SPA.pkg
cat3k_caa-rpcore.16.12.01.SPA.pkg
cat3k_caa-srdriver.16.12.01.SPA.pkg
cat3k_caa-universalk9.16.12.01.SPA.bin
cat3k_caa-guestshell.16.12.01.SPA.pkg
cat3k_caa-webui.16.12.01.SPA.pkg
packages.conf
[3]: Files that will be deleted:
cat3k_caa-rpbase.16.12.01.SPA.pkg
cat3k_caa-rpcore.16.12.01.SPA.pkg
cat3k_caa-srdriver.16.12.01.SPA.pkg
cat3k_caa-universalk9.16.12.01.SPA.bin
cat3k_caa-guestshell.16.12.01.SPA.pkg
cat3k_caa-webui.16.12.01.SPA.pkg
packages.conf
[4]: Files that will be deleted:
cat3k_caa-rpbase.16.12.01.SPA.pkg
cat3k_caa-rpcore.16.12.01.SPA.pkg
cat3k_caa-srdriver.16.12.01.SPA.pkg
cat3k_caa-universalk9.16.12.01.SPA.bin
cat3k_caa-guestshell.16.12.01.SPA.pkg
cat3k_caa-webui.16.12.01.SPA.pkg
```

```
[1 2 3 4]: Do you want to proceed with the deletion? [yes/no]: yes
[1 2 3 4]: Clean up completed
Switch#
```

b) **copy tftp: flash:**

Use this command to copy the image from your TFTP server to flash

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin flash:
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Destination filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin...
Loading cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!
!!!!!!!!!!!!!
[OK - 311154824 bytes]
311154824 bytes copied in 68.781 secs (4523849 bytes/sec)
Switch#
```

c) **software expand**

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

```
Switch# software expand file flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Preparing expand operation ...
[1]: Copying software from active switch 1 to switches 2,3,4
[1]: Finished copying software to switches 2,3,4
[1 2 3 4]: Expanding bundle flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
[1 2 3 4]: Copying package files
[1 2 3 4]: Package files copied
[1 2 3 4]: Finished expanding bundle
flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Switch#
```

Step 5 Edit the boot variable

a) **no boot system**

Use this command to clear the boot variable.

```
Switch(config)# no boot system
```

b) **boot system**

Use this command to edit the boot variable to point to the new image.

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

c) **write memory**

Use this command to save configuration changes.

```
Switch# write memory
```

d) **show boot**

Use this command to confirm that your boot variable is pointing to the new image

```
Switch# show boot
----------------------------
Switch 1
----------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;
```

```
Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes
Switch#
```

Step 6 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash**

Use this command to manually boot flash:packages.conf, to reload the switch. If your switches are configured with auto boot, the stack will automatically boot up with the new image.

```
switch:boot flash:packages.conf
```

c) **show version**

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

```
Switch# show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 03.07.02E RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 24-Jul-19 23:51 by prod_rel_team
```

d) **delete flash:**

After you have successfully installed the image, you no longer need the .bin image. Use this command to delete the file from the flash of each switch if you had copied to flash.

```
Switch# delete flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Delete filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Delete flash:/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin? [confirm]
Switch#
```

Downgrading to Cisco IOS XE 3.x.xE in Install Mode

Follow these instructions to downgrade to older Cisco IOS XE Release 3.x.xE releases in install mode.

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Denali 16.x.x or Cisco IOS XE Everest 16.x.x	Only **request platform software** commands.	Cisco IOS XE Release 3.x.xE

The sample output shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Release 3.7.2E.

Procedure

Step 1 Clean Up

a) **request platform software package clean**

Use this command to clean up old installation files; this ensures that you have sufficient space in the flash drive, to expand a new image. Use the **switch all** option to clean up all switches in your stack.

```
Switch# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-rpbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-guestshell.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.12.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
Running command on switch 2
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-rpbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-guestshell.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.12.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

Running command on switch 3
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-rpbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-guestshell.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-webui.16.12.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
```

```
done.

Running command on switch 4
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat3k_caa-rpbase.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-rpcore.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-srdriver.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-guestshell.16.12.01.SPA.pkg
File is in use, will not delete.
cat3k_caa-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:
[1]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-
[2]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-
[3]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-
[4]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[2]:
```

```
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[4]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
Switch#
```

Step 2 Copy new image to stack

Copy the target Cisco IOS XE 3.x.xE image to flash: (you can skip this step if you want to use the image from your TFTP server).

a) **copy tftp: flash:**

Use this command to copy the image from your tftp server to flash.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin flash:
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Destination filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin...
Loading cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!
!!!!!!!!!!!!!!!
[OK - 311154824 bytes]

311154824 bytes copied in 68.781 secs (4523849 bytes/sec)
Switch#
```

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:/

47718 -rw- 311154824 Jul 24 2019 18:17:21 +00:00
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin

3458338816 bytes total (2468995072 bytes free)
```

```
Switch#
```

Step 3 Downgrade Software Image

a) **request platform software package install**

You can point to the source image on your tftpserver or in flash if you have it copied to flash.

Use this command with the **new** option, to downgrade your stack. Use the **switch all** option to downgrade all the switches in your stack. Use the **auto-copy** option to copy the .bin image from flash: to all other switches in your stack.

```
Switch# request platform software package install switch all file flash:cat3k_caa-
universalk9.SPA.03.07.02.E.152-3.E2.bin new auto-copy

Expanding image file: flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
[4]: Copying flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from switch 4 to
switch 1 2 3
[1 2 3]: Finished copying to switch 1 2 3
[1 2 3 4]: Expanding file
[1 2 3 4]: Finished expanding all-in-one software package in switch 1 2 3 4
SUCCESS: Finished expanding all-in-one software package.
[1 2 3 4]: Performing install
SUCCESS: install Finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-rpbase.16.12.01.SPA.pkg
Removed cat3k_caa-rpcore.16.12.01.SPA.pkg
Removed cat3k_caa-srdriver.16.12.01.SPA.pkg
Removed cat3k_caa-guestshell.16.12.01.SPA.pkg
Removed cat3k_caa-webui.16.12.01.SPA.pkg
New files list:
Added cat3k_caa-base.SPA.03.07.02E.pkg
Added cat3k_caa-drivers.SPA.03.07.02E.pkg
Added cat3k_caa-infra.SPA.03.07.02E.pkg
Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
Added cat3k_caa-platform.SPA.03.07.02E.pkg
Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-rpbase.16.12.01.SPA.pkg
Removed cat3k_caa-rpcore.16.12.01.SPA.pkg
Removed cat3k_caa-srdriver.16.12.01.SPA.pkg
Removed cat3k_caa-guestshell.16.12.01.SPA.pkg
Removed cat3k_caa-webui.16.12.01.SPA.pkg
New files list:
Added cat3k_caa-base.SPA.03.07.02E.pkg
Added cat3k_caa-drivers.SPA.03.07.02E.pkg
Added cat3k_caa-infra.SPA.03.07.02E.pkg
Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
Added cat3k_caa-platform.SPA.03.07.02E.pkg
Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
Old files list:
```

```
Removed cat3k_caa-rpbase.16.12.01.SPA.pkg
Removed cat3k_caa-rpcore.16.12.01.SPA.pkg
Removed cat3k_caa-srdriver.16.12.01.SPA.pkg
Removed cat3k_caa-guestshell.16.12.01.SPA.pkg
Removed cat3k_caa-webui.16.12.01.SPA.pkg
New files list:
Added cat3k_caa-base.SPA.03.07.02E.pkg
Added cat3k_caa-drivers.SPA.03.07.02E.pkg
Added cat3k_caa-infra.SPA.03.07.02E.pkg
Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
Added cat3k_caa-platform.SPA.03.07.02E.pkg
Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[3]: Finished install successful on switch 3
[4]: install package(s) on switch 4
--- Starting list of software package changes ---
Old files list:
Removed cat3k_caa-rpbase.16.12.01.SPA.pkg
Removed cat3k_caa-rpcore.16.12.01.SPA.pkg
Removed cat3k_caa-srdriver.16.12.01.SPA.pkg
Removed cat3k_caa-guestshell.16.12.01.SPA.pkg
Removed cat3k_caa-webui.16.12.01.SPA.pkg
New files list:
Added cat3k_caa-base.SPA.03.07.02E.pkg
Added cat3k_caa-drivers.SPA.03.07.02E.pkg
Added cat3k_caa-infra.SPA.03.07.02E.pkg
Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
Added cat3k_caa-platform.SPA.03.07.02E.pkg
Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[4]: Finished install successful on switch 4
Checking status of install on [1 2 3 4]
[1 2 3 4]: Finished install in switch 1 2 3 4
SUCCESS: Finished install: Success on [1 2 3 4]
```

The old files listed in the logs should be removed using the **software clean** command, after reload.

b) **delete flash:**

After you have successfully installed the image, you no longer need the .bin image. Use this command to delete the file from flash of each switch if you copied it to flash.

```
Switch# delete flash: cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Delete filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Delete flash:/ cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin? [confirm]
Switch#
```

Step 4 Reload

a) **reload**

Use this command in the privileged EXEC mode to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If the switch is configured with auto boot, then the stack automatically boots up with the new image. If not, you can manually boot flash:packages.conf

Note
When you downgrade to a Cisco IOS XE 3.xE image, the boot loader does not automatically downgrade. It remains updated. The new boot loader can support booting both Cisco IOS XE Release 3.x.xE releases as well as Cisco IOS XE Denali 16.x.x, Cisco IOS XE Everest 16.x.x, Cisco IOS XE Fuji 16.x.x, and Cisco IOS XE Gibraltar 16.x.x releases.

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

Upgrading from Cisco IOS XE Gibraltar 16.12.1 in Install Mode

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

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Cisco IOS XE Fuji 16.x.x or Cisco IOS XE Gibraltar 16.12.x	Either **install** commands or **request platform software** commands	A later Cisco IOS XE 16.x.x release

The sample output in this section displays upgrade from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Gibraltar 16.12.1, by using **install** commands. It also provides information about the corresponding **request platform software** command, but not the sample output.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- **install remove inactive**
- **request platform software package clean**

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

```
Switch# install remove inactive
install_remove: START Wed Jul 24 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:

/flash/cat3k_caa-rpbase.16.08.01a.SPA.pkg
/flash/cat3k_caa-rpcore.16.08.01a.SPA.pkg
```

```
/flash/cat3k_caa-srdriver.16.08.01a.SPA.pkg
/flash/cat3k_caa-guestshell.16.08.01a.SPA.pkg
/flash/cat3k_caa-webui.16.08.01a.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat3k_caa-rpbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat3k_caa-rpcore.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat3k_caa-guestshell.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.08.01a.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Wed Jul 24 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat3k_caa-universalk9.16.12.01.SPA.bin flash:
destination filename [cat3k_caa-universalk9.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat3k_caa-universalk9.16.12.01.SPA.bin...
Loading /cat3k_caa-universalk9.16.12.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

b) **dir flash:**

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

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

Directory of flash:/

434184 -rw- 601216545 Jul 24 2019 10:18:11 -07:00 cat3k_caa-universalk9.16.12.01.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

- **install add file activate commit**
- **request platform software package install**

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.12.1 software image to flash, by using the **install add file activate commit** command:

```
Switch# install add file flash:cat3k_caa-universalk9.16.12.01.SPA.bin activate commit

install_add_activate_commit: START Wed Jul 24 19:54:51 UTC 2018

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y
Building configuration...

[OK]Modified configuration has been saved

*Jul 24 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 24 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat3k_caa-universalk9.16.12.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat3k_caa-universalk9.16.12.01.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
Following packages shall be activated:
/flash/cat3k_caa-rpbase.16.12.01.SPA.pkg
/flash/cat3k_caa-rpcore.16.12.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.12.01.SPA.pkg
/flash/cat3k_caa-guestshell.16.12.01.SPA.pkg
/flash/cat3k_caa-webui.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

*Jul 24 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 24 19:57:41 rollback_timer.sh:

%INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200
 seconds [1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Wed Jul 24 19:57:48 UTC 2019
Switch#
```

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

Step 5 **dir flash:**

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

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

```
Switch# dir flash:*.pkg

Directory of flash:/
475140 -rw- 2012104   Jul 24 2019 09:52:41 -07:00 cat3k_caa-rpbase.16.08.01a.SPA.pkg
475141 -rw- 70333380  Jul 24 2019 09:52:44 -07:00 cat3k_caa-rpcore.16.08.01a.SPA.pkg
475142 -rw- 13256     Jul 24 2019 09:52:44 -07:00 cat3k_caa-srdriver.16.08.01a.SPA.pkg
475143 -rw- 349635524 Jul 24 2019 09:52:54 -07:00 cat3k_caa-guestshell.16.08.01a.SPA.pkg
475149 -rw- 24248187  Jul 24 2019 09:53:02 -07:00 cat3k_caa-webui.16.08.01a.SPA.pkg

491524 -rw- 25711568  Jul 24 2019 11:49:33 -07:00 cat3k_caa-rpbase.16.12.01.SPA.pkg
491525 -rw- 78484428  Jul 24 2019 11:49:35 -07:00 cat3k_caa-rpcore.16.12.01.SPA.pkg
491526 -rw- 1598412   Jul 24 2019 11:49:35 -07:00 cat3k_caa-srdriver.16.12.01.SPA.pkg
491527 -rw- 404153288 Jul 24 2019 11:49:47 -07:00 cat3k_caa-guestshell.16.12.01.SPA.pkg
491533 -rw- 31657374  Jul 24 2019 11:50:09 -07:00 cat3k_caa-webui.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
- `cat3k_caa-universalk9.16.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

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

```
Directory of flash:/*.conf
Directory of flash:/
72882  -rw-        4779  Jul 24 2019 15:29:03 +00:00  packages.conf
72883  -rw-       4779  Jul 24 2019 15:26:21 +00:00  cat3k_caa-universalk9.16.12.01.SPA.conf

11353194496 bytes total (8963174400 bytes free)
```

Step 6 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

Downgrading from Cisco IOS XE Gibraltar 16.12.1 in Install Mode

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

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Fuji 16.x.x or Cisco IOS XE Gibraltar 16.12.x	Either **install** commands or **request platform software** commands	An earlier Cisco IOS XE 16.x.x release

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Fuji 16.9.2, by using **install** commands. It also provides information about the corresponding **request platform software** command, but not the sample output.



Important New switch models that are introduced in a release cannot be downgraded. The release in which a switch model is introduced is the minimum software version for that model. If you add a new switch model to an existing stack, we recommend upgrading all existing switches to the latest release.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- **install remove inactive**
- **request platform software package clean**

The following sample output displays the cleaning up of Cisco IOS XE Gibraltar 16.12.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Wed Jul 24 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat3k_caa-rpbase.16.12.01.SPA.pkg
/flash/cat3k_caa-rpcore.16.12.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.12.01.SPA.pkg
/flash/cat3k_caa-guestshell.16.12.01.SPA.pkg
/flash/cat3k_caa-webui.16.12.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat3k_caa-rpbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-rpcore.16.12.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-guestshell.16.12.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.12.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.

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

```
SUCCESS: install_remove Wed Jul 24 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat3k_caa-universalk9.16.09.02.SPA.bin flash:
Destination filename [cat3k_caa-universalk9.16.09.02.SPA.bin]?
Accessing tftp://10.8.0.6//cat3k_caa-universalk9.16.09.02.SPA.bin...
Loading /cat3k_caa-universalk9.16.09.02.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 Jul 24 2019 13:35:16 -07:00 cat3k_caa-universalk9.16.09.02.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

- **install add file activate commit**
- **request platform software package install**

The following example displays the installation of the Cisco IOS XE Fuji 16.9.2 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat3k_caa-universalk9.16.09.02.SPA.bin activate commit

install_add_activate_commit: START Wed Jul 24 19:54:51 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]yBuilding
 configuration...

[OK]Modified configuration has been saved

*Jul 24 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 24 19:54:55 install_engine.sh:
 %INSTALL-
5-INSTALL_START_INFO: Started install one-shot flash:cat3k_caa-universalk9.16.09.02.SPA.bin
 install_add_activate_commit: Adding PACKAGE

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

--- Starting initial file syncing ---
Info: Finished copying flash:cat3k_caa-universalk9.16.09.02.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
Following packages shall be activated:
/flash/cat3k_caa-rpbase.16.09.02.SPA.pkg
/flash/cat3k_caa-rpcore.16.09.02.SPA.pkg
/flash/cat3k_caa-srdriver.16.09.02.SPA.pkg
/flash/cat3k_caa-guestshell.16.09.02.SPA.pkg
/flash/cat3k_caa-webui.16.09.02.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

*Jul 24 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 24 19:57:41 rollback_timer.sh:
 %INSTALL-
5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200 seconds
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Wed Jul 24 19:57:48 UTC 2019
Switch#
```

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

Step 4 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

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

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

Note
When you downgrade the software image, the boot loader will not automatically downgrade. It will remain updated.

c) **show version**

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

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

The following sample output of the **show version** command displays the Cisco IOS XE Fuji 16.9.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.09.02
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version
 16.9.2, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
<output truncated>
```

Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 3850 Series Switches.

License Levels

The software features available on Cisco Catalyst 3850 Series Switches fall under these base or add-on license levels.

Base Licenses

- LAN Base—Provides basic Layer 2+ features, including access control lists (ACLs) and quality of service (QoS), up to 255 VLANs, support for routing protocols (Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Policy-Based Routing (PBR), Protocol Independent Multicast Stub Routing (PIM Stub Routing) with IPv4 and IPv6, and routed access with IPv4 and IPv6 (OSPF — up to 1000 routes, Multicast — up to 1000 routes).
- IP Base—Provides Layer 2+ and basic Layer 3 features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, Enhanced Interior Gateway Routing Protocol (EIGRP) stub routing, IP multicast routing, RIP, basic IPv6 management, the OSPF Protocol (for routed access only). The license supports up to 4094 VLANs.
- IP Services—Provides a richer set of enterprise-class intelligent services and full IPv6 support. It includes all IP Base features plus full Layer 3 routing (IP unicast routing and IP multicast routing). The IP Services feature set includes protocols such as the EIGRP, OSPF Protocol. The license supports up to 4094 VLANs.

Add-On Licenses

The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Advantage

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

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

- A permanent license can be moved from one device to another.
- A switch stack cannot contain mixed license levels. Also, the switches must be of the same platform.
- 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.

Cisco Smart Licensing

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

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

To use Smart Licensing, you must first set up a Smart Account on Cisco License Central. For a more detailed overview on Cisco Licensing, visit the Licensing Hub.



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

Deploying Smart Licensing

Procedure

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

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.

What to do next

Register and convert traditional licenses to Smart Licenses

Converting Traditional Licenses to Smart Licenses

For Cisco Catalyst 3850 Series Switches, after you have upgraded the software image and deployed Smart Licensing, all traditional licenses on the device must be migrated, to Cisco Smart Software Manager. This is a one-time migration process that you must complete on each device.

Procedure

Step 1 Register the device

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 a Device in CSSM*.

Step 2 Migrate base licenses

The system converts traditional licenses to smart licenses and sends migration data to Cisco Smart Software Manager, which in turn Cisco Smart Software Manager creates license entitlements and deposits them in your user account. In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Migrating a License with License Conversion*..

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.

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 and then converted. After conversion, they are made available in your Smart Account.

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

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

Scaling Guidelines

System Feature	Maximum Limit
Number of HTTP session redirections system-wide	Up to 100 clients per second
Number of HTTPS session redirections system-wide	Up to 20 clients per second

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.
  - Cisco TrustSec cannot be configured on a pure bridging domain with the IPSG feature enabled. You must either enable IP routing or disable the IPSG feature in the bridging domain.
  - Dynamic SGACL download is limited to 6KB per destination group tag (DGT)
- DHCP Client—Starting with Cisco IOS XE Denali 16.1.x, a DHCP client that includes option 61 (used by DHCP clients to specify their unique client identifier) in their DHCP discover/offer packet must accept

the response message with option 61 from the DHCP server/relay. A client that fails to accept the response message with option 61, is not in compliance with RFC 6842 and requires a firmware upgrade.

- Centralized Management Mode (CMM)—Starting with Cisco IOS XE Denali 16.3.1, CMM is not supported.
- Flexible NetFlow—You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
- Flex Links are not supported. We recommend that you use spanning tree protocol (STP) as the alternative.
- In-Service Software Upgrade (ISSU)
  - 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.
  - ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x is not supported in the FIPs mode of operation.
  - While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
  - If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
  - If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.
  - When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

    Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.
- Stack ports buffer is not shared as part of the shared pool. The dedicated buffer for stack ports can only be used by stack ports.
- 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.

- UPoE connections—On the WS-C3850-12X48U-L, WS-C3850-12X48U-S and WS-C3850-12X48U-E switch models, a maximum of 28 ports are available for UPoE connections.
- 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.
- Secure Password Migration—Autoconversion to password type 6 is supported from Cisco IOS XE Gibraltar 16.12.1 and later releases.

  If the startup configuration has a type 6 password and you downgrade to a version in which type 6 password is not supported, you can/may be locked out of the device.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Caveats

Caveats describe unexpected behavior in Cisco IOS-XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE Gibraltar 16.12.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.14

Identifier	Headline
CSCwk56468	Vulnerability in BSAFE Crypto-C Affecting Cisco IOS and Cisco IOS XE Software
CSCwm41327	Cisco IOS XE Software CLI Argument Injection Vulnerability
CSCwm57073	Cisco IOS XE Software WebUI Reflected Cross-Site Scripting Vulnerability

Identifier	Headline
CSCwm99306	Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability
CSCwn46756	Cisco IOS XE Software Network-Based Application Recognition Denial of Service Vulnerability
CSCwo35704	Cisco IOS Software and IOS XE Software HTTP Server Remote Code Execution Vulnerability
CSCwo35779	Cisco IOS XE Software HTTP Server Remote Code Execution Vulnerability
CSCwo49948	Cisco IOS, IOS XE Software IKEv2 Denial of Service Vulnerability
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.13

Identifier	Headline
CSCwi33204	Cisco IOS XE Software Model-Driven Programmability Authorization Bypass Vulnerability
CSCwk23580	Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature
CSCwk40885	Cisco IOS Software and IOS XE Software IKEv2 Denial of Service Vulnerability
CSCwk80897	Cisco IOS, IOS XE, and IOS XR Software TWAMP Denial of Service Vulnerability
CSCwm35433	Cisco IOS XE Wireless Controller Software Unauthorized User Deletion Vulnerability
CSCwm59330	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwm64309	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwm66565	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwm68661	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwm72787	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwm79554	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79564	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79570	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79577	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79581	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79590	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79596	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities

Identifier	Headline
CSCwm89600	Cisco IOS, IOS XE, and IOS XR SNMP Denial of Service Vulnerabilities

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.12

Identifier	Headline
CSCwj05481	Cisco IOS and IOS XE Software Resource Reservation Protocol Denial of Service Vulnerabilit
CSCwi59624	Cisco IOS and IOS XE Software Web UI Cross-Site Request Forgery Vulnerability
CSCwh81471	Cisco IOS XE Software for Wireless Controllers CWA Pre-Auth ACL Bypass Vulnerability
CSCwk36431	Cisco IOS XE Software SD-Access Fabric Edge Node Denial of Service Vulnerability
CSCwe24431	Cisco IOS and IOS XE Software SNMP Extended Named Access Control List Bypass Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.11

Identifier	Description
CSCwi05260	C3650-12X48UQ | PSUs may show bad/disabled status randomly which can affect PoE
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerability
CSCwh41093	Cisco IOS XE Software SD-Access Fabric Edge Node Denial of Service Vulnerability
CSCwc68836	CISCO-CONFIG-COPY-MIB: Files not copied to stby-nvram
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability
CSCwe70596	Cisco IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.10a

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

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.10

Identifier	Description
CSCwa64171	Inactive flows do not age and remain stale in the flow table after 1yr+ system uptime.

Identifier	Description
CSCwe60256	Cisco IOS XE Software for Catalyst 3650 & 3850 Switches Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.9

Identifier	Description
CSCwd93978	WS-C3850-48XS-E Can't configure SVL with 40G port

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.8

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

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.7

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

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

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5b

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

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

Identifier	Description
CSCvv18875	MKA MACSEC don't support GCM-AES-256 after upgrading to 16.12.3a
CSCvv28324	CAT3K intermittently not responding to SNMP
CSCvv47869	FAN OID value "EnvMonFanStatusEntry" can't be obtained
CSCvv50628	Cat3850 : PoE doesn't work - Power given, but State Machine Power Good wait timer timed out
CSCvw07961	SNMP: After OIR of PSU, PSU entities are missing from cefcFRUPowerStatusTable
CSCvw63161	ZTP failing with error in creating downloaded_script.py

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.4

Identifier	Description
CSCvr71393	C3850 24 of 48 ports stop working after upgrade
CSCvr82708	Device crash when upgrading via ISSU
CSCvs15819	No Log on the switch when removing power cable.
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs73383	"show mac address-table" does not show remote EIDs when vlan filter used
CSCvs77781	Critical auth failing to apply DEFAULT_CRITICAL_DATA_TEMPLATE
CSCvt13518	QoS ACL matching incorrectly when udp range is used
CSCvt70277	Power allocation issue in 16.9.x/16.12.x
CSCvt72427	Cat3k/9k Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan
CSCvt98435	16.12.3 not creating system-reports on crashes
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
CSCvp64464	CRC error incrementing with GLC-TE SFPs with speed 10
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvp85601	STP TCN is generated on etherchannel port during a switchover in a stack
CSCvq17759	DACL not properly enforced when pre auth acl present for some phone
CSCvq25360	PD's not getting PoE on multiple interfaces in 3850 stack
CSCvq53573	Cat3k take 1~2 hours to boot.
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr23358	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr41906	Imax error on adjacent interfaces in port-group
CSCvr59959	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr88090	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction
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
CSCvs01830	DHCP snooping causing mac flaps when connecting IE-3200
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.

Identifier	Description
CSCvs31472	Cat3k: MCU is generating fault events, causing PDs to be reported off after reload in case of PPoE
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 16.12.1

Identifier	Description
CSCvj16691	port LED may turn to amber
CSCvm89086	cat 9300 | span destination interface not dropping ingress traffic
CSCvn04524	IP Source Guard blocks traffic after host IP renewal
CSCvn30230	Catalyst 3k/9k: Slow memory leak in linux_iosd-imag
CSCvn31653	Missing/incorrect FED entries for IGMP Snooping on Cat9300/Cat3850/Cat3650
CSCvn66396	MACSEC Portchannel member interface stays permanently down after link flap
CSCvn77683	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvn81334	Default ACL being enforced even dACL is applied after Reload
CSCvn98703	FED_QOS_ERRMSG-3-POLICER_HW_ERROR on Catalysts 3650/3850 running 16.6 releases
CSCvo15594	Hardware MAC address programming issue for remote client catalyst 9300
CSCvo17778	Cat9k not updating checksum after DSCP change

Identifier	Description
CSCvo24073	multiple CTS sessions stuck in HELD/SAP_NE
CSCvo27371	Memory leak in MACSec seen during SAP scale longevity
CSCvo32446	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo33983	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo34804	3850 stack SFP cannot be recognized on some port and the port link also do not up
CSCvo56629	Cat9500 - Interface in Admin shutdown showing incoming traffic and interface Status led in green.
CSCvo57768	NetFlow issue 3850 switch not sending TCP flags
CSCvo59504	Cat3K | Cat9K - SVI becomes inaccesible upon reboot
CSCvo65974	QinQ tunnels causing L2 loop in specific topology of Cat3850
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 3850 Series Switches is at this URL: https://www.cisco.com/go/cat3850_docs

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

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

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

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

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

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

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2025 Cisco Systems, Inc. All rights reserved.