Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2022-09-22

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Gibraltar 16.12.x

Introduction

Cisco Catalyst 9300 Series Switches are Cisco's lead stackable access platforms for the next-generation enterprise and have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

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

Whats New in Cisco IOS XE Gibraltar 16.12.8

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

Whats New in Cisco IOS XE Gibraltar 16.12.7

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

Whats New in Cisco IOS XE Gibraltar 16.12.6

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

Whats New in Cisco IOS XE Gibraltar 16.12.5b

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

Whats New in Cisco IOS XE Gibraltar 16.12.5

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

Whats New in Cisco IOS XE Gibraltar 16.12.4

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

Whats New in Cisco IOS XE Gibraltar 16.12.3a

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

Whats New in Cisco IOS XE Gibraltar 16.12.3

Software Features in Cisco IOS XE Gibraltar 16.12.3

Feature Name	Description
Forwarding Scale Enhancements	The forwarding scale numbers for the following features have changed: • Layer 2 Unicast MAC Addresses: 49152 • Layer 3 Multicast: 32768 • QoS Access Control Entries: 6144 • Policy Based Routing ACEs / NAT ACEs: 14336 Supported switch models—C9300-24UB, C9300-24UXB, and C9300-48UB

Whats New in Cisco IOS XE Gibraltar 16.12.2

Hardware Features in Cisco IOS XE Gibraltar 16.12.2

Feature Name	Description and Documentation Link
Cisco Catalyst 9300 Series Switches (C9300L)	The following new models have been introduced in the series: • C9300L-48PF-4G: Stackable 48 10/100/1000 Mbps PoE+ ports; 4x1G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320. • C9300L-48PF-4X: Stackable 48 10/100/1000 Mbps PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320. For information about the hardware including installation and technical specifications, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide. For information about the software, see the Software Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9300 Switches).
Cisco Catalyst 9300 Series Switches, MultiGigabit Ethernet (C9300L)	The following new MultiGigabit Ethernet models have been introduced in the series: • C9300L-24UXG-4X: Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 880 W with 1100 WAC power supply; supports StackWise-320. • C9300L-24UXG-2Q: Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 722 W with 1100 WAC power supply; supports StackWise-320. • C9300L-48UXG-4X: Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320. • C9300L-48UXG-2Q: Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320. For information about the hardware including installation and technical specifications, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide. For information about the software, see the Software Configuration Guide, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9300 Switches).

Whats New in Cisco IOS XE Gibraltar 16.12.1

Hardware Features in Cisco IOS XE Gibraltar 16.12.1

Feature Name	Description and Documentation Link
Cisco Catalyst 9300 Series Switches (C9300-24UB, C9300-24UXB, C9300-48UB)	These new UPOE stackable switch models are introduced: • C9300-24UB— 24 10/100/1000 Mbps UPOE ports • C9300-24UXB— 24 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports • C9300-48UB— 48 10/100/1000 Mbps UPOE ports
Direct-Attach Copper Cable	• Supported cable product number: QSFP-H40G-CU0-5M • Compatible switch model numbers: All C9300 SKUs For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Gibraltar 16.12.1

Feature Name	Description, Documentation Link, and License Level Information
Autoconf Device Granularity to PID of Cisco Switch	Introduces the **platform type** filter option for class map and parameter map configurations. Use the **map platform-type** command in parameter map filter configuration mode, to set the parameter map attribute and the **match platform-type** command in control class-map filter configuration mode, to evaluate control classes. See Network Management → Configuring Autoconf. (Network Essentials and Network Advantage)
Border Gateway Protocol (BGP) Ethernet VPN (EVPN) Route Target (RT) Autonomous System Number (ASN) Rewrite	Introduces support for the **rewrite-evpn-rt-asn** command in address-family configuration mode. This command enables the rewrite of the ASN portion of the EVPN route target that originates from the current autonomous system, with the ASN of the target eBGP EVPN peer. See IP Routing Commands → rewrite-evpn-rt-asn. (Network Advantage)
Bidirectional Protocol Independent Multicast (PIM)	Introduces support for bidirectional PIM. This feature is an extension of the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-sparse mode, bidirectional PIM avoids keeping source-specific state in a router and allows trees to scale to an arbitrary number of sources. See IP Multicast Routing → Configuring Protocol Independent Multicast (PIM). (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Bluetooth Dongle	Introduces support for external USB Bluetooth dongles. The connected dongle acts as a Bluetooth host and serves as a management port connection on the device. See Interface and Hardware Components → Configuring an External USB Bluetooth Dongle. (Network Essentials)
Energy Efficient Ethernet (EEE) support on Multigigabit (mGig) Ethernet ports	EEE is now supported on switches with mGig ports. See Interface and Hardware Components → Configuring EEE. (Network Essentials and Network Advantage)
Ethernet over MPLS (EoMPLS) Xconnect on Subinterfaces	Transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN through a single virtual circuit over an Multiprotocol Label Switching (MPLS) network. See Multiprotocol Label Switching → Configuring Ethernet-over-MPLS and Pseudowire Redundancy. (Network Advantage)
Flexlink+	Configures a pair of Layer 2 interfaces - one interface is configured to act as a backup for the other interface. See Layer 2 → Configuring Flexlink+. (Network Essentials and Network Advantage)
High Availability support for MACsec Key Agreement (MKA)	Support for high availability for MKA sessions is introduced. MKA sessions are now SSO-aware. In the event of failure of the active switch, the standby switch takes over the existing MKA sessions in a minimally disruptive switchover. See Security → MACsec Encryption. (Network Advantage)
IEEE 1588v2, Precision Time Protocol (PTP) support	Introduces PTP support on native Layer 3 ports. See Layer 2 → Configuring Precision Time Protocol (PTP). (Network Advantage)
IPv4 and IPv6: Object Groups for access control lists (ACLs)	Enables you to classify users, devices, or protocols into groups and apply them to ACLs, to create access control policies for these groups. With this feature, you use object groups instead of individual IP addresses, protocols, and ports, which are used in conventional ACLs. It allows multiple access control entries (ACEs), and you can use each ACE to allow or deny an entire group of users the access to a group of servers or services. See Security → Object Groups for ACLs. (Network Essentials and Network Advantage)

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

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

Feature Name	Description, Documentation Link, and License Level Information
IPv6: PBR Recursive Next-Hop	IPv6 support is introduced for PBR Recursive Next-Hop option. (Network Advantage and Network Essentials)
IPv6-based Posture Validation	IPv6 support is introduced for Posture Validation. (Network Advantage and Network Essentials)
IPv6: Proxy Mobile	IPv6 support is introduced for PMIPv6 Hybrid Access.
IPv6: Open Shortest Path First (OSPF)	IPv6 support is introduced for the following OSPF features: • IPv6: NSF - OSPF • IPv6: OSPF Flooding Reduction • IPv6: OSPF Link State Database Overload Protection • IPv6: OSPF On Demand Circuit (RFC 1793) • IPv6: OSPF Packet Pacing • IPv6: OSPF Support for Multi-VRF on CE Routers • IPv6: OSPFv3 NSR • IPv6: OSPFv3 Retransmission Limits • IPv6: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec • IPv6: OSPFv3 Graceful Restart • IPv6: VRF aware OSPFv3, EIGRPv6, BGPv6 • IPv6: OSPFv3 Fast Convergence - LSA and SPF throttling (Network Advantage and Network Essentials)
IPv6: Services	IPv6 support is introduced for AAAA DNS Lookups over an IPv6 Transport. (Network Advantage and Network Essentials)
IPv6: Time-Based Access Lists Using Time Ranges	IPv6 support is introduced for Time-Based Access Lists using time ranges. (Network Advantage and Network Essentials)
IPv6: Triggered RIP	IPv6 support is introduced for Triggered Extensions to RIP.
Layer 3 Subinterface	Layer 3 interfaces forward IPv4 and IPv6 packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter-VLAN routing of Layer 2 traffic. See VLAN → Configuring Layer 3 Subinterfaces. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
MPLS VPN-Inter-AS Option B	Allows an MPLS Virtual Private Network (VPN) service provider to interconnect different autonomous systems to provide VPN services. In an Inter-AS Option B network, autonomous system boundary router (ASBR) peers are connected by one or more interfaces that are enabled to receive MPLS traffic. See Multiprotocol Label Switching → Configuring MPLS InterAS Option B.
MPLS Layer 2 VPN over GRE	Provides a mechanism for tunneling Layer 2 MPLS packets over a non-MPLS network. See Multiprotocol Label Switching → Configuring MPLS Layer 2 VPN over GRE. (Network Advantage)
MPLS Subinterface Support	MPLS is now supported on Layer 3 subinterfaces. See VLAN → Configuring Layer 3 Subinterfaces. (Network Advantage)
MPLS Layer 3 VPN over Generic Routing Encapsulation (GRE)	Provides a mechanism for tunneling Layer 3 MPLS packets over a non-MPLS network. See Multiprotocol Label Switching → Configuring MPLS Layer 3 VPN over GRE. (Network Advantage)
Network Address Translation (NAT) license level change	The NAT feature is now available with the Network Advantage license. See IP Addressing Services → Configuring Network Address Translation. (Network Advantage)
Port Channel with Subinterface	Subinterfaces can now be created on Layer 3 port channels. See VLAN → Configuring Layer 3 Subinterfaces. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • Guest Shell and App Hosting: Front-Panel USB Port Access • Guest Shell and App Hosting: Front-Panel Network Port Access • IoX Support of Docker • Model-Driven Telemetry gNMI Dial-In • NETCONF-YANG SSH Server Support • OpenFlow Power over Ethernet • YANG Data Models	The following programmability features are introduced in this release: • Guest Shell and App Hosting: Front-Panel USB Port Access—Datapath connectivity between IOS XE Guest Shell, App Hosting container, and front-panel USB ports. • Guest Shell and App Hosting: Front-Panel Network Port Access—Datapath connectivity between IOS XE Guest Shell, App Hosting container, and front-panel network ports. **Note** Enables ZTP functionalty on the front-panel network port. • IOx Support of Docker—Introduces an IOx Kernel Virtual Machine (KVM)-based application. This application runs a Docker daemon within the customer-created IOx KVM guest operating system. • Model-Driven Telemetry gNMI Dial-In—Support for telemetry subscriptions and updates over a gRPC Network Management Interface (gNMI). • NETCONF-YANG SSH Server Support—NETCONF-YANG supporting the use of IOS Secure Shell (SSH) public keys (RSA) to authenticate users as an alternative to password-based authentication. • OpenFlow Power over Ethernet—Power over Ethernet (PoE) support on OpenFlow ports. • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121/BIC. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)
Seamless MPLS	Integrates multiple networks into a single MPLS domain. It removes the need for service-specific configurations in network transport nodes. See Multiprotocol Label Switching → Configuring Seamless MPLS. (Network Advantage)
Simplified Factory Reset for Removable Storage	Performing a factory reset now also erases the contents of removable storage devices such as Serial Advanced Technology Attachment (SATA), Solid State Drive (SSD), and USB. See System Management → Performing Factory Reset. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Source Group Tag (SGT), Destination Group Tag (DGT) over FNF for IPv6 traffic	Introduces support for SGT and DGT fields over FNF, for IPv6 traffic. See Network Management → Configuring Flexible NetFlow. (Network Advantage)
Stack troubleshooting optimization	The output of the **show tech-support stack** command has been enhanced to include more stack-related information. See Stack Manager and High Availability Commands → show tech-support stack. (A license level does not apply)
Support for 802.3bt Type 3 Standard	UPOE switches in the series (C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-48UN) now support the IEEE 802.3bt Type 3 standard. You can enable the 802.3bt mode, by entering the **hw-module switch upoe-plus** command in global configuraton mode. In the 802.3bt mode, the switch functions as a 802.3bt Type 3 switch, supporting up to Class 6 powered devices on every port. The device is power-cycled automatically after you enter the **hw-module switch upoe-plus** command in order to apply the mode change. Data stack and stack-power will get disrupted. See Interface and Hardware Components → Configuring PoE. (Network Essentials and Network Advantage)
VPN Routing and Forwarding-aware Policy Based Routing (VRF-aware PBR)	The PBR feature is now VRF-aware and can be configured on VRF lite interfaces. You can enable policy based routing of packets for a VRF instance. See IP Routing → Configuring VRF aware PBR. (Network Advantage)

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

Important Notes

• Unsupported Features
• Complete List of Supported Features
• Accessing Hidden Commands

- Microcode Backward Compatibility When Downgrading, on page 13
- Default Behaviour, on page 13

Unsupported Features

- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- IPsec VPN
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

Complete List of Supported Features

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

Accessing Hidden Commands

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

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface → Understanding the Help System* chapter of the Command Reference document.

Hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

Further, the following applies to hidden commands under Category 1 and 2:

- The commands have CLI help. Entering enter a question mark (?) at the system prompt displays the list of available commands.

  Note: For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

- The system generates a %PARSER-5-HIDDEN syslog message when the command is used. For example:

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
 is a hidden command.
Use of this command is not recommended/supported and will be removed in future.
```

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.

Important We recommend that you use any hidden command only under TAC supervision.

If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

Microcode Backward Compatibility When Downgrading

Starting from Cisco IOS XE Gibraltar 16.12.1, a new microcode is introduced to support IEEE 802.3bt Type 3 standard for UPOE switches in the series (C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-48UN). The new microcode is not backward-compatible with the following releases:

- Cisco IOS XE Everest 16.6.1 through Cisco IOS XE Everest 16.6.6
- Cisco IOS XE Fuji 16.9.1 through Cisco IOS XE Fuji 16.9.2

If microcode downgrade does not occur, PoE features will be impacted after downgrading. See Downgrading in Install Mode, on page 38 for more information.

Note The microcode downgrades and the system reboots when a downgrade happens from Cisco IOS XE Gibraltar 16.12.1 to any of the following releases:

- Cisco IOS XE Everest 16.6.1 through Cisco IOS XE Everest 16.6.6
- Cisco IOS XE Fuji through Cisco IOS XE Fuji 16.9.2

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 9300 Series Switches—Model Numbers

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

Table 1: Cisco Catalyst 9300 Series Switches

Switch Model	Default License Level	Description
C9300-24P-A	Network Advantage	Stackable 24 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower
C9300-24P-E	Network Essentials	
C9300-24S-A	Network Advantage	Stackable 24 1G SFP ports; two power supply slots with 715 WAC power supply installed by default; supports StackWise-480 and StackPower.
C9300-24S-E	Network Essentials	
C9300-24T-A	Network Advantage	Stackable 24 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-24T-E	Network Essentials	
C9300-24U-A	Network Advantage	Stackable 24 10/100/1000 UPoE ports; PoE budget of 830W; 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24U-E	Network Essentials	
C9300-24UB-A	Network Advantage	Stackable 24 10/100/1000 Mbps UPOE ports that provide deep buffers and higher scale; PoE budget of 830W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UB-E	Network Essentials	
C9300-24UX-A	Network Advantage	Stackable 24 Multigigabit Ethernet 100/1000/2500/5000/10000 UPoE ports; PoE budget of 490 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UX-E	Network Essentials	
C9300-24UXB-A	Network Advantage	Stackable 24 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports that provide deep buffers and higher scale; PoE budget of 560 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-24UXB-E	Network Essentials	
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-48T-E	Network Essentials	

Switch Model	Default License Level	Description
C9300-48P-A	Network Advantage	Stackable 48 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower
C9300-48P-E	Network Essentials	
C9300-48S-A	Network Advantage	Stackable 48 1G SFP ports; two power supply slots with 715 WAC power supply installed by default; supports StackWise-480 and StackPower.
C9300-48S-E	Network Essentials	
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower
C9300-48T-E	Network Essentials	
C9300-48U-A	Network Advantage	Stackable 48 10/100/1000 UPoE ports; PoE budget of 822 W; 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48U-E	Network Essentials	
C9300-48UB-A	Network Advantage	Stackable 48 10/100/1000 Mbps UPOE ports that provide deep buffers and higher scale; PoE budget of 822 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48UB-E	Network Essentials	
C9300-48UN-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5 Gbps) UPoE ports; PoE budget of 610 W with 1100 WAC power supply; supports StackWise-480 and StackPower
C9300-48UN-E	Network Essentials	
C9300-48UXM-A	Network Advantage	Stackable 48 (36 2.5G Multigigabit Ethernet and 12 10G Multigigabit Ethernet Universal Power Over Ethernet (UPOE) ports)
C9300-48UXM-E	Network Essentials	

Table 2: Cisco Catalyst 9300L Series Switches

Switch Model	Default License Level	Description
C9300L-24T-4G-A	Network Advantage	Stackable 24x10/100/1000M Ethernet ports; 4x1G SFP fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-24T-4G-E	Network Essentials	
C9300L-24P-4G-A	Network Advantage	Stackable 24x10/100/1000M PoE+ ports; 4x1G SFP fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-24P-4G-E	Network Essentials	
C9300L-24T-4X-A	Network Advantage	Stackable 24x10/100/1000M Ethernet ports; 4x10G SFP+ fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-24T-4X-E	Network Essentials	
C9300L-24P-4X-A	Network Advantage	Stackable 24x10/100/1000M PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-24P-4X-E	Network Essentials	
C9300L-48T-4G-A	Network Advantage	Stackable 48x10/100/1000M Ethernet ports; 4x1G SFP fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-48T-4G-E	Network Essentials	
C9300L-48P-4G-A	Network Advantage	Stackable 48x10/100/1000M PoE+ ports; 4x1G SFP fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-48P-4G-E	Network Essentials	
C9300L-48T-4X-A	Network Advantage	Stackable 48x10/100/1000M Ethernet ports; 4x10G SFP+ fixed uplink ports; 350 WAC power supply; supports StackWise-320.
C9300L-48T-4X-E	Network Essentials	
C9300L-48P-4X-A	Network Advantage	Stackable 48x10/100/1000M PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.
C9300L-48P-4X-E	Network Essentials	

Switch Model	Default License Level	Description
C9300L-48PF-4G-A	Network Advantage	Stackable 48 10/100/1000 Mbps PoE+ ports; 4x1G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48PF-4G-E	Network Essentials	
C9300L-48PF-4X-A	Network Advantage	Stackable 48 10/100/1000 Mbps PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48PF-4X-E	Network Essentials	
C9300L-24UXG-4X-A	Network Advantage	Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 880 W with 1100 WAC power supply; supports StackWise-320.
C9300L-24UXG-4X-E	Network Essentials	
C9300L-24UXG-2Q-A	Network Advantage	Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 722 W with 1100 WAC power supply; supports StackWise-320.
C9300L-24UXG-2Q-E	Network Essentials	
C9300L-48UXG-4X-A	Network Advantage	Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48UXG-4X-E	Network Essentials	
C9300L-48UXG-2Q-A	Network Advantage	Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320.
C9300L-48UXG-2Q-E	Network Essentials	

Network Modules

The following table lists the optional uplink network modules with 1-Gigabit, 10-Gigabit, 25-Gigabit, and 40-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 [1]	Four 1 Gigabit Ethernet SFP module slots
C3850-NM-2-10G [1]	Two 10 Gigabit Ethernet SFP module slots

Network Module	Description
C3850-NM-4-10G [1]	Four 10 Gigabit Ethernet SFP module slots
C3850-NM-8-10G [1]	Eight 10 Gigabit Ethernet SFP module slots
C3850-NM-2-40G [1]	Two 40 Gigabit Ethernet SFP module slots
C9300-NM-4G [2]	Four 1 Gigabit Ethernet SFP module slots
C9300-NM-4M [2]	Four MultiGigabit Ethernet slots
C9300-NM-8X [2]	Eight 10 Gigabit Ethernet SFP+ module slots
C9300-NM-2Q [2]	Two 40 Gigabit Ethernet QSFP+ module slots
C9300-NM-2Y [2]	Two 25 Gigabit Ethernet SFP28 module slots

Note

1. These network modules are supported only on the C3850 and C9300 SKUs of the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 9300 Series Switches respectively.
2. These network modules are supported only on the C9300 SKUs of the Cisco Catalyst 9300 Series Switches.

The following table lists the network modules that are supported on the Cisco Catalyst 9300X-HXN Series Switches and the ports that are usable on each of these network module:

Table 3: Network Modules Supported on Catalyst 9300X-HXN Series Switches

Network Module	Cisco IOS XE Cupertino 17.7.1 and Previous Releases	Cisco IOS XE Cupertino 17.8.1 and Later Releases
C9300X-NM-8Y (8x25G)	Ports 1 to 4 usable.	Ports 1 to 6 usable. Ports 7 and 8 are permanently disabled.
C9300X-NM-8M (8xmGig)	Ports 1 to 4 usable.	Ports 1 to 6 usable. Ports 7 and 8 are permanently disabled.
C9300X-NM-2C (2x100G/2x40G)	Ports 1 to 2 usable. No breakout cable support.	Ports 1 and 2 usable. Breakout cable supported only on port 1. No support for breakout cable on port 2.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables

at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9300 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.8	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.7	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.6	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5b	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5	2.6	-	C9300: PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack C9300L: - See Cisco Prime Infrastructure 3.9 → Downloads.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.4	2.6	-	C9300: PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack C9300L: - See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.2	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	-	C9300: PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack C9300L: - See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4 → **Downloads**.
Gibraltar 16.10.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.8	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.7	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → **Downloads**.
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.2	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack See Cisco Prime Infrastructure 3.3→ **Downloads**.

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.5.1a	2.1 Patch 3	5.4 5.5	-

Web UI System Requirements

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

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1280 x 800 or higher	Small

[1] We recommend 1 GHz
[2] 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 16.12.8	CAT9K_IOSXE	cat9k_iosxe.16.12.08.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.08.
Cisco IOS XE Gibraltar 16.12.7	CAT9K_IOSXE	cat9k_iosxe.16.12.07.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.07.
Cisco IOS XE Gibraltar 16.12.6	CAT9K_IOSXE	cat9k_iosxe.16.12.06.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.06.

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

Automatic Boot Loader Upgrade

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

For subsequent Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x releases, if there is a new bootloader in that 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.

<table>
<tr><th>Scenario</th><th>Automatic Boot Loader Response</th></tr>
<tr><td>If you boot Cisco IOS XE Gibraltar 16.12.2 or 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 or Cisco IOS XE Gibraltar 16.12.7 or Gibraltar 16.12.8 the first time</td><td>On the C9300 models, the boot loader may be upgraded to version 16.12.2r. For example:
<pre>ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.12.2r, RELEASE
SOFTWARE (P)</pre>On the C9300L models, the boot loader may be upgraded to version 16.12.2r . For example:
<pre>ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.12.2r, RELEASE
SOFTWARE (P)</pre>When using install commands to upgrade software, you may see this during the install operation:
<pre>!!!
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Wed Jul 31
18:03:28 Universal 2019 PLEASE DO NOT POWER CYCLE
BOOT LOADER UPGRADING
waiting for upgrades to complete...</pre></td></tr>
<tr><td>If you boot Cisco IOS XE Gibraltar 16.12.1 for the first time</td><td>On the C9300 models, the boot loader may be upgraded to version 16.12.1r[FC1]. For example:
<pre>ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.12.1r, RELEASE
SOFTWARE (P)</pre>On the C9300L models, the boot loader may be upgraded to version 16.11.1r[FC2]. For example:
<pre>ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.11.1r, RELEASE
SOFTWARE (P)</pre>When using install commands to upgrade software, you may see this during the install operation:
<pre>!!!
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Wed Jul 31
18:03:28 Universal 2019 PLEASE DO NOT POWER CYCLE
BOOT LOADER UPGRADING
waiting for upgrades to complete...</pre></td></tr>
</table>

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 mismatch: 0
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_1 mismatch: 1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_2 mismatch: 1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_3 mismatch: 0

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 ...393734 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 290 seconds
```

Software Installation Commands

Summary of Software Installation Commands **Supported starting from Cisco IOS XE Everest 16.6.2 and later releases**	
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.

Summary of Software Installation Commands Supported starting from Cisco IOS XE Everest 16.6.2 and later releases	
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.



Note The **request platform software** commands are deprecated starting from Cisco IOS XE Gibraltar 16.10.1. The commands are visible on the CLI in this release and you can configure them, but we recommend that you use the **install** commands to upgrade or downgrade.

Summary of request platform software Commands	
`Device# request platform software package ?`	
clean	Cleans unnecessary package files from media
copy	Copies package to media
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

Upgrading in Install Mode

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

Before you begin

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

When upgrading from ...	Use these commands...	To upgrade to...
Cisco IOS XE Everest 16.5.1a or Cisco IOS XE Everest 16.6.1	Only **request platform software** commands	Cisco IOS XE Gibraltar 16.12.1
Cisco IOS XE Everest 16.6.2 and later	Either **install** commands or **request platform software** commands	

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1 using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1 using **install** commands.

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.

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

The following sample output displays the cleaning up of unused files, by using the **request platform software package clean** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1. Use the **switch all** option to clean up all the switches in your stack

Note
Ignore the hexdump: messages in the CLI when you enter the command; they have no functional impact and will be removed in a later release. You will see this only on member switches and not on the active or standby. In the sample output below, hexdump messages are seen on switch 3, which is a member switch.

```
Switch# request platform software package clean switch all
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.
done.
```

```
Running command on switch 2
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.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
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
head: cannot open 'NVRAM' for reading: No such file or directory
NVRAM: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: stdin: Bad file descriptor
tail: cannot open 'NVRAM' for reading: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.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/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[2]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[3]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
```

```
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted
```

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1:

```
Switch# install remove inactive
install_remove: START Mon Jul 22 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.16.06.03.SPA.pkg
/flash/cat9k-guestshell.16.06.03.SPA.pkg
/flash/cat9k-rpbase.16.06.03.SPA.pkg
/flash/cat9k-rpboot.16.06.03.SPA.pkg
/flash/cat9k-sipbase.16.06.03.SPA.pkg
/flash/cat9k-sipspa.16.06.03.SPA.pkg
/flash/cat9k-srdriver.16.06.03.SPA.pkg
/flash/cat9k-webui.16.06.03.SPA.pkg
/flash/cat9k-wlc.16.06.03.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.06.03.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
```

```
Finished Post_Remove_Cleanup

SUCCESS: install_remove Mon Jul 22 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin flash:
destination filename [cat9k_iosxe.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin...
Loading /cat9k_iosxe.16.12.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

b) **dir flash:**

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

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

Directory of flash:/

434184 -rw- 601216545 Jul 22 2019 10:18:11 -07:00 cat9k_iosxe.16.12.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

Step 3 Set boot variable

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

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

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

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

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

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

```
Switch# show boot system
```

Step 4 Software install image to flash

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

You can point to the source image on your TFTP server or in flash if you have it copied to flash. 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 (flash-3):

```
Switch# request platform software package install switch all file
flash-3:cat9k_iosxe.16.12.01.SPA.bin auto-copy.
```

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.12.1 software image to flash, by using the **request platform software package install** command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.12.01.SPA.bin auto-copy

--- Starting install local lock acquisition on switch 1 ---
Finished install local lock acquisition on switch 1

Expanding image file: flash:cat9k_iosxe.16.12.01.SPA.bin
[1]: Copying flash:cat9k_iosxe.16.12.01.SPA.bin from switch 1 to switch 2 3
[2 3]: Finished copying to switch 2 3
[1 2 3]: Expanding file
[1 2 3]: Finished expanding all-in-one software package in switch 1 2 3
SUCCESS: Finished expanding all-in-one software package.
[1 2 3]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.12.01.SPA.pkg
Added cat9k-espbase.16.12.01.SPA.pkg
Added cat9k-guestshell.16.12.01.SPA.pkg
Added cat9k-rpbase.16.12.01.SPA.pkg
Added cat9k-rpboot.16.12.01.SPA.pkg
Added cat9k-sipbase.16.12.01.SPA.pkg
Added cat9k-sipspa.16.12.01.SPA.pkg
Added cat9k-srdriver.16.12.01.SPA.pkg
Added cat9k-webui.16.12.01.SPA.pkg
Added cat9k-wlc.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 cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
```

```
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.12.01.SPA.pkg
Added cat9k-espbase.16.12.01.SPA.pkg
Added cat9k-guestshell.16.12.01.SPA.pkg
Added cat9k-rpbase.16.12.01.SPA.pkg
Added cat9k-rpboot.16.12.01.SPA.pkg
Added cat9k-sipbase.16.12.01.SPA.pkg
Added cat9k-sipspa.16.12.01.SPA.pkg
Added cat9k-srdriver.16.12.01.SPA.pkg
Added cat9k-webui.16.12.01.SPA.pkg
Added cat9k-wlc.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 cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.12.01.SPA.pkg
Added cat9k-espbase.16.12.01.SPA.pkg
Added cat9k-guestshell.16.12.01.SPA.pkg
Added cat9k-rpbase.16.12.01.SPA.pkg
Added cat9k-rpboot.16.12.01.SPA.pkg
Added cat9k-sipbase.16.12.01.SPA.pkg
Added cat9k-sipspa.16.12.01.SPA.pkg
Added cat9k-srdriver.16.12.01.SPA.pkg
Added cat9k-webui.16.12.01.SPA.pkg
Added cat9k-wlc.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
Checking status of install on [1 2 3]
[1 2 3]: Finished install in switch 1 2 3
SUCCESS: Finished install: Success on [1 2 3]
```

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

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, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1:

```
Switch# install add file flash:cat9k_iosxe.16.12.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 22 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

*Mar 06 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.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:cat9k_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg

This operation 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

*Mar 06 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: mar 06 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 Mon Jul 22 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 ten new `.pkg` files and three `.conf` files.

The following is sample output of the **dir flash:** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg

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

11353194496 bytes total (8963174400 bytes free)
```

The following is sample output of the **dir flash:** command for the Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1 upgrade scenario:

```
Switch# dir flash:*.pkg

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

491524 -rw- 25711568  Jul 22 2019 11:49:33 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
491525 -rw- 78484428  Jul 22 2019 11:49:35 -07:00 cat9k-espbase.16.12.01.SPA.pkg
491526 -rw- 1598412   Jul 22 2019 11:49:35 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
491527 -rw- 404153288 Jul 22 2019 11:49:47 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
491533 -rw- 31657374  Jul 22 2019 11:50:09 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
491528 -rw- 27681740  Jul 22 2019 11:49:48 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
```

```
491529 -rw- 52224968  Jul 22 2019 11:49:49 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
491530 -rw- 31130572  Jul 22 2019 11:49:50 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
491531 -rw- 14783432  Jul 22 2019 11:49:51 -07:00 cat9k-webui.16.12.01.SPA.pkg
491532 -rw- 9160      Jul 22 2019 11:49:51 -07:00 cat9k-wlc.16.12.01.SPA.pkg
11353194496 bytes total (9544245248 bytes free)
Switch#
```

The following sample output displays the .conf files in the flash partition; note the two .conf files:

- `packages.conf`—the file that has been re-written with the newly installed .pkg files
- `cat9k_iosxe.16.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Jul 22 2019 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 22 2019 10:58:08 -07:00 cat9k_iosxe.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 (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 30-Jul-19 19:26 by mcpre

<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Gibraltar 16.12.1	Either **install** commands or **request platform software** commands	Cisco IOS XE Gibraltar 16.11.x or earlier releases

Starting from Cisco IOS XE Gibraltar 16.12.1, a new microcode is introduced to support IEEE 802.3bt Type 3 standard for UPOE switches in the series (C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-48UN). The new microcode is not backward-compatible with some releases, because of which you must also downgrade the microcode when you downgrade to one of these releases. If the microcode is not downgraded, PoE features will be impacted after the downgrade.

Depending on the release you are downgrading to and the commands you use to downgrade, review the table below for the action you may have to take:

When downgrading from ...	To one of These Releases	by Using...	Action For Microcode Downgrade
Cisco IOS XE Gibraltar 16.12.1 or a later release	Cisco IOS XE Everest 16.6.1 through Cisco IOS XE Everest 16.6.6 Cisco IOS XE Fuji 16.9.1 through Cisco IOS XE Fuji 16.9.2	**install** commands	Microcode will roll back automatically as part of the software installation. No further action is required.
		request platform software commands or or bundle boot	Manually downgrade the microcode before downgrading the software image. Enter the **hw-module mcu rollback** command in global configuration mode, to downgrade microcode.

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Everest 16.6.1, by using the **install** commands.

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.

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

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 Mon Jul 22 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.12.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.

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

SUCCESS: install_remove Mon Jul 22 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

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

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin flash:
Destination filename [cat9k_iosxe.16.06.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin...
Loading /cat9k_iosxe.16.06.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)
```

b) **dir flash:**

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

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

Directory of flash:/

434184 -rw- 508584771 Jul 22 2018 13:35:16 -07:00 cat9k_iosxe.16.06.01.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 Everest 16.6.1 software image to flash with microcode downgrade, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.16.06.01.SPA.bin activate commit

install_add_activate_commit: START Tue Jul 30 23:51:14 UTC 2019
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

Image added. Version: 16.6.1.0.202
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-webui.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.01.SPA.pkg

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

```
[1] Activate package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.12.01.SPA.pkg
Removed cat9k-espbase.16.12.01.SPA.pkg
Removed cat9k-guestshell.16.12.01.SPA.pkg
Removed cat9k-rpbase.16.12.01.SPA.pkg
Removed cat9k-rpboot.16.12.01.SPA.pkg
Removed cat9k-sipbase.16.12.01.SPA.pkg
Removed cat9k-sipspa.16.12.01.SPA.pkg
Removed cat9k-srdriver.16.12.01.SPA.pkg
Removed cat9k-webui.16.12.01.SPA.pkg
Removed cat9k-wlc.16.12.01.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.06.01.SPA.pkg
Added cat9k-espbase.16.06.01.SPA.pkg
Added cat9k-guestshell.16.06.01.SPA.pkg
Added cat9k-rpbase.16.06.01.SPA.pkg
Added cat9k-rpboot.16.06.01.SPA.pkg
Added cat9k-sipbase.16.06.01.SPA.pkg
Added cat9k-sipspa.16.06.01.SPA.pkg
Added cat9k-srdriver.16.06.01.SPA.pkg
Added cat9k-webui.16.06.01.SPA.pkg
Finished list of software package changes
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

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

[1]: Performing Upgrade_Service
%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (local/local): Starting boot preupgrade
300+0 records in
300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.315648 s, 973 kB/s
/tmp/microcode_update/boot_pkg/nyquist/usr/platform/polaris_adelphi_rommon_sb.bin: No such
 file or directory
MM [1] MCU version 127 sw ver 172
MM [2] MCU version 127 sw ver 172


MCU UPGRADE IN PROGRESS... PLEASE DO NOT POWER CYCLE!!

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 ...409334 bytes.
Front-end Microcode IMG MGR: Programming device
0% 10 20 30 40 50 60 70 80 90 100
Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...25210 bytes.
Front-end Microcode IMG MGR: Programming device
```

```
0...rrrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%....100%w

% Front-end Microcode IMG download pre-reload on sub=0
Front-end Microcode IMG MGR: Preparing to program device[0], index=3 ...90974 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 263 seconds


MCU UPGRADE COMPLETED!!... SUCCESS: Upgrade_Service finished
Install will reload the system now!
SUCCESS: install_add_activate_commit Tue Jul 30 23:59:48 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 Everest 16.6.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Fri 16-Mar-18 06:38 by mcpre
<output truncated>
```

Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 9000 Series Switches.

License Levels

The software features available on Cisco Catalyst 9300 Series Switches fall under these base or add-on license levels.

Base Licenses

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

Add-On Licenses

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

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

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

License Types

The following license types are available:

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

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.

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

Table 4: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[3]	Yes

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

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

Cisco Smart Licensing

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

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

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

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

Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device that is running Cisco IOS XE Fuji 16.9.1 or later releases. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

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

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

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

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

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

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

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

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

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

With this,

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

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

Starting from Cisco IOS XE Fuji 16.9.1, if an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

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

How Upgrading or Downgrading Software Affects Smart Licensing

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



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

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

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

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

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

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9300 Series Switches datasheet at:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.html

Limitations and Restrictions

- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Flexible NetFlow limitations
  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
  - You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.
  - You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
  - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.
- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.

- When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

  Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- Stacking:
  - A switch stack supports up to eight stack members.
  - Mixed stacking is not supported. Cisco Catalyst 9300 Series Switches cannot be stacked with Cisco Catalyst 3850 Series Switches or C9300L models of Cisco Catalyst 9300 Series Switches.
  - Auto upgrade for a new member switch is supported only in the install mode.

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the tacacs server command in global configuration mode.
- USB Authentication—When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

  ```
  Device(config)# password encryption aes
  Master key change notification called without new or old key
  ```

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- Wired Application Visibility and Control limitations:
  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)
  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance—Each switch member is able to handle 2000 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.

- Scale—Able to handle up to 20000 bi-directional flows per 24 access ports and per 48 access ports.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- The File System Check (fsck) utility is not supported in install mode.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Caveats

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

Cisco Bug Search Tool

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

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

Open Caveats in Cisco IOS XE Gibraltar 16.12.x

Identifier	Description
CSCvr87767	PDs not detected and powered up on 9300 with 2-pair cables
CSCvs89494	C9300-24UX-A connected to 3rd party device stop packet forwarding

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.8

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

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.7

Identifier	Description
CSCvz18983	Interface with "power inline never" and "speed auto 10 100" disables autonegotiation.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

Identifier	Description
CSCvv27849	Cat 9K & 3K: Unexpected reload caused by the FED process.
CSCvw65866	Packet loss and jitter seen for media traffic when connected to C9300-48UN
CSCvw87096	Cat9300 interface remains down after a reload of an individual stack member
CSCvw91573	C9300 port LED amber with NIM card
CSCvx11287	9300L - No connectivity when using GLC-LH-SMD on uplinks with speed nonegotiate on both ends
CSCvx90075	9300-NM-8X + SFP-H10GB-CU 3m or 5m and certain link partners could experience long link times
CSCvx94722	Radius protocol generate jumbo frames for dot1x packets
CSCvx96576	C9300 switches incorrectly log %THERMAL-1-THERMAL_GREEN_THRESHOLD: Switch 1 R0/0:
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
CSCvw65866	Packet loss and jitter seen for media traffic when connected to C9300-48UN

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5

Identifier	Description
CSCvu62273	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading
CSCvv16874	Catalyst Switch: SISF Crash due to a memory leak
CSCvw63161	ZTP failing with error in creating downloaded_script.py
CSCvw74061	Cat9300 & Cat9500 series switches may see unexpected reloads due to Localsoft or CpuCatastrophicErr

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.4

Identifier	Description
CSCvp77133	systemd service flash-recovery.service always in the running mode
CSCvq17488	show module info for active switch is n/a after booting remaining switches
CSCvq65380	Switch sending EAP-Request/Identity after receiving EAPOL-Logoff request from a non-existent client
CSCvr41932	17.1.1 - Memory leak @ SAMsgThread.
CSCvr86162	Output of crepSegmentComplete is incorrect for the switches with single Edge port
CSCvr92287	EPC with packet-len opt breaks CPU in-band path for bigger frames
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs42154	EEM action "force-switchover" not working properly
CSCvs71084	Cat9k - Not able to apply Et-analytics on an interface
CSCvs73383	"show mac address-table" does not show remote EIDs when vlan filter used
CSCvs75010	Traffic forwarding stops when Session Idle time out is configured 10 sec with active traffic running
CSCvs77781	Critical auth failing to apply DEFAULT_CRITICAL_DATA_TEMPLATE
CSCvs80968	kernel error message seen when usb insert/remove
CSCvs83963	AppGig interface changed to down on "no iox"
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs91593	offer is dropped in data vlan with dhcp snooping using dot1x/mab
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt01187	Eigrp neighbor down up occurred frequently
CSCvt02962	Uplink Port-channel Trunk member link Port LED truns to amber blinking after link down/up
CSCvt30243	connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt44928	incorrect default action for pnp startup vlan
CSCvt60246	C9300L-48T-4X cannot detect PSU oir after fullly booting up.
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

Identifier	Description
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvt88722	cat9k keep auto-neg enabled even with hard code speed and duplex causing auto-neg mismatch
CSCvt93918	c9300 reboot due to ACL count being huge.
CSCvt98435	16.12.3 not creating system-reports on crashes
CSCvt99199	MACSEC issue in SDA deployment
CSCvu00069	CLI addition to tune MSRP timers
CSCvu13029	Intermittent Link Flaps on mGig Cat9k switches to mGig capable endpoints
CSCvu15007	Crash when invalid input interrupts a role-based access-list policy installation
CSCvu35345	AVB: msrp stream fails to re-establish after mcast addr change

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
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvq24181	Crash/Unresponsiveness after TDR test is set through SNMP
CSCvq72472	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr13950	Silent loss and TCP Re-transmissions seen with certain host pcs connected to c9300-48UXM
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

Identifier	Description
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
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.
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
CSCvs52594	9300L-48P suddenly stops providing PoE on certain ports
CSCvs61571	Cat3k/Cat9k- OBJ_DWNLD_TO_DP_FAILED after exceeding hardware capacity for adjacency table
CSCvs62003	In COPP policy, ARP traffic should be classified under the "system-cpp-police-forus" class
CSCvs68255	Traceback seen when IS-IS crosses LSP boundary and tries to add information in new LSP
CSCvs73580	Memory leak in fed main event qos
CSCvt00402	cat3k Switch with 1.6GB flash size unable to do SWIM upgrade between 16.12.x images

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.2

Identifier	Description
CSCvo66246	Enabling SPAN source of VLAN 1 affects LACP operations
CSCvp37771	Mgig - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones
CSCvp62101	~3sec Traffic Loss on Uplink Port Channel After Active SUP removal
CSCvp66193	IOSd Crash within "DHCPD Receive" process
CSCvp70112	EnvMon trap not received after Power Supply and FAN OIR
CSCvp95156	Memory leak in linux_iosd when polling mabClientIndexTest mib.
CSCvq22224	// evpn/vxlan // dhcp relay not working over l3vni
CSCvq26295	cat9300: missing system_report when crashed
CSCvq29115	Failed to get Board ID shown if stack member boots up
CSCvq30460	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq35631	Switch crashed due to HTTP Core
CSCvq36108	Traceback seen during issu with IGMP and MLD snooping features enabled
CSCvq40137	Mac address not being learnt when "auth port-control auto" command is present
CSCvq44397	ospf down upon switchover with aggressive timers "hello-interval 1" and "dead-interval 4"
CSCvq50632	SUP uplinks and/or slot 7 or slot 8 stop passing traffic or fail POST upon SUP failover
CSCvq55779	FIVE GIG INTERFACE NOT SHOWING IN CLI WHILE CONFIGURING IP IGMP SNOOPING
CSCvq66802	igmp query with src ip 0.0.0.0 is not ignored
CSCvq89352	missing system_report when crashed - revisit fix of CSCvq26295
CSCvq94738	The COPP configuration back to the default After rebooting the device
CSCvq97906	"DHCPD Receive" process crash
CSCvr03905	Memory Leak on FED due to IPv6 Source Guard
CSCvr13950	Silent loss and TCP Re-transmissions seen with certain host pcs connected to c9300-48UXM
CSCvr15802	Forwarding unable to recover after reaching adjacency HW limitation without reload
CSCvr20522	BOOTREPLY dropped when DHCP snooping is enabled

Identifier	Description
CSCvr29921	Inserting 1Gige SFP (GLC-SX-MMD or SFP GE-T) to SUP port causes another port to link flap.
CSCvr46931	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr51939	Inactive Interfaces Incorrectly Holding Buffers, causing output drops on switch SUP active ports.
CSCvr70470	sessmgrd crash with "clear dot1x mac" command
CSCvr71158	Commands returning invalid PRC error message

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1

Identifier	Description
CSCvi56567	When 9300 switch boots up, link up of its downlink has delayed if switch has network module
CSCvk44346	Power high priority not observed in Strict mode on 9300
CSCvm77197	C9300/9500 : %IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:
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
CSCvn77683	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvn83940	Cat9k TFTP copy failed with Port Security enabled
CSCvo15594	Hardware MAC address programming issue for remote client catalyst 9300
CSCvo17778	Cat9k not updating checksum after DSCP change
CSCvo24073	multiple CTS sessions stuck in HELD/SAP_NE
CSCvo32446	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo33983	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo56403	Standby Switch Stuck in HA Sync config after Stack-Merge
CSCvo56629	Cat9500 - Interface in Admin shutdown showing incoming traffic and interface Status led in green.
CSCvo59504	Cat3K | Cat9K - SVI becomes inaccesible upon reboot
CSCvo62414	C9300, C9200, C9200L switches are unable to stack, one switch stuck in Initializing

Identifier	Description
CSCvo71264	Cat3k / Cat9k Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo75559	Cat9300 | First packet not forwarded when (S,G) needs to be built
CSCvo78538	Counters in the "show interface" command are not increasing
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 9300 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html

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

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

Communications, Services, and Additional Information

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

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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)

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