Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Everest 16.6.x

First Published: July 31, 2017
Last Updated: September 30, 2019

This release note gives an overview of the hardware and software with Cisco IOS XE Everest 16.6.x, on the Cisco Catalyst 9300 Series Switches.
Unless otherwise noted, the terms switch and device refer to a standalone switch and to a switch stack.

- For information about unsupported features, see Important Notes, page 9.
- For information about software and hardware restrictions and limitations, see Limitations and Restrictions, page 39.
- For information about open issues with the software, see Caveats, page 42.

Introduction

Cisco Catalyst 9300 Series Switches are Cisco’s lead stackable access platforms for the next-generation enterprise. It has been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.
Cisco Catalyst 9300 Series Switches deliver complete convergence 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). The series forms the foundational building block for SD-Access, which is Cisco’s lead enterprise architecture.
The series offers 1Gigabit copper Ethernet switches with 80G uplink bandwidth, Multigigabit Ethernet switches, and the industry’s highest 480 Gigabit stacking bandwidth solution. It also provides a highly resilient and efficient power architecture with StackPower that delivers high density of UPoE and PoE+ ports.
Whats New in Cisco IOS XE Everest 16.6.7

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.6

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.5

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.4a

There are no new hardware or software features in this release.

Whats New in Cisco IOS XE Everest 16.6.4

Hardware Features in Cisco IOS XE Everest 16.6.4

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9300 Series Switches—MultiGigabit Ethernet Uplink Network Module (C9300-NM-4M)</td>
<td>This module has four 10G MultiGigabit Ethernet ports that support interface speeds of 100M/1G/2.5G/5G/10G; it can be installed in all models of Cisco Catalyst 9300 Series Switches. See the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.</td>
</tr>
</tbody>
</table>

Whats New in Cisco IOS XE Everest 16.6.3

There are no new hardware or software features in this release.
Whats New in Cisco IOS XE Everest 16.6.2

Hardware Features in Cisco IOS XE Everest 16.6.2

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9300-48UXM-E</td>
<td>Stackable 48 (36 2.5G Multigigabit Ethernet and 12 10G Multigigabit Ethernet Universal Power Over Ethernet (UPOE) ports).</td>
</tr>
<tr>
<td>C9300-48UXM-A</td>
<td>See the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.</td>
</tr>
</tbody>
</table>

Software Features in Cisco IOS XE Everest 16.6.2

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Install</td>
<td>The Software Install feature facilitates moving from one version of the software to another version in install mode.</td>
</tr>
<tr>
<td></td>
<td>See System Management -&gt; Performing Device Setup Configuration.</td>
</tr>
<tr>
<td>YANG Data Models</td>
<td>YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to <a href="https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1662">https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1662</a>.</td>
</tr>
<tr>
<td></td>
<td>Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release. (Network Essentials and Network Advantage)</td>
</tr>
</tbody>
</table>
What's New in Cisco IOS XE Everest 16.6.1

Hardware Features in Cisco IOS XE Everest 16.6.1

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multigigabit Ethernet Switch Model—C9300-24UX</td>
<td>Cisco Catalyst 9300 Series Switches now support C9300-24UX—a Stackable 24 Multigigabit Ethernet 100/1000/2500/5000/10000 switch with UPoE ports; PoE budget of 490 W with 1100 WAC power supply; supports StackWise-480 and StackPower. See the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.</td>
</tr>
<tr>
<td>Cisco QSFP to SFP or SFP+ Adapter (Cisco QSA Module) —CVR-QSFP-SFP10G</td>
<td>Cisco Catalyst 9300 Series Switches support the Cisco QSA Module, which is a pluggable adapter that converts a QSFP port into an SFP+ port. You can connect only an SFP+ module. See SFP and SFP+ Modules.</td>
</tr>
</tbody>
</table>

Software Features in Cisco IOS XE Everest 16.6.1

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description and License Level Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>New in Wired Switching</td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Protocol Bypass</td>
<td>A backward compatible mode, equivalent to not having Cisco Discovery Protocol support. When the feature is enabled, Cisco Discovery Protocol packets are received and transmitted unchanged. Received packets are not processed; no packets are generated. In this mode, 'bump-in-the-wire' behavior is applied to Cisco Discovery Protocol packets. See Security -&gt; Cisco Discovery Protocol Bypass. (Network Essentials and Network Advantage)</td>
</tr>
<tr>
<td>Cisco Nonstop Forwarding (NSF) Support for IPv6</td>
<td>Cisco NSF is now supported for IPv6 traffic. Cisco NSF works with the Stateful switchover (SSO) feature to minimize the amount of time a network is unavailable to its users following a switchover. See Stack Manager and High Availability -&gt; Configuring NSF with SSO. (Network Advantage)</td>
</tr>
<tr>
<td>Encrypted Traffic Analytics (ETA)</td>
<td>Studies the packet flow behavior of an application to determine the flow characteristics such as, malware analysis and crypto audit. See Network Management -&gt; Configuring Encrypted Traffic Analytics. (DNA Advantage)</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>High Availability— Graceful Insertion and Removal (GIR)</td>
<td>Uses a maintenance mode to isolate the switch from the network in order to perform debugging, or an upgrade. GIR is supported for Layer 2 interface shutdown and the Intermediate System to Intermediate System (IS-IS) routing protocol. When you place the switch in maintenance mode, supported protocols are isolated, and Layer 2 interfaces are shut down. When normal mode is restored, the supported protocols and ports are brought back up. See Stack Manager and High Availability -&gt; Configuring Graceful Insertion and Removal (GIR).</td>
</tr>
<tr>
<td>High Availability: (1:1) Redundancy</td>
<td>Determines the active and standby role for a specific switch in a stack, based on the flash ROMMON variable. WARNING: Changing the switch role may result in redundancy mode being configured to 1+1 mode for the stack. If the configured Active or Standby switch does not boot up, then the stack will not be able to boot. See Stack Manager and High Availability-&gt; Configuring 1:1 Redundancy.</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) Explicit Tracking</td>
<td>Enables a multicast device to explicitly track the membership of all multicast hosts in a particular multiaccess network. The explicit tracking of hosts, groups, and channels enables the device to keep track of each individual host that is joined to a particular group or channel. See IP Multicast Routing -&gt; IGMP Explicit Tracking.</td>
</tr>
<tr>
<td>IPv6 Multicast with Virtual Private Networks (VPN) Routing Forwarding Table (VRF-Lite)</td>
<td>Allows a service provider to support two or more VPNs with overlapping IP addresses using one interface. VRF-Lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. See IP Multicast Routing -&gt; Configuring VRF-lite.</td>
</tr>
</tbody>
</table>
| Locator ID Separator Protocol (LISP) Extranet Support and Source Group Access Control List (SGACL) Cell Statistics | • LISP Extranet Support—Refers to subscriber-to-provider communication across instance IDs in a LISP network. With LISP Extranet support, hosts in VRF “A”, for example, can access shared resources in VRF “B”.  
• SGACL Cell Statistics—An enhancement in the `show cts role-based counters ipv4` command, to display all SGACL enforcement statistics for IPv4, providing visibility at the cell level.  
See [Campus Fabric](#) (DNA Advantage) |

See [Campus Fabric](#) (DNA Advantage)
Multiprotocol Label Switching

- Ethernet over MPLS (EoMPLS)
- Virtual Private LAN Services (VPLS)
- EIGRP MPLS VPN PE-CE Site of Origin (SoO)
- Route Target Rewrite
- external BGP (eBGP) and internal BGP (iBGP) OR eiBGP
- IPv6 Provider Edge over MPLS (6PE)
- IPv6 VPN Provider Edge over MPLS (6VPE)

The following MPLS features are introduced in this release:

- EoMPLS—One of the Any Transport over MPLS (AToM) transport types. EoMPLS provides a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and uses label stacking to forward them across the MPLS network.

- VPLS—A class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP/MPLS network. VPLS uses the provider core to join multiple attachment circuits together, to simulate a virtual bridge that connects the multiple attachment circuits together.

- EIGRP MPLS VPN PE-CE SoO—Introduces the capability to filter MPLS Virtual Private Network (VPN) traffic on a per-site basis for Enhanced Interior Gateway Routing Protocol (EIGRP) networks. SoO filtering is configured at the interface level and is used to manage MPLS VPN traffic, and to prevent transient routing loops from occurring in complex and mixed network topologies.

- Route Target Rewrite—Allows the replacement of route targets on incoming and outgoing Border Gateway Protocol (BGP) updates. Route targets are carried as extended community attributes in BGP Virtual Private Network IP Version 4 (VPNv4) updates. Route target extended community attributes are used to identify a set of sites and VPN routing and forwarding (VRF) instances that can receive routes with a configured route target.

- eiBGP—Enables you to configure multipath load balancing with both eBGP and iBGP paths in Border Gateway Protocol (BGP) networks that are configured to use MPLS VPNs. The feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks.

- 6PE—A technique that provides global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices. 6PE allows IPv6 domains to communicate with one another over the IPv4 without an explicit tunnel setup, requiring only one IPv4 address per IPv6 domain.

- 6VPE—A mechanism to use the IPv4 backbone to provide VPN IPv6 services. 6VPE is like a regular IPv4 MPLS-VPN provider edge, with an addition of IPv6 support within VRF. It provides logically separate routing table entries for VPN member devices.

See Multiprotocol Label Switching.
(Network Advantage)
### Programmability

- **Zero-Touch Provisioning (ZTP):** HTTP Download.
- **Model-Driven Telemetry**
- **Preboot Execution Environment Client (iPXE)**
- **YANG Data Models**

Programmability features introduced or enhanced in this release:

- **ZTP**—Now supports HTTP file download along with TFTP file download.
- **Model-Driven Telemetry**—Provides a mechanism to stream data from a Model-Driven Telemetry-capable device, to a destination. The data to be streamed is driven through subscription. The feature is enabled automatically, when NETCONF-YANG is started on a device.
- **iPXE**—An open Preboot eXecution Environment (PXE) client that allows a device to boot from a network boot image. iPXE is supported with IPv4 only.
- **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/1661](https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1661). 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.


(University of Network Essentials and Network Advantage)

### Software Maintenance Upgrade (SMU)

SMU is a package that can be installed on a system, to provide a patch fix or security resolution to a released image. See System Management -> Software Maintenance Upgrade.

(DNA Advantage)

### Stateful Switchover (SSO) Support for IPv6

SSO is now supported for IPv6 traffic.

With this feature, when an active switch fails, the standby switch starts up in a fully-initialized state and synchronizes with the persistent configuration and the running configuration of the active switch. The new active switch uses existing Layer 2 switching information to continue forwarding traffic.

See Stack Manager and High Availability -> Configuring NSF with SSO.

(Network Essentials and Network Advantage)

### Virtual Private Network Routing and Forwarding-Aware Generic Routing Encapsulation (GRE)

Enables you to configure the source and destination of a GRE IP tunnel to belong to any VRF table.

See Routing -> Configuring Generic Routing Encapsulation (GRE) Tunnel IP Source and Destination VRF Membership.

(Network Advantage)

New in Software-Defined Access Wireless
The Enterprise Fabric provides end-to-end enterprise-wide segmentation, flexible subnet addressing, and controller-based networking with uniform enterprise-wide policy and mobility. It moves the enterprise network from current VLAN-centric architecture to a user group-based enterprise architecture, with flexible Layer 2 extensions within and across sites.

See Campus Fabric.

Network Advantage

New on the Web User Interface

<table>
<thead>
<tr>
<th>Web UI support for DNS Proxy and troubleshooting</th>
<th>Features introduced and updated on the Web UI in this release:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DNS Proxy Support</td>
<td>• DNS Proxy Support</td>
</tr>
<tr>
<td>• Troubleshooting- Audit Device Configuration</td>
<td>• Troubleshooting- Debug Bundle</td>
</tr>
</tbody>
</table>

Important Notes

The following are the unsupported hardware and software features for the Cisco Catalyst 9300 Series Switches. For the list of supported features, go to http://www.cisco.com/go/cfn.

- Unsupported Hardware Features
  - The rear USB 3.0 port
  - Breakout cables

- Unsupported Software Features:
  - IPsec with FIPS

These features are supported on the Cisco Catalyst 3850 Series Switches, but not on the Cisco Catalyst 9300 Series Switches:

- 128-bit and 256-bit AES MACsec (IEEE 802.1AE) host link encryption (downlinks) with MACsec Key Agreement (MKA)
- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Bluetooth
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Gateway LoadBalancing Protocol (GLBP)
- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)
- Cisco Plug-in for OpenFlow 1.3
- IPsec VPN
- Performance Monitoring (PerfMon)
- Boot Integrity Visibility
Supported Hardware

Cisco Catalyst 9300 Series Switches—Model Numbers

Table 1 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, page 36.

<table>
<thead>
<tr>
<th>Switch Model No.</th>
<th>Default License Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9300-24T-E</td>
<td>Network Essentials</td>
<td>Stackable 24 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower.</td>
</tr>
<tr>
<td>C9300-24T-A</td>
<td>Network Advantage</td>
<td>Stackable 24 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower.</td>
</tr>
<tr>
<td>C9300-24P-E</td>
<td>Network Essentials</td>
<td>Stackable 24 10/100/1000 UPoE ports; PoE budget of 830W; 1100 WAC power supply; supports StackWise-480 and StackPower.</td>
</tr>
<tr>
<td>C9300-24P-A</td>
<td>Network Advantage</td>
<td>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.</td>
</tr>
<tr>
<td>C9300-24UX-E</td>
<td>Network Essentials</td>
<td>Catalyst 9300 48-port (12 mGig + 36x 2.5G) and UPoE</td>
</tr>
<tr>
<td>C9300-24UXM-A</td>
<td>Network Advantage</td>
<td>Catalyst 9300 48-port (12 mGig + 36x 2.5G) and UPoE</td>
</tr>
<tr>
<td>C9300-48T-E</td>
<td>Network Essentials</td>
<td>Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower.</td>
</tr>
<tr>
<td>C9300-48T-A</td>
<td>Network Advantage</td>
<td>Stackable 48 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower.</td>
</tr>
<tr>
<td>C9300-48P-E</td>
<td>Network Essentials</td>
<td>Stackable 48 10/100/1000 UPoE ports; PoE budget of 822 W; 1100 WAC power supply; supports StackWise-480 and StackPower.</td>
</tr>
<tr>
<td>C9300-48P-A</td>
<td>Network Advantage</td>
<td>Stackable 48 (36 2.5G Multigigabit Ethernet and 12 10G Multigigabit Ethernet Universal Power Over Ethernet (UPOE) ports).</td>
</tr>
</tbody>
</table>

1. See Table 9 Permitted Combinations, for information about the add-on licenses that you can order.
Network Modules

Table 2 lists the optional uplink network modules with 1-Gigabit, 10-Gigabit, and 40-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

<table>
<thead>
<tr>
<th>Network Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9300-NM-4G1</td>
<td>Four 1Gigabit Ethernet SFP module slots</td>
</tr>
<tr>
<td>C9300-NM-8X1</td>
<td>Eight 10 Gigabit Ethernet SFP+ module slots.</td>
</tr>
<tr>
<td>C9300-NM-2Q1</td>
<td>Two 40 Gigabit Ethernet QSFP+ module slots.</td>
</tr>
<tr>
<td>C3850-NM-4-1G</td>
<td>Four 1Gigabit Ethernet SFP module slots</td>
</tr>
<tr>
<td>C3850-NM-2-10G</td>
<td>Two 10 Gigabit Ethernet SFP module slots</td>
</tr>
<tr>
<td>C3850-NM-4-10G</td>
<td>Four 10 Gigabit Ethernet SFP module slots</td>
</tr>
<tr>
<td>C3850-NM-8-10G</td>
<td>Eight 10 Gigabit Ethernet SFP module slots</td>
</tr>
<tr>
<td>C3850-NM-2-40G</td>
<td>Two 40 Gigabit Ethernet SFP module slots</td>
</tr>
</tbody>
</table>

1. Supported only on Cisco Catalyst 9300 Series Switches

Optics Modules

Catalyst switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest (SFP) compatibility information:


Compatibility Matrix

Table 3 Software Compatibility Matrix

<table>
<thead>
<tr>
<th>Catalyst 9300</th>
<th>Cisco Identity Services Engine</th>
<th>Cisco Access Control Server</th>
<th>Prime Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everest 16.6.7</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>5.5</td>
<td>See Prime Infrastructure 3.1 on cisco.com</td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.6</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>5.5</td>
<td>See Prime Infrastructure 3.1 on cisco.com</td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Everest 16.6.5</td>
<td>2.2</td>
<td>5.4</td>
<td>PI 3.1.6 + Device Pack 13</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>5.5</td>
<td>See Prime Infrastructure 3.1 on cisco.com</td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Web UI System Requirements

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

Hardware Requirements

Table 4 Minimum Hardware Requirements

<table>
<thead>
<tr>
<th>Processor Speed</th>
<th>DRAM</th>
<th>Number of Colors</th>
<th>Resolution</th>
<th>Font Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>233 MHz minimum$^1$</td>
<td>512 MB$^2$</td>
<td>256</td>
<td>1024 x 768</td>
<td>Small</td>
</tr>
</tbody>
</table>

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Operating Systems
  - Windows 10 or later
  - Mac OS X 10.11 or later
- Browsers
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.

Table 5  Software Images

<table>
<thead>
<tr>
<th>Release</th>
<th>Image</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.7</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.07.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.07.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.6</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.06.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.06.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.5</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.05.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.05.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.4a</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.04a.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.04a.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.4</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.04.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.04.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.3</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.03.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.03.SPA.bin</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.2</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.02.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.02.SPA.bin</td>
</tr>
</tbody>
</table>
Upgrading the Switch Software

Note: You cannot use the Web UI to install, upgrade, or downgrade switch software.

This section covers the following:
- Automatic Boot Loader Upgrade
- Automatic Microcode Upgrade
- Upgrading in Install Mode
- Downgrading in Install Mode

Note: From Cisco IOS XE Everest 16.6.2 onwards, we support new install commands. These install commands are supported along with the previously supported request platform software commands. Both set of commands are supported at present.

<table>
<thead>
<tr>
<th>Release</th>
<th>Image</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.06.01.SPA.bin</td>
</tr>
<tr>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.06.01.SPA.bin</td>
<td></td>
</tr>
</tbody>
</table>

Table 6: request platform software commands to Upgrade or Downgrade Switch Software

<table>
<thead>
<tr>
<th>Switch# request platform software package?</th>
</tr>
</thead>
<tbody>
<tr>
<td>clean</td>
</tr>
<tr>
<td>copy</td>
</tr>
<tr>
<td>describe</td>
</tr>
<tr>
<td>expand</td>
</tr>
<tr>
<td>install</td>
</tr>
<tr>
<td>uninstall</td>
</tr>
<tr>
<td>verify</td>
</tr>
</tbody>
</table>

Table 7: install commands to Upgrade or Downgrade Switch Software

Switch# install add file filename [activate commit] — Use this command to install and activate the specified file, and to commit changes to be persistent across reloads.

Switch# install ? — You can also use the install command to separately install, activate, commit, abort, or remove the installation file.

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. |
### Table 7: install commands to Upgrade or Downgrade Switch Software (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activate</td>
<td>Activates the file, and reloads the device.</td>
</tr>
<tr>
<td>auto-abort-timer</td>
<td>The auto-abort-timer keyword automatically rolls back the image activation.</td>
</tr>
<tr>
<td>commit</td>
<td>Makes changes persistent over reloads.</td>
</tr>
<tr>
<td>rollback to committed</td>
<td>Rolls back the update to the last committed version.</td>
</tr>
<tr>
<td>abort</td>
<td>Aborts the file activation, and rolls back to the version that was running before the current installation procedure started.</td>
</tr>
<tr>
<td>remove</td>
<td>Deletes all unused and inactive software installation files.</td>
</tr>
</tbody>
</table>

### 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 IOS XE 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 8  

**Automatic Boot Loader Response**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Automatic Boot Loader Response</th>
</tr>
</thead>
</table>
| If you boot Cisco IOS XE Everest 16.6.2, or Cisco IOS XE Everest 16.6.3, or Cisco IOS XE Everest 16.6.4, or Cisco IOS XE Everest 16.6.4a, or Cisco IOS XE Everest 16.6.5, or Cisco IOS XE Everest 16.6.6, or Cisco IOS XE Everest 16.6.7 for the first time | The boot loader may be upgraded to version 16.10.1r[FC1]. For example:  
* ROM: IOS-XE ROMMON  
* BOOTLDR: System Bootstrap, Version 16.6.1r [FC1], RELEASE SOFTWARE (P)  
If the automatic boot loader upgrade occurs while booting, you will see the following on the console:  

```plaintext  
%IOSXEBOOT-Wed-###: (rp/0): Jul 26 16:57:44 Universal 2017 PLEASE DO NOT POWER CYCLE ###BOOT LOADER UPGRADES 4  
Both links down, not waiting for other switches  
Switch number is 1  
%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4  
```

| If you boot Cisco IOS XE Everest 16.6.1 the first time | The boot loader may be upgraded to version 16.6.1r [FC1]. For example:  
* ROM: IOS-XE ROMMON  
* BOOTLDR: System Bootstrap, Version 16.6.1r [FC1], RELEASE SOFTWARE (P)  
If the automatic boot loader upgrade occurs while booting Cisco IOS XE Everest 16.6.1, you will see the following on the console:  

```plaintext  
%IOSXEBOOT-Wed-###: (rp/0): Jul 26 16:57:44 Universal 2017 PLEASE DO NOT POWER CYCLE ###BOOT LOADER UPGRADES 4  
Both links down, not waiting for other switches  
Switch number is 1  
%IOSXEBOOT-loader-boot: (rp/0): upgrade successful 4  
```
Automatic Microcode Upgrade

During an IOS image upgrade or downgrade on a PoE or UPoE switch, the microcode is updated to reflect applicable feature enhancements and bug fixes. Do not restart the switch during the upgrade or downgrade process.

It takes approximately an additional 4 minutes to complete the microcode upgrade, in addition to the normal reload time. The microcode update 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.

The following console messages are displayed during microcode upgrade from Cisco IOS XE Everest 16.6.1 to Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3:

```
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: Preparing to program device[0], index=2 ...25186 bytes.
Front-end Microcode IMG MGR: Preparing to program device[0], index=3 ...86370 bytes.... Skipped[3].
```

Front-end Microcode IMG MGR: Microcode programming complete for device 0.
Front-end Microcode IMG MGR: Preparing to program device[0], index=0 ...594412 bytes.... Skipped[0].
Front-end Microcode IMG MGR: Microcode programming complete in 290 seconds
Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, in install mode.

**Note** The **install** commands are available only from Cisco IOS XE Everest 16.6.2.

In Cisco IOS XE Everest 16.6.2, a new set of **install** commands have been introduced for the installation and upgrade of images in install mode. You can either use the **install** commands or the **request platform software** commands for install, upgrade, and downgrade of software images. For more information, about the Software Install feature, see the Performing Device Setup Configuration chapter of the System Management Configuration Guide.

The sample output in this section covers upgrade from Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Everest 16.6.1 and from Cisco IOS XE Everest 16.6.1 to Cisco IOS XE Everest 16.6.2 in Install Mode.

This section provides examples of both **request platform software** and **install** commands.

**Summary Steps**—**Clean Up > Copy New Image to Flash > Set Boot Variable > Software Install Image to Flash > Reload**

**Clean Up**

**Step 1** 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. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.5.1a files:

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

```
Switch# request platform software package clean switch all
```

**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.

```
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.
```
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
  hexdump: stdin: Bad file descriptor
tail: cannot open 'NVRAM' for reading: No such file or directory
  hexdump: stdin: Bad file descriptor
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.
Upgrading the Switch Software

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

The following files will be deleted:
[1]:
_flash/cat9k-cc_srdriver.2017-07-26_17.04.SSA.pkg
_flash/cat9k-espbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-guestshell.2017-07-26_17.04.SSA.pkg
_flash/cat9k-rpbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-rpboot.2017-07-26_17.04.SSA.pkg
_flash/cat9k-sipbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-sipspa.2017-07-26_17.04.SSA.pkg
_flash/cat9k-srdriver.2017-07-26_17.04.SSA.pkg
_flash/cat9k-webui.2017-07-26_17.04.SSA.pkg
_flash/cat9k_iosxe.16.05.01a.SPA.conf
_flash/packages.conf.00-

[2]:
_flash/cat9k-cc_srdriver.2017-07-26_17.04.SSA.pkg
_flash/cat9k-espbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-guestshell.2017-07-26_17.04.SSA.pkg
_flash/cat9k-rpbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-rpboot.2017-07-26_17.04.SSA.pkg
_flash/cat9k-sipbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-sipspa.2017-07-26_17.04.SSA.pkg
_flash/cat9k-srdriver.2017-07-26_17.04.SSA.pkg
_flash/cat9k-webui.2017-07-26_17.04.SSA.pkg
_flash/cat9k_iosxe.16.05.01a.SPA.conf
_flash/packages.conf.00-

[3]:
_flash/cat9k-cc_srdriver.2017-07-26_17.04.SSA.pkg
_flash/cat9k-espbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-guestshell.2017-07-26_17.04.SSA.pkg
_flash/cat9k-rpbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-rpboot.2017-07-26_17.04.SSA.pkg
_flash/cat9k-sipbase.2017-07-26_17.04.SSA.pkg
_flash/cat9k-sipspa.2017-07-26_17.04.SSA.pkg
_flash/cat9k-srdriver.2017-07-26_17.04.SSA.pkg
_flash/cat9k-webui.2017-07-26_17.04.SSA.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.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:/cat9k-espbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:/cat9k-guestshell.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:/cat9k-rpbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:/cat9k-rpboot.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:/cat9k-sipbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:/cat9k-sipspa.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-srdriver.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-webui.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.

Deleting file flash:cat9k-cc_srdriver.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-espbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-guestshell.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-rpbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-rpboot.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-sipbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-sipspa.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-srdriver.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-webui.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.

Deleting file flash:cat9k-cc_srdriver.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-espbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-guestshell.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-rpbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-rpboot.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-sipbase.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-sipspa.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-srdriver.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-webui.2017-07-26_17.04.SSA.pkg ... done.
Deleting file flash:cat9k-iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.

You can also use the `install remove inactive` command to clean up old installation files in case of insufficient space. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.6.1 files:

```
Switch# install remove inactive
install_remove: START Mon Oct 30 19:51:48 UTC 2017
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.16.06.01.SPA.pkg
  /flash/cat9k-espbase.16.06.01.SPA.pkg
  /flash/cat9k-guestshell.16.06.01.SPA.pkg
  /flash/cat9k-rpbase.16.06.01.SPA.pkg
  /flash/cat9k-rpboot.16.06.01.SPA.pkg
  /flash/cat9k-sipbase.16.06.01.SPA.pkg
  /flash/cat9k-sipspa.16.06.01.SPA.pkg
  /flash/cat9k-srdriver.16.06.01.SPA.pkg
  /flash/cat9k-webui.16.06.01.SPA.pkg
  /flash/cat9k-wlc.16.06.01.SPA.pkg
  /flash/packages.conf

Do you want to remove the above files? [y/n] y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.01.SPA.pkg ... done.
```
Deleting file flash:cat9k-sipbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.06.01.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 Oct 30 19:52:25 UTC 2017
Switch#

Copy New Image to Flash

Step 2  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 - 601216545 bytes]
601216545 bytes copied in 50.649 secs (11870255 bytes/sec)

Use the dir flash 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 26 2017 10:18:11 -07:00 cat9k_iosxe.16.06.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)

Set Boot Variable

Step 3  Use the boot system flash:packages.conf command to set the boot variable.

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

Use the write memory command to save boot settings.

Switch# write memory

Use this command to verify BOOT variable = flash:packages.conf

Switch# show boot system

Software Install Image to Flash

Step 4  Use the request platform software package install switch all file flash: auto-copy command to install the target image 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.16.06.01.SPA.bin auto-copy
```

Expanding image file: flash-3: cat9k_iosxe.16.06.01.SPA.bin

```
[3]: Copying flash-3: cat9k_iosxe.16.06.01.SPA.bin from switch 3 to switch 1 2 4
```

The following example displays the installation of Cisco IOS XE Everest 16.6.1 software image:

Use the `switch all` option to upgrade all switches in your stack

Use the `auto-copy` option to copy the .bin image from flash: to all other switches in your stack

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.06.01.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.16.06.01.SPA.bin

[1]: Copying flash:cat9k_iosxe.16.06.01.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

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
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
Upgrading the Switch Software

You can also use the **install add file activate commit** command to install the target image to flash. This example displays the installation of Cisco IOS XE Everest 16.6.2:

```
Switch# install add file flash:cat9k_iosxe.16.06.02.SPA.bin activate commit
install_add_activate_commit: START Mon Oct 30 19:54:51 UTC 2017
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command.
[y/n/q] yBuilding configuration...
[OK] Modified configuration has been saved
```
Upgrading the Switch Software

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
After the software has been successfully installed, verify that the flash partition has nine new .pkg files and three .conf files. See sample output below. The following is sample output from the dir flash:

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

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

The following is sample output from the dir flash:

Switch# dir flash:
Directory of flash:/

253956  -rw-  2097152 Nov 3 2017 21:37:04 07:00 nvram_config
253955  -rw-  2097152 Nov 3 2017 21:37:04 07:00 nvram_config_bkup
253954  -rw- 239 Nov 3 2017 21:28:47 07:00 boothelper.log
253957  -rw-  752 Nov 3 2017 21:28:47 07:00 packages.conf
303110  -rw- 5297096 Nov 1 2017 23:27:26 07:00 cat9k-cc_srdriver.16.06.01.SPA.pkg
253961  -rw-  7523 Nov 1 2017 23:27:26 07:00 packages.conf
344067  -rw- 5186504 Nov 1 2017 23:27:26 07:00 cat9k-espbase.16.06.02.SPA.pkg
303111  -rw-  8094616 Nov 1 2017 23:27:26 07:00 cat9k-guestshell.16.06.01.SPA.pkg
303113  -rw- 376865728 Nov 1 2017 23:27:40 07:00 cat9k-rpbase.16.06.01.SPA.pkg
303118  -rw-  29545049 Nov 1 2017 23:27:53 07:00 cat9k-rpboot.16.06.01.SPA.pkg
303114  -rw- 55440320 Oct 30 2017 10:58:00 07:00 cat9k-sipbase.16.06.01.SPA.pkg
303115  -rw-  55440320 Nov 1 2017 23:27:43 07:00 cat9k-sipspa.16.06.01.SPA.pkg
294913 drwx  4096 Nov 3 2017 21:28:25 07:00 .installer
253966  -rw-  16280 Nov 3 2017 21:28:42 07:00 bootloader_evt.handle.log
303105 drwx  4096 Oct 26 2017 20:57:12 07:00 core
311297 drwx  4096 Nov 2 2017 23:41:45 07:00 .prst_sync
327681 drwx  4096 Nov 1 2017 23:56:42 07:00 .rollback_timer
335873 drwx  4096 Nov 3 2017 21:28:46 07:00 dc_profile_dir
335875 drwx  4096 Oct 26 2017 20:48:50 07:00 gs_script
253959  -rw-  556 Nov 2 2017 23:42:12 07:00 vlan.dat
253968  -rw- 98869 Nov 3 2017 21:28:59 07:00 memleak.tcl
294914 drwx  4096 Oct 26 2017 21:19:34 07:00 tech_support
303107 drwx  4096 Oct 26 2017 21:27:19 07:00 onep
319490 drwx  4096 Oct 26 2017 21:27:19 07:00 CRDU
303115  -rw- 55440320 Nov 1 2017 23:27:43 07:00 cat9k-sipspa.16.06.01.SPA.pkg
303116  -rw- 11813828 Nov 1 2017 23:27:43 07:00 cat9k-cc_srdriver.16.06.01.SPA.pkg

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Everest 16.6.x
Upgrading the Switch Software

In the following sample output that displays the .conf files in the flash partition, note the three .conf files:

- packages.conf — the file that has been re-written with the newly installed .pkg files
- packages.conf.00 — backup file of the previously installed image
- cat9k_iosxe.16.06.01.SPA.conf — a copy of packages.conf and not used by the system.

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

Reload

Step 6 Reload the switch
Switch# reload

Step 7 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

When the new image boots up, you can verify the version of the new image, using the show version command:

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

The following show version command output displays the Cisco IOS XE Everest 16.6.1 image on the device:

Switch# show version
Cisco OS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1, RELEASESOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 22-Jul-17 05:51 by mcpre
Upgrading the Switch Software

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

```
Switch# show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.2, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 28-Oct-17 06:38 by mcpre
```

Downgrading in Install Mode

**Note**

New switch models that are introduced in a release cannot be downgraded, so if you add a new switch to an existing stack, we recommend upgrading all existing switches. For the list of models introduced in a release, see the list of hardware features in that release.

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

The sample output in this section covers downgrade from Cisco IOS XE Everest 16.6.1 to Cisco IOS XE Everest 16.5.1a and from Cisco IOS XE Everest 16.6.2 to Cisco IOS XE Everest 16.6.1 in Install Mode.

This section provides examples of both `request platform software` and `install` commands.

**Summary Steps**—Clean Up > Copy New Image to Flash > Downgrade Software Image > Reload

Clean Up

**Step 1**

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. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.6.1 files:

```
Switch# request platform software package clean switch all
This operation may take several minutes...
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.16.06.01.SPA.pkg
    File is in use, will not delete.
    cat9k-espbase.16.06.01.SPA.pkg
    File is in use, will not delete.
    cat9k-guestshell.16.06.01.SPA.pkg
```

**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 an active or standby. In the sample output below, hexdump messages are seen on switch 3, which is a member switch.
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.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.06.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

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.16.06.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.06.01.SPA.pkg
File is in use, will not delete.

cat9k-guestshell.16.06.01.SPA.pkg
  File is in use, will not delete.
cat9k-rpbase.16.06.01.SPA.pkg
  File is in use, will not delete.
cat9k-rpboot.16.06.01.SPA.pkg
  File is in use, will not delete.
cat9k-sipbase.16.06.01.SPA.pkg
  File is in use, will not delete.
cat9k-sipspa.16.06.01.SPA.pkg
  File is in use, will not delete.
cat9k-srdriver.16.06.01.SPA.pkg
  File is in use, will not delete.
cat9k-webui.16.06.01.SPA.pkg
  File is in use, will not delete.
packages.conf
  File is in use, will not delete.
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.05.01a.SPA.pkg
/flash/cat9k-espbase.16.05.01a.SPA.pkg
/flash/cat9k-guestshell.16.05.01a.SPA.pkg
/flash/cat9k-rpbase.16.05.01a.SPA.pkg
/flash/cat9k-rpboot.16.05.01a.SPA.pkg
/flash/cat9k-sipbase.16.05.01a.SPA.pkg
/flash/cat9k-sipspa.16.05.01a.SPA.pkg
/flash/cat9k-srdriver.16.05.01a.SPA.pkg
/flash/cat9k-webui.16.05.01a.SPA.pkg
/flash/cat9k_iosxe.16.06.01.SPA.bin
/flash/cat9k_iosxe.16.06.01.SPA.conf
/flash/packages.conf.00-
[switch 2]:
/flash/cat9k-cc_srdriver.16.05.01a.SPA.pkg
/flash/cat9k-espbase.16.05.01a.SPA.pkg
/flash/cat9k-guestshell.16.05.01a.SPA.pkg
/flash/cat9k-rpbase.16.05.01a.SPA.pkg
/flash/cat9k-rpboot.16.05.01a.SPA.pkg
/flash/cat9k-sipbase.16.05.01a.SPA.pkg
/flash/cat9k-sipspa.16.05.01a.SPA.pkg
/flash/cat9k-srdriver.16.05.01a.SPA.pkg
/flash/cat9k-webui.16.05.01a.SPA.pkg
/flash/cat9k_iosxe.16.06.01.SPA.bin
/flash/cat9k_iosxe.16.06.01.SPA.conf
/flash/packages.conf.00-
[switch 3]:
/flash/cat9k-cc_srdriver.16.05.01a.SPA.pkg
/flash/cat9k-espbase.16.05.01a.SPA.pkg
/flash/cat9k-guestshell.16.05.01a.SPA.pkg
/flash/cat9k-rpbase.16.05.01a.SPA.pkg
/flash/cat9k-rpboot.16.05.01a.SPA.pkg
/flash/cat9k-sipbase.16.05.01a.SPA.pkg
/flash/cat9k-sipspa.16.05.01a.SPA.pkg
/flash/cat9k-srdriver.16.05.01a.SPA.pkg
/flash/cat9k-webui.16.05.01a.SPA.pkg
/flash/cat9k_iosxe.16.06.01.SPA.bin
/flash/cat9k_iosxe.16.06.01.SPA.conf
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[switch 1]:

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Everest 16.6.x
Deleting file flash:cat9k-cc_srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.bin ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.

[switch 2]:
Deleting file flash:cat9k-cc_srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.bin ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.

[switch 3]:
Deleting file flash:cat9k-cc_srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.05.01a.SPA.pkg ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.bin ... done.
Deleting file flash:cat9k-iosxe.16.06.01.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.

You can also use the install remove inactive command to clean up old installation files in case of insufficient space. The following sample output displays the cleaning up of Cisco IOS XE Everest 16.6.2 files:

Switch# install remove inactive
install_remove: START Mon Oct 30 19:51:48 UTC 2017
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.16.06.02.SPA.pkg
flash:/cat9k-espbase.16.06.02.SPA.pkg
flash:/cat9k-guestshell.16.06.02.SPA.pkg
flash:/cat9k-rpbase.16.06.02.SPA.pkg
flash:/cat9k-rpboot.16.06.02.SPA.pkg
flash:/cat9k-sipbase.16.06.02.SPA.pkg
Upgrading the Switch Software

Do you want to remove the above files? [y/n] y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.02.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.06.02.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 Oct 30 19:52:25 UTC 2017
Switch#

Copy New Image to Flash

Step 2  Copy the target Cisco IOS XE Everest 16.5.1a image to flash: (you can skip this step if you want to use the image from your TFTP server).

Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.05.01a.SPA.bin flash:
Destination filename [cat9k_iosxe.16.05.01a.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.05.01a.SPA.bin...
Loading /cat9k_iosxe.16.05.01a.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)

Step 3  Use the dir flash command to confirm that the image has been successfully copied to flash.

Switch# dir flash:/*.bin
Directory of flash:/
434184 -rw- 508584771 Jul 26 2017 13:35:16 -07:00 cat9k_iosxe.16.05.01a.SPA.bin
11353194496 bytes total (9055866880 bytes free)
Downgrade Software Image

Step 4 Use the request platform software package install command, to downgrade your stack. You can point to the source image on your tftp server or in flash if you have it copied to flash. The following example displays the installation of Cisco IOS XE Everest 16.5.1a software image:

Use the switch all option to upgrade all switches in your stack.

Use the auto-copy option to copy the .bin image from flash: to all the other switches in your stack.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.05.01a.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.16.05.01a.SPA.bin
[1]: Copying flash:cat9k_iosxe.16.05.01a.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.16.06.01.SPA.pkg
Removed cat9k-espbase.16.06.01.SPA.pkg
Removed cat9k-guestshell.16.06.01.SPA.pkg
Removed cat9k-rpbase.16.06.01.SPA.pkg
Removed cat9k-rpboot.16.06.01.SPA.pkg
Removed cat9k-sipbase.16.06.01.SPA.pkg
Removed cat9k-sipspa.16.06.01.SPA.pkg
Removed cat9k-srdriver.16.06.01.SPA.pkg
Removed cat9k-webui.16.06.01.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.05.01a.SPA.pkg
Added cat9k-espbase.16.05.01a.SPA.pkg
Added cat9k-guestshell.16.05.01a.SPA.pkg
Added cat9k-rpbase.16.05.01a.SPA.pkg
Added cat9k-rpboot.16.05.01a.SPA.pkg
Added cat9k-sipbase.16.05.01a.SPA.pkg
Added cat9k-sipspa.16.05.01a.SPA.pkg
Added cat9k-srdriver.16.05.01a.SPA.pkg
Added cat9k-webui.16.05.01a.SPA.pkg
Added cat9k-wlc.16.05.01a.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.16.06.01.SPA.pkg
Removed cat9k-espbase.16.06.01.SPA.pkg
Removed cat9k-guestshell.16.06.01.SPA.pkg
Removed cat9k-rpbase.16.06.01.SPA.pkg
Removed cat9k-rpboot.16.06.01.SPA.pkg
Removed cat9k-sipbase.16.06.01.SPA.pkg
Removed cat9k-sipspa.16.06.01.SPA.pkg
Removed cat9k-srdriver.16.06.01.SPA.pkg
Removed cat9k-webui.16.06.01.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.05.01a.SPA.pkg
```
Added cat9k-espbase.16.05.01a.SPA.pkg
Added cat9k-guestshell.16.05.01a.SPA.pkg
Added cat9k-rpbase.16.05.01a.SPA.pkg
Added cat9k-rpboot.16.05.01a.SPA.pkg
Added cat9k-sipbase.16.05.01a.SPA.pkg
Added cat9k-sipspe.16.05.01a.SPA.pkg
Added cat9k-srdriver.16.05.01a.SPA.pkg
Added cat9k-webui.16.05.01a.SPA.pkg
Added cat9k-wlc.16.05.01a.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.16.06.01.SPA.pkg
Removed cat9k-espbase.16.06.01.SPA.pkg
Removed cat9k-guestshell.16.06.01.SPA.pkg
Removed cat9k-rpbase.16.06.01.SPA.pkg
Removed cat9k-rpboot.16.06.01.SPA.pkg
Removed cat9k-sipbase.16.06.01.SPA.pkg
Removed cat9k-sipspe.16.06.01.SPA.pkg
Removed cat9k-srdriver.16.06.01.SPA.pkg
Removed cat9k-webui.16.06.01.SPA.pkg

New files list:
Added cat9k-cc_srdriver.16.05.01a.SPA.pkg
Added cat9k-espbase.16.05.01a.SPA.pkg
Added cat9k-guestshell.16.05.01a.SPA.pkg
Added cat9k-rpbase.16.05.01a.SPA.pkg
Added cat9k-rpboot.16.05.01a.SPA.pkg
Added cat9k-sipbase.16.05.01a.SPA.pkg
Added cat9k-sipspe.16.05.01a.SPA.pkg
Added cat9k-srdriver.16.05.01a.SPA.pkg
Added cat9k-webui.16.05.01a.SPA.pkg
Added cat9k-wlc.16.05.01a.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]

You can also use the **install add file activate commit** command to install the target image to flash. This example displays the installation of Cisco IOS XE Everest 16.6.1:

```
Switch# install add file flash:cat9k_iosxe.16.06.01.SPA.bin activate commit
install_add_activate_commit: START Mon Oct 30 19:54:51 UTC 2017
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
```

```
install_engine.sh: %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.01.SPA.bin install_add_activate_commit: Adding PACKAGE

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y
```
--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.05.01a.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.16.06.01.SPA.pkg
/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 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

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 Oct 30 19:57:48 UTC 2017

Switch#

--- Note ---
The system reloads automatically after executing the **install add file activate commit** command. There is no need to manually reload the system.
Reload

Step 5  Reload the switch

Switch# reload

Step 6  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.

When the new image boots up, you can verify the version of the new image, by checking the show version command.

The following show version command output displays the Cisco IOS XE Everest 16.5.1a image on the device:

Switch# show version
Cisco IOS XE Software, Version 16.05.01a
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.5.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Tue 30-May-17 00:36 by mcpre

The following show version command output 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 Sat 28-Oct-17 06:38 by mcpre

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 the 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—Require a Network Essentials or 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 http://www.cisco.com/go/cfn. 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—for a license level, preinstalled on the device, and for a 90-day trial period only.

Ordering with Smart Accounts

We recommend that you use Smart Accounts to order devices as well as licenses. Smart Accounts enable you to manage all of your software licenses for switches, routers, firewalls, access-points or tools from one centralized website. To create Smart Accounts, use the Cisco Smart Software Manager (Cisco SSM).

Note

This is especially relevant to the term licenses that you order, because information about the expiry of term licenses is available only through the Cisco SSM website.

For more information about Cisco SSM, see:

The possible deployment modes are:

- Right-to-use (RTU) licensing mode—Supported on Cisco Catalyst 9000 Series Switches. See The RTU Licensing Mode, page 37.
- Smart Licensing mode—Currently not supported on Cisco Catalyst 9000 Series Switches. It is on the roadmap for future releases.

The RTU Licensing Mode

This is the currently supported licensing mode for Cisco Catalyst 9000 Series Switches.

Right-to-use (RTU) licensing allows you to order and activate a specific license type for a given license level, and then to manage license usage on your switch.

Note

The RTU licensing structure has been modified to match the packaging model that will be used with Smart Licensing mode in the future. Unified licensing structures across the RTU and Smart Licensing modes, along with usage reports, will simplify migration and reduce the implementation time required for Smart Licensing.
The **license right-to-use** command (privilege EXEC mode) provides options to activate or deactivate any license supported on the platform.

**Options for Base Licenses**

```
license right-to-use [activate | deactivate] [network-essentials | network-advantage] [all | evaluation | subscription {all | slot <1-8>}] [acceptEULA]
```

**Options for Add-On Licenses**

```
license right-to-use [activate | deactivate] addon [dna-essentials | dna-advantage] [all | evaluation | subscription {all | slot <1-8>}] [acceptEULA]
```

**Usage Guidelines for the RTU Licensing Mode**

- Licenses may be activated on a standalone device, device stack, or a single device in a stack.
- Base licenses (Network Essentials and Network Advantage) may be ordered only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) may be ordered only with a term license type.

You can set up Cisco SSM to receive daily e-mail alerts, to be notified of expiring add-on licenses that you want to renew.

You must order an add-on license in order to purchase a switch. On term expiry, you can either renew the add-on license 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>
<thead>
<tr>
<th>Table 9</th>
<th>Permitted Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DNA Essentials</td>
</tr>
<tr>
<td>Network Essentials</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Advantage</td>
<td>Yes¹</td>
</tr>
</tbody>
</table>

1. For this combination, the DNA-Essentials license must be ordered separately using Cisco SSM.

- The following features are currently available only at the Network Advantage license level.

However, the correct minimum license level for these features is Network Essentials and the CFN reflects this correct license level.

You will be able to configure the features with a Network Essentials license level after the correction is made in an upcoming release.

- IPv6 Multicast
- IPv6 ACL Support for HTTP Servers
• Evaluation licenses cannot be ordered. They can be activated temporarily, without purchase. Warning system messages about the evaluation license expiry are generated 10 and 5 days before the 90-day window. Warning system messages are generated every day after the 90-day period. An expired evaluation license cannot be reactivated after reload.

For detailed configuration information about using the RTU Licensing Mode, see the System Management > Configuring Right-To-Use Licenses chapter of the software configuration guide for your software release:

Scaling Guidelines

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

Limitations and Restrictions

• Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.

• Control Plane Policing (CoPP)—Starting with Cisco IOS XE Everest 16.6.4, 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.

• Flexible NetFlow (FNF) 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 switched virtual interfaces (SVIs), port-channel, loopback, tunnels.
  – You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

• Hardware limitations:
  – For all the devices running Cisco IOS XE Everest 16.6.1 or Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3, autonegotiation is disabled by default when you use Cisco 40GBASE-CR4 QSFP Direct-Attach Copper Cables, If the other end of the link has autonegotiation enabled, the link does not come up.

  Note There is no option to turn on autonegotiation on the ports which connect to Cisco 40GBASE-CR4 QSFP cable.

  – For all the Catalyst 9300 Series Switches running Cisco IOS XE Everest 16.6.4 and later, autonegotiation is enabled by default when you use Cisco 40GBASE-CR4 QSFP Direct-Attach Copper Cables. If the other end of the link does not support autonegotiation, the link does not come up. You can turn autonegotiation off on the ports which connect to Cisco 40GBASE-CR4
QSFP cable. Use the `speed nonegotiate` command at the interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the `no speed nonegotiate` command.

- Interoperability limitations:
  - If one end of the link has a device running Cisco IOS XE Everest 16.6.1 or Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3 and the other end is running Cisco IOS XE Fuji 16.8.1, the link does not come up. To avoid this interoperability issue between releases, it is recommended to use the same image across all the Catalyst 9300 Series Switches and Catalyst 9500 Series Switches in the network.

- Memory leak—When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may fail. As a workaround, disable the logging discriminator on the device.

- QoS restrictions:
  - When configuring a QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only SVIs are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.

- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.
  - When the device is running SCP (Secure Copy Protocol) 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.

- Smart Install—The feature is deprecated starting with Cisco IOS XE Everest 16.5.1a. The commands are visible on the CLI until Cisco IOS XE Everest 16.6.1, but the feature is not supported. Enter the `no vstack` command in global configuration mode and disable the feature. Starting from Cisco IOS XE Everest 16.6.2, the `vstack` command is not available on the CLI.

- 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.
  - Auto upgrade for a new member switch is supported only in the install mode.

- 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 AVC 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 or 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 attributes based QoS is not supported (‘match protocol attribute’).
- 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 limitations—A maximum of 20 simultaneous NETCONF sessions are supported.
Caveats

Caveats describe unexpected behavior in Cisco IOS 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, page 42
- Open Caveats in Cisco IOS XE Everest 16.6.x, page 42
- Resolved Caveats in Cisco IOS XE Everest 16.6.5, page 44
- Resolved Caveats in Cisco IOS XE Everest 16.6.4a, page 46
- Resolved Caveats in Cisco IOS XE Everest 16.6.4, page 46
- Resolved Caveats in Cisco IOS XE Everest 16.6.3, page 48
- Resolved Caveats in Cisco IOS XE Everest 16.6.2, page 48
- Resolved Caveats in Cisco IOS XE Everest 16.6.1, page 49

Cisco Bug Search Tool

The 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 Everest 16.6.x

The following are the open caveats in this release.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvk60809</td>
<td>Wrong Time-Stamp is saved in pcap.</td>
</tr>
<tr>
<td>CSCvq13053</td>
<td>NAT translation entry not cleared after fin-rst time-out</td>
</tr>
<tr>
<td>CSCvq72713</td>
<td>Forwarding traffic can’t follow the rule of EIGRP unequal cost load-balancing</td>
</tr>
<tr>
<td>CSCvr21001</td>
<td>QoS with policing traffic that do not match the ACL on the class-map</td>
</tr>
<tr>
<td>CSCvr21641</td>
<td>Default command doesn't work for not connected port.</td>
</tr>
<tr>
<td>CSCvq13053</td>
<td>NAT translation entry not cleared after fin-rst time-out</td>
</tr>
<tr>
<td>CSCvh72186</td>
<td>ROMMON: HTTP booting does not allow specified port number</td>
</tr>
<tr>
<td>CSCvi36291</td>
<td>Incorrect budget allocated for StackPower</td>
</tr>
<tr>
<td>CSCvi56567</td>
<td>When 9300 switch boots up, link up of its down link has delayed if switch has network module</td>
</tr>
<tr>
<td>CSCvj82886</td>
<td>FNF export not working after second switchover when ETA+FNF is configured</td>
</tr>
</tbody>
</table>
## Resolved Caveats in Cisco IOS XE Everest 16.6.7

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvf42299</td>
<td>User defined System MTU is not taking effect on PO and SVI</td>
</tr>
<tr>
<td>CSCvj16691</td>
<td>Port LED may turn to amber</td>
</tr>
<tr>
<td>CSCvn30230</td>
<td>Slow memory leak in linux_iosd-img</td>
</tr>
<tr>
<td>CSCvn81334</td>
<td>Default ACL being enforced even when dACL is applied after Reload</td>
</tr>
<tr>
<td>CSCvo65974</td>
<td>QinQ tunnels causing L2 loop in specific topology.</td>
</tr>
<tr>
<td>CSCvo71264</td>
<td>Gateway routes DHCP offer incorrectly after DHCP snooping</td>
</tr>
<tr>
<td>CSCvo83305</td>
<td>MAC Access List Blocks Unintended Traffic</td>
</tr>
<tr>
<td>CSCvo85183</td>
<td>Uplinkfast take time when recovery from link failure</td>
</tr>
<tr>
<td>CSCvo85422</td>
<td>Directly connected IPv4/IPv6 hosts not programmed in HW - %FMFP-3-OBJ_DWNLD_TO_DP_FAILED</td>
</tr>
<tr>
<td>CSCvo94058</td>
<td>URPF packet drop despite &quot;rx allow-default&quot; option</td>
</tr>
<tr>
<td>CSCvp00026</td>
<td>No audio during first few seconds of voice call between 2 Fabric Edge</td>
</tr>
<tr>
<td>CSCvp05090</td>
<td>Shutdown one port will cause other port flap</td>
</tr>
<tr>
<td>CSCvp15389</td>
<td>Port security configuration on interface causing connectivity issue</td>
</tr>
<tr>
<td>CSCvp26792</td>
<td>Control plane impacted when &gt; 1Gbps multicast passes through and no entry in IGMP snooping</td>
</tr>
<tr>
<td>CSCvp30239</td>
<td>Memory leak when there are constant changes in REP ring</td>
</tr>
<tr>
<td>CSCvp33294</td>
<td>Asic 0 Core 0 buffer stuck, rwePbcStall seen</td>
</tr>
<tr>
<td>CSCvp37754</td>
<td>Non mgig - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones</td>
</tr>
<tr>
<td>CSCvp43131</td>
<td>Mgmt port &quot;speed 1000&quot; and &quot;negotiation auto&quot; in show run</td>
</tr>
<tr>
<td>CSCvp54779</td>
<td>[SDA] 1st ARP Reply is dropped at remote Fabric Edge</td>
</tr>
<tr>
<td>CSCvp69629</td>
<td>Authentication sessions does not come up on configuring dot1x when there is active client traffic.</td>
</tr>
<tr>
<td>CSCvp75221</td>
<td>Modules shows faulty status when specific MAC ACL is applied on interfaces</td>
</tr>
<tr>
<td>CSCvp89755</td>
<td>VPN label is wrongly derived as explicit-null in Cat9k for L3 VPN traffic</td>
</tr>
<tr>
<td>CSCvp90279</td>
<td>ADV and REP DHCPv6 packets are sent to SISF when source udp port is not 547</td>
</tr>
<tr>
<td>CSCvp01185</td>
<td>SNMP-3-RESPONSE_DELAYED: and timeout when polling ent Sensor Value Entry</td>
</tr>
<tr>
<td>CSCvp22011</td>
<td>ARP replies are dropped when IPDT gleans from ARP</td>
</tr>
<tr>
<td>CSCvp30316</td>
<td>[SDA] 1st ARP fix for CSCvp00026 is eventually failing after longevity</td>
</tr>
<tr>
<td>CSCvp30460</td>
<td>SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn</td>
</tr>
<tr>
<td>CSCvp40137</td>
<td>Mac address not being learnt when &quot;auth port-control auto&quot; command is present</td>
</tr>
<tr>
<td>CSCvp44397</td>
<td>ospf down upon switchover with aggressive timers &quot;hello-interval 1&quot; and &quot;dead-interval 4&quot;</td>
</tr>
</tbody>
</table>
Resolved Caveats in Cisco IOS XE Everest 16.6.6

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvn08296</td>
<td>DNA Center 1.2.5 - SDA Border as RP incorrectly resolving RPF next-hop as LISP interface</td>
</tr>
<tr>
<td>CSCvo32446</td>
<td>High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped</td>
</tr>
<tr>
<td>CSCuw36080</td>
<td>SNMP with Extended ACL</td>
</tr>
<tr>
<td>CSCvg73991</td>
<td>PBR adjacency not getting updated correctly after shut/no shut on interface</td>
</tr>
<tr>
<td>CSCvm07353</td>
<td>Router may crash when a SSH session is closed after configure TACACS</td>
</tr>
<tr>
<td>CSCvm48084</td>
<td>Remark in DACL causes Authorization failure</td>
</tr>
<tr>
<td>CSCvm77197</td>
<td>C9300/9500:%IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:</td>
</tr>
<tr>
<td>CSCvm89086</td>
<td>SPAN destination interface not dropping ingress traffic</td>
</tr>
<tr>
<td>CSCvn01822</td>
<td>cmnMacMoveNotification is generated when a MAC address is moved between same Port-channel interface</td>
</tr>
<tr>
<td>CSCvn23706</td>
<td>no mac address-table notification mac-move can't be saved after reload device</td>
</tr>
<tr>
<td>CSCvn31477</td>
<td>Layer 2 SSM Multicast traffic hitting the CPU when SVI is configured with PIM Spare Mode</td>
</tr>
<tr>
<td>CSCvn46517</td>
<td>some sg acl were not installed after update a Cell in ISE</td>
</tr>
<tr>
<td>CSCvn56579</td>
<td>MQIPC memory corruption resulting dot1x/MAB not working for wired clients</td>
</tr>
<tr>
<td>CSCvn72973</td>
<td>Device is getting crashed on the &quot;cts role-based enforcement&quot;</td>
</tr>
<tr>
<td>CSCvn74807</td>
<td>Cisco TrustSec crash while processing CoA update</td>
</tr>
<tr>
<td>CSCvn79221</td>
<td>MAC ADDRESS LEARNING FAILURE ON PORT CONFIGURED WITH PORT-SECURITY</td>
</tr>
<tr>
<td>CSCvn97961</td>
<td>9300 Mgig port 5 - Interface don't come UP and Can't read port related CLI</td>
</tr>
<tr>
<td>CSCvo15594</td>
<td>MATM programming issue for remote client</td>
</tr>
<tr>
<td>CSCvo40004</td>
<td>C9300-48P</td>
</tr>
<tr>
<td>CSCvo42353</td>
<td>SDA; Cat3K,Cat9K:-External border creating incorrect CEF/map-cache entry due to multicast</td>
</tr>
<tr>
<td>CSCvo59504</td>
<td>Cat3K</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.5

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvh88885</td>
<td>IPv6 stale entries not expiring</td>
</tr>
<tr>
<td>CSCvi48988</td>
<td>SNMP timeout when querying entSensorValueEntry</td>
</tr>
<tr>
<td>CSCvi81569</td>
<td>FNF is not exporting after reload when ETA + FNF enabled on interface</td>
</tr>
<tr>
<td>CSCvi96965</td>
<td>Radius Automate Tester probe on feature is not working as expected.</td>
</tr>
<tr>
<td>CSCvj79694</td>
<td>sgt-map gets cleared for some of the end points for unknown reason</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCvj92201</td>
<td>16.6.4: Device-tracking does not consistently show DH4 for DHCP clients</td>
</tr>
<tr>
<td>CSCvk20003</td>
<td>Polaris: Host limit of 32 for session monitoring sessions</td>
</tr>
<tr>
<td>CSCvk30813</td>
<td>MAB fails to start negotiation after device moves to another layer 2 adjacent switch</td>
</tr>
<tr>
<td>CSCvk32866</td>
<td>SISF probing behavior should be changed from broadcast to unicast</td>
</tr>
<tr>
<td>CSCvk33624</td>
<td>SFF8472-3-READ_ERROR message seen for SVL ports</td>
</tr>
<tr>
<td>CSCvk34927</td>
<td>DHCP snooping table not updated from DHCP snooping DB file upon reload.</td>
</tr>
<tr>
<td>CSCvk39041</td>
<td>SDA: IP phone latency in fabric is close to 4 sec's</td>
</tr>
<tr>
<td>CSCvk60752</td>
<td>DHCP offer with Option 82 but no Remote ID suboption dropped by CAT9K relay agent</td>
</tr>
<tr>
<td>CSCvk63089</td>
<td>show logging onboard switch active uptime detail shows 133 years as uptime</td>
</tr>
<tr>
<td>CSCvm00765</td>
<td>BFD crash on imitating traffic loss</td>
</tr>
<tr>
<td>CSCvm07921</td>
<td>OOB TX path excessive congestion cause software to force crash a switch</td>
</tr>
<tr>
<td>CSCvm33622</td>
<td>WCCP redirection to proxy server breaks in certain scenarios.</td>
</tr>
<tr>
<td>CSCvm35904</td>
<td>16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP</td>
</tr>
<tr>
<td>CSCvm36333</td>
<td>MAC address programming issue</td>
</tr>
<tr>
<td>CSCvm39894</td>
<td>False authorizations and authentications even without radius server for dot1x/mab</td>
</tr>
<tr>
<td>CSCvm43071</td>
<td>[IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list</td>
</tr>
<tr>
<td>CSCvm46814</td>
<td>session management process smd crash at cts_sga due to TDL memory depletion.</td>
</tr>
<tr>
<td>CSCvm60720</td>
<td>Broadcast Gratuitous ARP changed to unicast by switch leading to DHCP decline from client</td>
</tr>
<tr>
<td>CSCvm62274</td>
<td>Multicast traffic is software switched when switch is provisioned as Edge in Fabric - SDA Deployment</td>
</tr>
<tr>
<td>CSCvm63651</td>
<td>Memory leak due to authentication mac-move permit</td>
</tr>
<tr>
<td>CSCvm75378</td>
<td>Cat9x00: IPv6 SPAN filter still applied in hardware when removing entire monitor session</td>
</tr>
<tr>
<td>CSCvm86135</td>
<td>SMD crash after removing access-session attributes filter-list</td>
</tr>
<tr>
<td>CSCvm89005</td>
<td>Packets looped internally during VXLAN decap in SD-Access environment</td>
</tr>
<tr>
<td>CSCvm95352</td>
<td>uRPF TCAM Resources exhausted even without uRPF configured on the switch</td>
</tr>
<tr>
<td>CSCvm97660</td>
<td>C9300 reflects back traffic on the same interface</td>
</tr>
<tr>
<td>CSCvn08672</td>
<td>DHCP packets cause unknown protocol drops on 16.6.x</td>
</tr>
<tr>
<td>CSCvn36398</td>
<td>WCCP Access-list might not be removed from interface after a WCCP loss of service</td>
</tr>
<tr>
<td>CSCvn46171</td>
<td>Rapid Memory Leak in &quot;FED Main Event&quot; Process due to Modifying Adjacencies</td>
</tr>
</tbody>
</table>
Resolved Caveats in Cisco IOS XE Everest 16.6.4a

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvj83551</td>
<td>SISF crash in IPV6 neighbor discovery packets</td>
</tr>
<tr>
<td>CSCvm09611</td>
<td>C9x00 crashed with multicast memory corruption.</td>
</tr>
<tr>
<td>CSCvk32774</td>
<td>ACE entry with *established or range * in ACL drops TCP/UDP packets.</td>
</tr>
<tr>
<td>CSCvk31115</td>
<td>Device-sensor doesn't send data off initial boot</td>
</tr>
<tr>
<td>CSCvj86644</td>
<td>SDA: DHCP does not remove option 82 when sending packets to end-hosts</td>
</tr>
<tr>
<td>CSCvk02589</td>
<td>Connectivity is lost every four hours when ipv4 and ipv6 dual stack is configured.</td>
</tr>
<tr>
<td>CSCvf81710</td>
<td>C9300 fan curve hysteresis and oscillation</td>
</tr>
<tr>
<td>CSCvi49725</td>
<td>C9300: Group of 4 ports stop forwarding traffic</td>
</tr>
<tr>
<td>CSCvi90160</td>
<td>Incremental Rx bytes Counter increase while ports inactive</td>
</tr>
<tr>
<td>CSCvk08304</td>
<td>Slowness for x11perf with MGig port on 9300</td>
</tr>
<tr>
<td>CSCvk18900</td>
<td>Multiple LRM modules in C9300-NM-8X result in link drop</td>
</tr>
<tr>
<td>CSCvk39041</td>
<td>SDA: IP phone latency in fabric is close to 4 sec's</td>
</tr>
<tr>
<td>CSCvk60752</td>
<td>DHCP offer with Option 82 but no Remote ID suboption dropped by CAT9K relay agent</td>
</tr>
<tr>
<td>CSCvm35904</td>
<td>16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP</td>
</tr>
<tr>
<td>CSCvj33865</td>
<td>Clearing mac address table should not delete entries created by control plane/remote entries</td>
</tr>
<tr>
<td>CSCvk07070</td>
<td>Observing bmalloc smd leaks at OBJ_WEBAUTH_LOGOUT_URL with webauth</td>
</tr>
<tr>
<td>CSCvk16813</td>
<td>DHCP client traffic dropped with DHCP snooping and port-channel or cross stack uplinks.</td>
</tr>
<tr>
<td>CSCvk46664</td>
<td>DNA Center SWIM Upgrade fails and unable to upgrade manually</td>
</tr>
<tr>
<td>CSCvk50734</td>
<td>Device Tracking - Memory leak observed with IPv6 NS/NA Packets.</td>
</tr>
<tr>
<td>CSCvk53444</td>
<td>Packets with Fragment Offset not forwarded with DHCP Snooping Enabled in 16.6.4</td>
</tr>
<tr>
<td>CSCvm09121</td>
<td>Evaluation of IOS-XE for CVE-2018-5391 (FragmentSmack)</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.4

The following are the resolved caveats in Cisco IOS XE Everest 16.6.4.

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvk00115</td>
<td>Ulink FRU module hardware authentication failed</td>
</tr>
<tr>
<td>CSCvi69699</td>
<td>9400 - 9300: 40G copper QSFP interoperability broken (link down)</td>
</tr>
<tr>
<td>CSCvi83373</td>
<td>Repetitive logs show up 47K times in fed tracelogs</td>
</tr>
<tr>
<td>CSCvj52681</td>
<td>dynamic vlan assignment causes all sisf entries under the port to be deleted</td>
</tr>
<tr>
<td>Caveat ID Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCvi91714</td>
<td>IPv6 address not assigned or delayed when RA Guard is enabled</td>
</tr>
<tr>
<td>CSCvi76084</td>
<td>Device-tracking entry stuck in TENTATIVE for certain Mac Pro hosts configured with static IP</td>
</tr>
<tr>
<td>CSCvi38916</td>
<td>Persistent Telnet and SSH crashes when configured in 16.6.2</td>
</tr>
<tr>
<td>CSCvi26398</td>
<td>&quot;%LISP-4-LOCAL_EID_RLOC_INCONSISTENCY&quot; should be suppressed in SDA context</td>
</tr>
<tr>
<td>CSCvi20882</td>
<td>Netconf IP-SLA udp-jitter case missing leaf codec</td>
</tr>
<tr>
<td>CSCvi11970</td>
<td>Abnormal output for show pnp tech-support</td>
</tr>
<tr>
<td>CSCvh85772</td>
<td>Switch not responding to ARP request for GW Anycast IP</td>
</tr>
<tr>
<td>CSCvh79942</td>
<td>Chunk corruption crash related to PNP or Guestshell</td>
</tr>
<tr>
<td>CSCvh21909</td>
<td>LISP: Overlapping prefix causes &quot;probe-down&quot; for map-cache entry</td>
</tr>
<tr>
<td>CSCvh09334</td>
<td>SDA-IPV6::SISF traceback @ar_relay_create_entry - L2 Binding tbl entry insertion failed</td>
</tr>
<tr>
<td>CSCvg45950</td>
<td>packet drop seen intermittently if 40G traffic sent via cts interface</td>
</tr>
<tr>
<td>CSCvb69966</td>
<td>Memory leak under LLDP Protocol process</td>
</tr>
<tr>
<td>CSCvg41950</td>
<td>Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability</td>
</tr>
<tr>
<td>CSCvg53159</td>
<td>%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch</td>
</tr>
<tr>
<td>CSCvg71118</td>
<td>Dot1x configuration on AP Trunk Ports causes unreachability</td>
</tr>
<tr>
<td>CSCvg95580</td>
<td>interface speed config went lost after same FRU OIR with &quot;write mem&quot;</td>
</tr>
<tr>
<td>CSCvh11396</td>
<td>Switchport Security Command triggering Bulk Sync Failure</td>
</tr>
<tr>
<td>CSCvh48397</td>
<td>create_directory_cache: failed to stat flash message see when device managed by dnac</td>
</tr>
<tr>
<td>CSCvh49334</td>
<td>Cat9300 stops forwarding multicast - L3M Failed to allocate REP RI</td>
</tr>
<tr>
<td>CSCvh52059</td>
<td>SFP-GE-T 100M full link is half duplex after reinserting SFP</td>
</tr>
<tr>
<td>CSCvh71539</td>
<td>Command &quot;show aaa servers&quot; reloads the switch</td>
</tr>
<tr>
<td>CSCvh84345</td>
<td>IOS CLI &quot;show platform software fed switch active punt cause summary&quot; may display negative counts</td>
</tr>
<tr>
<td>CSCvh87131</td>
<td>TRACEBACK: OID cefcModuleEntry crashes the box</td>
</tr>
<tr>
<td>CSCvi08459</td>
<td>Set different words for username and password, but username shown the same as password</td>
</tr>
<tr>
<td>CSCvi19809</td>
<td>Memory leak in TMS process</td>
</tr>
<tr>
<td>CSCvi26179</td>
<td>Cat9k crash while accessing OBFL</td>
</tr>
<tr>
<td>CSCvi38191</td>
<td>Memory leak in lman process due to &quot;ld_license_ext.dat&quot; build-up.</td>
</tr>
<tr>
<td>CSCvi39202</td>
<td>DHCP fails when DHCP snooping trust is enabled on uplink etherchannel</td>
</tr>
<tr>
<td>CSCvi48995</td>
<td>On mGig SKU (downlink ports) - Link down with forced speed100/full duplex on both ends</td>
</tr>
<tr>
<td>CSCvi69699</td>
<td>9400 - 9300: 40G copper QSFP interoperability broken (link down)</td>
</tr>
<tr>
<td>CSCvi70528</td>
<td>Cat9K- 40G QSFP Tx/Rx power out of valid range</td>
</tr>
</tbody>
</table>
Caveats

Resolved Caveats in Cisco IOS XE Everest 16.6.3

The following are the resolved caveats in Cisco IOS XE Everest 16.6.3.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvg71134</td>
<td>Cannot transmit more than 400 Bytes on mGig ports going to Intel NIC.</td>
</tr>
<tr>
<td>CSCvg63006</td>
<td>No traffic seen for SFP-10G-SR/QSA.</td>
</tr>
<tr>
<td>CSCvh31431</td>
<td>Memory leak in linux_iosd-image on 16.6 releases.</td>
</tr>
<tr>
<td>CSCvh52882</td>
<td>Memory Leak due to nbar config.</td>
</tr>
<tr>
<td>CSCvh69402</td>
<td>Dot1x specific configuration applied but not working on the interface.</td>
</tr>
<tr>
<td>CSCvh81152</td>
<td>Local SVI IP is registered as dynamic-eid.</td>
</tr>
<tr>
<td>CSCvh06383</td>
<td>16.6.x: Intermittent traffic loss for MAB devices after successful intial authentication.</td>
</tr>
<tr>
<td>CSCvh04282</td>
<td>Cat9300 non-default system MTU config value is not respected after reload.</td>
</tr>
<tr>
<td>CSCvh18282</td>
<td>Interface up is slow on Standby(Member) after Stand(Mem) reload or redundancy force-switchover on ACT.</td>
</tr>
<tr>
<td>CSCvh27460</td>
<td>SPAN destination port forward traffic.</td>
</tr>
<tr>
<td>CSCvg56727</td>
<td>Crashes with 'server-key' command using key of 128 characters or more.</td>
</tr>
<tr>
<td>CSCve32330</td>
<td>%UTIL-6-RANDOM: A pseudo-random number was generated twice in succession.</td>
</tr>
<tr>
<td>CSCvg22515</td>
<td>After upgrade of IOS, SSH passwords longer than 25 characters do not work.</td>
</tr>
<tr>
<td>CSCvg60288</td>
<td>Device IP address AV pair replaced with 192.168.1.5.</td>
</tr>
<tr>
<td>CSCvg92736</td>
<td>Incorrect RPF failure for default MDT packets result in missing VRF PIM neighbors.</td>
</tr>
<tr>
<td>CSCvh32416</td>
<td>Evaluation of all for CPU Side-Channel Information Disclosure Vulnerability.</td>
</tr>
<tr>
<td>CSCvh55578</td>
<td>To add recovery mechanism for glean entry.</td>
</tr>
<tr>
<td>CSCvf84349</td>
<td>Router crash on polling cEigrpPeerEntry.</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.2

The following are the resolved caveats in Cisco IOS XE Everest 16.6.2.
The following are the resolved caveats in Cisco IOS XE Everest 16.6.1.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvd89966</td>
<td>Device does not get power upon toggling power inline setting from never to auto.</td>
</tr>
<tr>
<td>CSCvf40147</td>
<td>Catalyst 9300: ASIC Ballot failed message seen on during bootup in overnight reload test.</td>
</tr>
<tr>
<td>CSCvf67024</td>
<td>PID for &quot;c9xxx Stack&quot; changes after reboots.</td>
</tr>
<tr>
<td>CSCvf67030</td>
<td>Gi0/0 is operationally down after upgrade from Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Everest 16.6.1.</td>
</tr>
<tr>
<td>CSCvf73553</td>
<td>Catalyst 9k crash after executing the <code>factory-reset all</code> CLI.</td>
</tr>
<tr>
<td>CSCvf75518</td>
<td>Controller port error interface.</td>
</tr>
<tr>
<td>CSCvf75880</td>
<td>File size gets doubled after copy is done from FTP/USB to flash memory.</td>
</tr>
<tr>
<td>CSCvf32705</td>
<td>Exports stop working upon disable enable ETA on the second interface.</td>
</tr>
</tbody>
</table>

Resolved Caveats in Cisco IOS XE Everest 16.6.1

The following are the resolved caveats in Cisco IOS XE Everest 16.6.1.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvd84135</td>
<td>9300-webUI: 8x10G NM is not displayed correctly in the switch view page</td>
</tr>
</tbody>
</table>

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL: http://www.cisco.com/en/US/support/index.html

Choose Product Support > Switches. Then choose your product and click Troubleshoot and Alerts to find information for the problem that you are experiencing.
Related Documentation

- Cisco Catalyst 9300 Series Switches documentation at this URL:
  http://www.cisco.com/go/c9300
- Cisco IOS XE 16 documentation at this URL:
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes at this URL:
- Cisco Validated Designs documents at this URL:
  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation, which lists all new and revised Cisco Technical documentation, as an RSS feed and deliver content directly to your desktop using a read application. The RSS feeds are a free service.

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: www.cisco.com/go/trademarks. 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)

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.

© 2019 Cisco Systems, Inc. All rights reserved.