Release Notes for Catalyst 3850 Series Switch, Cisco IOS XE Everest 16.4.1

First Published: November 30, 2016

This release note gives an overview of the features for the Cisco IOS XE Everest 16.4.1 software on the Cisco Catalyst 3850 Series Switches.

Unless otherwise noted, the terms *switch* and *device* refer to a standalone switch and to a switch stack.

Note
- For information about unsupported features, see Important Notes, page 2.
- For information about software and hardware restrictions and limitations, see Limitations and Restrictions, page 27.
- For information about open issues with the software and past opens that are resolved now, see Caveats, page 28.

Introduction

Cisco Catalyst 3850 Series Switches are the next generation of enterprise class stackable access layer switches that provide full convergence between wired and wireless networks on a single platform. This convergence is built on the resilience of new and improved 480-Gbps StackWise-480 and Cisco StackPower. Wired and wireless security and wireless application visibility and control are natively built into the switch.

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

Whats New in Cisco IOS XE Everest 16.4.1

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

Important Notes

- Starting with Cisco IOS XE Denali 16.3.x, Secure Shell (SSH) Version 1 is deprecated. Use SSH Version 2 instead.
- Although visible in the CLI, the following commands are not supported:
  - **collect flow username**
  - **authorize-lsc-ap** (CSCui93659)
- The following features available in Cisco IOS XE Release 3.7.3E, are not supported in Cisco IOS XE Everest 16.4.1:
  - Cisco Plug-In for OpenFlow (OpenFlow 1.0 and 1.3)
- The following feature is available in Cisco IOS XE Release 3.6.3E, but is not supported in Cisco IOS XE Everest 16.4.1:
  - Cisco Discovery Protocol (CDP) Bypass
- The following features are not supported in Cisco IOS XE Everest 16.4.1:
  - IP-in-IP (IPIP) Tunneling
  - Mesh, FlexConnect, and OfficeExtend access point deployment
  - Wireless Guest Anchor Controller (Cisco Catalyst 3850 Series Switches can be configured as a foreign controller.)
  - DVMRP Tunneling
  - Port Security on EtherChannel
  - 802.1x Configurable username and password for MAB
  - IEEE 802.1X-2010 with 802.1AE support
  - Command Switch Redundancy
  - CNS Config Agent
  - Dynamic Access Ports
  - IPv6 Ready Logo phase II - Host
  - IPv6 IKEv2 / IPSecv3
  - Fallback bridging for non-IP traffic
  - DHCP snooping ASCII circuit ID
  - Protocol Storm Protection

- Per VLAN Policy & Per Port Policer
- Packet Based Storm Control
- Ingress/egress Shared Queues
- Trust Boundary Configuration
- Cisco Group Management Protocol (CGMP)
- Device classifier for ASP
- IPSLA Media Operation
- Passive Monitoring
- Performance Monitor (Phase 1)
- AAA: TACACS over IPv6 Transport
- Auto QoS for Video endpoints
- EX SFP Support (GLC-EX-SMD)
- IPv6 Strict Host Mode Support
- IPv6 Static Route support on LAN Base images
- VACL Logging of access denied
- RFC5460 DHCPv6 Bulk Leasequery
- DHCPv6 Relay Source Configuration
- RFC 4293 IP-MIB (IPv6 only)
- RFC 4292 IP-FORWARD-MIB (IPv6 only)
- RFC4292/RFC4293 MIBs for IPv6 traffic
- Layer 2 Tunneling Protocol Enhancements
- UniDirectional Link Routing (UDLR)
- Pragmatic General Multicast (PGM)
- DAI, IPSG Interoperability
- Ingress Strict Priority Queuing (Expedite)
- Weighted Random Early Detect (WRED)
- Improvements in QoS policing rates
- Fast SSID support for guest access WLANs

Supported Hardware

Catalyst 3850 Switch Models

Table 1 Catalyst 3850 Switch Models

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

Table 1 Catalyst 3850 Switch Models (continued)

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

Table 1 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-48T-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-24P-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48P-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48F-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set
WS-C3850-24U-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
WS-C3850-48U-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
WS-C3850-12S-E	IP Services	12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-E	IP Services	24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-E	IP Services	Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 -W power supply
WS-C3850-16XS-E	IP Services	Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.
WS-C3850-24XS-E	IP Services	Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply
WS-C3850-32XS-E	IP Services	Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-E switch

Table 1 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-12X48U-E	IP Services	Stackable 12 100M/1G/2.5G/5G/10G and 36 1 G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-E	IP Services	Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-48XS-E	IP Services	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750 WAC front-to-back power supply. 1 RU.
WS-C3850-48XS-F-E	IP Services	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC back-to-front power supply. 1 RU.

Network Modules

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

Table 2 Supported Network Modules

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

Table 2 Supported Network Modules (continued)

Network Module	Description
C3850-NM-8-10G	This module has eight 10 G slots with an SFP+ port in each slot. Each port supports a 1 G or 10 G connection **Note** This is supported on the following switch models: – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-24XS
C3850-NM-2-40G	This module has two 40 G slots with a QSFP+ connector in each slot. **Note** This is supported on the following switch models: – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-24XS

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:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Access Points and Connected Mobile Experiences (CMX)

Table 3 lists the supported products of the Catalyst 3850 Switch.

Note Telnet is not supported on Cisco 1800 Series APs

Table 3 Catalyst 3850 Switch Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 1810W, 1830, 1850, 2600, 2700, 2800, 3500, 3600, 3700, 3800
Mobility Services Engine	3365, Virtual Appliance

Table 4 lists the specific supported Cisco access points.

Table 4 Supported Access Points

Access Points	
Cisco Aironet 700 Series	AIR-CAP702I-x-K9
Cisco Aironet 700W Series	AIR-CAP702Wx-K9

Table 4 Supported Access Points (continued)

Access Points	
Cisco Aironet 1040 Series	AIR-AP1041N
	AIR-AP1042N
	AIR-LAP1041N
	AIR-LAP1042N
Cisco Aironet 1140 Series	AIR-AP1141N
	AIR-AP1142N
	AIR-LAP1141N
	AIR-LAP1142N
Cisco Aironet 1260 Series	AIR-LAP1261N
	AIR-LAP1262N
	AIR-AP1261N
	AIR-AP1262N
Cisco Aironet 1530 Series	AIR-CAP1532I-x-K9
	AIR-CAP1532E-x-K9
Cisco Aironet 1570 Series	AIR-AP1572EAC-A-K9
	AIR-AP1572ECx-A-K9
	AIR-AP1572ICx-A-K9
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 1700 Series	AIR-CAP1702I-x-K9
Cisco Aironet 1810W Series	AIR-AP1810w-x-K9
Cisco Aironet 1830 Series	AIR-AP1832I-UXK9
	AIR-AP1832I-UXK9C
	AIR-AP1832I-x-K9
	AIR-AP1832I-x-K9C
Cisco Aironet 1850 Series	AIR-AP1852I-UXK9
	AIR-AP1852I-UXK9C
	AIR-AP1852E-UXK9
	AIR-AP1852E-UXK9C
	AIR-AP1852E-x-K9
	AIR-AP1852E-x-K9C
	AIR-AP1852I-x-K9
	AIR-AP1852I-x-K9C
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I

Table 4 Supported Access Points (continued)

Access Points	
Cisco Aironet 2700 Series	AIR-CAP2702I-x-K9
	AIR-CAP2702E-x-K9
Cisco Aironet 2800 Series	AIR-AP2802I-x-K9
	AIR-AP2802E-x-K9
Cisco Aironet 3500 Series	AIR-CAP3501E
	AIR-CAP3501I
	AIR-CAP3501P
	AIR-CAP3502E
	AIR-CAP3502I
	AIR-CAP3502P
Cisco Aironet 3600 Series Modules Supported: • AIR-RM3000AC-x-K9= • AIR-RM3000M= • AIR-RM3010L-x-K9= with AIR-ANT-LOC-01=	AIR-CAP3602E
	AIR-CAP3602I
Cisco Aironet 3700 Series Modules supported: • AIR-RM3000M= • AIR-RM3010L-x-K9= with AIR-ANT-LOC-01=	AIR-CAP3702I
	AIR-CAP3702E
	AIR-CAP3702P
Cisco Aironet 3800 Series	AIR-AP3802I-x-K9
	AIR-AP3802E-x-K9

Compatibility Matrix

Table 5 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
Everest 16.4.1	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.1 Patch 1 (Wired and Wireless)	5.4 5.5	-
Denali 16.3.2	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.1 Patch 1 (Wired and Wireless)	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack[1] (Wired and Wireless). See Prime Infrastructure 3.1 on cisco.com.
Denali 16.3.1	03.07.04E 03.06.05E	8.2.0, 8.3.0	CMX 10.2.2	2.0 Patch 3 1.4 Patch 7 1.3 Patch 6 (Wired and Wireless)	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack[1] (Wired and Wireless). See Prime Infrastructure 3.1 on cisco.com.
Denali 16.2.2	03.07.03E 03.06.03E[3]	8.1.0, 8.2.0	CMX 10.2.2	1.3 Patch 5 (Wired and Wireless)	5.3 5.4	3.1.0 + Device Pack 1 (Wired and Wireless)
Denali 16.2.1	03.07.03E 03.06.03E[3]	8.1.0, 8.2.0	CMX 10.2.2	1.3 Patch 5 (Wired and Wireless)	5.3 5.4	3.1.0 (Wired) 3.1.0, 3.0.2[2] + Device Pack 4 + PI 3.0 Technology Pack (Wireless)
Denali 16.1.3	03.07.02E 03.06.03E[3]	8.1.0	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + Device Pack 5+ PI 3.0 Technology Pack
Denali 16.1.2	03.07.02E 03.06.03E[3]	8.1.0	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + Device Pack 4 + PI 3.0 Technology Pack
Denali 16.1.1	03.07.02E 03.06.03E[3]	8.1.0	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + PI 3.0 Device Pack 2 + PI 3.0 Technology Pack
03.07.03E 03.07.02E 03.07.01E 03.07.00E	03.07.03E 03.07.02E 03.07.01E 03.07.00E	8.0 8.0 8.0 7.6	8.0 8.0[4]	1.3 1.3	5.2 5.2 5.3	2.2

Table 5 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2	MSE/CMX	ISE	ACS	Cisco PI
03.06.04E 03.06.03E 03.06.02aE 03.06.01E 03.06.00E	03.06.04E 03.06.02aE 03.06.01E 03.06.00E	8.0 8.0 7.6	8.0 8.0	1.3 1.2	5.2 5.2 5.3	2.2 2.2, 2.1.2, or 2.1.1 if MSE is also deployed[5] 2.1.0 if MSE is not deployed
03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	7.6[6] 7.5[7]	7.6 7.5	1.2	5.2 5.3	2.0

1. For maintenance release patches, go to Prime Infrastructure Patches. For the latest device pack, go to Prime Infrastructure Device Pack.
2. The Cisco IOS XE Denali 16.2.1 features are not available with 3.0.2, but 3.0.2 is compatible with Cisco IOS XE Denali 16.2.1.
3. Cisco 5700 (with Cisco IOS XE Release 03.06.03E/Cisco IOS XE Release 03.07.02E) inter-operates as a Peer MC with Catalyst 3850 running Cisco IOS XE Denali 16.1.1.
4. Because of SHA-2 certificate implementation, MSE 7.6 is not compatible with Cisco IOS XE Release 3.6E and later. Therefore, we recommend that you upgrade to MSE 8.0.
5. If MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.
6. Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.
7. Prime Infrastructure 2.0 enables you to manage Cisco WLC 7.5.102.0 with the features of Cisco WLC 7.4.110.0 and earlier releases. Prime Infrastructure 2.0 does not support any features of Cisco WLC 7.5.102.0 including the new AP platforms.

For more information on the compatibility of wireless software components across releases, see the *Cisco Wireless Solutions*

Web UI System Requirements

Hardware Requirements

Table 6 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

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

Software Requirements

- Operating Systems
  - Windows 7
  - Mac OS X 10.9.5

- Browsers
  - Google Chrome—Version 38 and later (On Windows)
  - Microsoft Internet Explorer—Versions 10 and later (On Windows)
  - Mozilla Firefox—Version 33 and later (On Windows and Mac)
  - Safari—Version 7 and later (On Mac)

Finding the Software Version and Feature Set

Table 7 shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
Everest 16.4.1	Not applicable	Everest 16.4.1	15.3(3)JPD
Denali 16.3.2	Not applicable	Denali 16.3.2	15.3(3)JPC2
Denali 16.3.1	Not applicable	Denali 16.3.1	15.3(3)JPC
Denali 16.2.2	Not applicable	Denali 16.2.2	15.3(3)JPB1
Denali 16.2.1	Not applicable	Denali 16.2.1	15.3(3)JPB
Denali 16.1.3	Not applicable	Denali 16.1.3	15.3(3)JNP2
Denali 16.1.2	Not applicable	Denali 16.1.2	15.3(3)JNP1
Denali 16.1.1	Not applicable	Denali 16.1.1	15.3(3)JNP
03.07.03E	15.2(3)E3	10.3.130.0	15.3(3)JNB3
03.07.02E	15.2(3)E2	10.3.100.0	15.3(3)JNB1
03.07.01E	15.2(3)E1	10.3.100.0	15.3(3)JNB1
03.07.00E	15.2(3)E	10.3.100.0	15.3(3)JNB
03.06.04E	15.2(2)E4	10.2.140.0	15.3(3)JN8
03.06.03E	15.2(2)E3	10.2.131.0	15.3(3)JN7
03.06.02aE	15.2(2)E2	10.2.120.0	15.3(3)JN4
03.06.01E	15.2(2)E1	10.2.111.0	15.3(3)JN3
03.06.00E	15.2(2)E	10.2.102.0	15.3(3)JN
03.03.05SE	15.0(1)EZ5	10.1.150.0	15.2(4)JB7
03.03.04SE	15.0(1)EZ4	10.1.140.0	15.2(4)JB6
03.03.03SE	15.0(1)EZ3	10.1.130.0	15.2(4)JB5h
03.03.02SE	15.0(1)EZ2	10.1.121.0	15.2(4)JB5
03.03.01SE	15.0(1)EZ1	10.1.110.0	15.2(4)JB2
03.03.00SE	15.0(1)EZ	10.1.100.0	15.2(4)JN

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.

Upgrading the Switch Software

This section covers the following scenarios:

- Automatic Boot Loader Upgrade
- Automatic Microcode Upgrade
- Upgrading to Cisco IOS XE Everest 16.4.1
- Downgrading from Cisco IOS XE Everest 16.4.1
- Upgrading RTU Licenses

Note You cannot use the Web UI to install, upgrade to, or downgrade from Cisco IOS XE Denali 16.1.x, 16.2.x,16.3.x, or Cisco IOS XE Everest 16.4.1.

Table 8 Software Images

Release	Image	File Name
Cisco IOS XE Everest 16.4.1	Universal	cat3k_caa-universalk9.16.04.01.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.04.01.SPA.bin

Table 9 Changes in Software Installation CLI Commands

Cisco IOS XE 3.xE	
`Switch#software ?`	
`auto-upgrade`	Initiate auto upgrade for switches running incompatible software
`clean`	Clean unused package files from local media
`commit`	Commit the provisioned software and cancel the automatic rollback timer
`expand`	Expand a software bundle to local storage, default location is where the bundle currently resides
`install`	Install software
`rollback`	Rollback the committed software
Cisco IOS XE Denali and Everest 16.x.x Commands	
`Switch#request platform software package ?`	
`clean`	Clean unnecessary package files from media

copy	Copy package to media
describe	Describe package content
expand	Expand all-in-one package to media
install	Package installation
uninstall	Package uninstall
verify	Verify ISSU software package compatibility

Automatic Boot Loader Upgrade

When you upgrade from any prior IOS 3.xE release to an IOS XE 16.x.x release for the first time, the boot loader is automatically upgraded and it will take effect on the next reload. For subsequent IOS XE 16.x.x releases, if the boot loader is updated in those releases, it will be automatically upgraded when you load the new release on the switch. If you go back to an IOS 3.xE release, your boot loader will not be downgraded. The updated boot loader supports all previous IOS 3.xE releases.

Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Everest 16.4.1 the first time	The boot loader is upgraded to version 4.28. For example:
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.28, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Everest 16.4.1, you will see the following on the console:
	`%IOSXEBOOT-Wed-###: (rp/0): Nov 30 01:17:05 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.3.2 the first time	The boot loader is upgraded to version 4.28. For example:
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.28, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.3.2, you will see the following on the console:
	`%IOSXEBOOT-Wed-###: (rp/0): Nov 2 20:46:19 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.3.1 the first time	The boot loader is upgraded to version 3.78. For example:
	`CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 3.78, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.3.1, you will see the following on the console:
	`%IOSXEBOOT-Mon-###: (rp/0): Jul 25 16:22:25 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Denali 16.2.x the first time	The boot loader is upgraded to version 3.58. For example:
	`switch: ver`
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 3.58, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.2.1, you will see the following on the console:
	`%IOSXEBOOT-Thu-###: (rp/0): Mar 24 18:18:10 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.1.x the first time	The boot loader is upgraded to version 3.2. For example:
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 3.2, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade while booting Cisco IOS XE Denali 16.1.x, you will see the following on the console:
	`%IOSXEBOOT-PLEASE-###: (rp/0): DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-Nov-Tue: (rp/0): 24 11:04:42 Universal 2015 boot loader upgrade successful`

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. With the Cisco IOS XE Denali 16.x.x release, 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:

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

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0]...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0]...381758 bytes.
Front-end Microcode IMG MGR: Programming device
0...rwRrrrrrrw..0%............................................................
.
..10%.....................................................................20%........
.
............................................................30%......................
.................................................40%...............................
.....................................50%...........................................
........................60%.........................................................
............70%.
......................................................................80%...........
..........................................................90%........................
..............................................100%
Front-end Microcode IMG MGR: Preparing to program device[0]...25166 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%..
..100%
Front-end Microcode IMG MGR: Microcode programming complete for device 0.
Front-end Microcode IMG MGR: Preparing to program device[0]...86370 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 237 seconds
```

Upgrading to Cisco IOS XE Everest 16.4.1

This section describes the process you have to follow to upgrade from Cisco IOS XE 3.xE or Cisco IOS XE Denali 16.x.x releases to Cisco IOS XE Everest 16.4.1.

Due to an increase in the Cisco IOS XE Everest 16.4.1 software image size, there may not be sufficient space to perform an upgrade using **`flash:`** (See CSCvc26183). The In-Place Package Expansion for Software Image feature was instroduced in prior releases to help with this issue, but the feature is not supported on all releases. Depending on the existing software version you are using you may have to first upgrade to an intermediate release and then then to Cisco IOS XE Everest 16.4.1.

Refer to the table below to know the upgrade proces you have to follow.

- Existing Release—This is the software release you are currently using.
- Intermediate Release—Indicates the software release you must first upgrade to, before upgrading to the target release. The link provides information about the procedure you have to follow.
- Target Release—Provides information about how you can upgrade to Cisco IOS XE Everest 16.4.1. Whether you upgraded to an intermediate release or not, you must complete this step to upgrade to Cisco IOS XE Everest 16.4.1

Existing Release	Intermediate Release	Target Release
Cisco IOS XE 3.xE	Cisco IOS XE Denali 16.3.1 (1GB of flash space reqd.) See Upgrading from Cisco IOS XE 3.xE to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in Install Mode.	Cisco IOS XE Everest 16.4.1. See Upgrading from Cisco IOS XE Denali 16.3.x to Cisco IOS XE 16.x in Install Mode
Cisco IOS XE Denali 16.1.1	Cisco IOS XE Denali 16.3.1 (1GB of flash space reqd.) See Upgrading from Cisco IOS XE Denali 16.1.1 to 16.1.x, 16.2.x, or 16.3.x in Install Mode.	
Cisco IOS XE Denali 16.1.2	Cisco IOS XE Denali 16.3.1 (1GB of flash space reqd.) See Upgrading from Cisco IOS XE Denali 16.3.x to Cisco IOS XE 16.x in Install Mode.	
Cisco IOS XE Denali 16.1.3 and later	Not required, upgrade directly to the target release.	
Cisco IOS XE Denali 16.2.1	Cisco IOS XE Denali 16.3.1 (1GB of flash space reqd.) See Upgrading from Cisco IOS XE Denali 16.3.x to Cisco IOS XE 16.x in Install Mode	
Cisco IOS XE Denali 16.2.2 and later	Not required, upgrade directly to the target release.	
Cisco IOS XE Denali 16.3.1 and later	Not required, upgrade directly to the target release.	

Downgrading from Cisco IOS XE Everest 16.4.1

Follow these instructions to downgrade from Cisco IOS XE 16.x to older Cisco IOS XE 3.xE releases in Install Mode.

- Downgrade from Cisco IOS XE 16.x to Cisco IOS XE 3.xE in Install Mode
- Downgrade from Cisco IOS XE 16.x to Cisco IOS XE 3.xE in Bundle Mode

Upgrading RTU Licenses

In Cisco IOS XE Denali 16.1.1, right-to-use (RTU) licensing has been modified to allow stack members to join a stack without having the same license level as the rest of the existing stack. The mismatched switch will not be put into Lic-Mismatch state. Even though the switch with the mismatched license is allowed to join the stack, the following syslog message is displayed periodically reminding you to fix the RTU license level:

```
%STACK_RTU_LICENSE-6-IOSD_LIC_MISMATCH:Switch 5 R0/0: stack_mgr: Switch #5:
Current IOSd runs on lanbase license while RTU active license is ipservices.
Please configure RTU license to current IOSd license.
```

For more information, see CSCux27336.

The EXEC mode **Right to Use License** command allows you to activate or deactivate feature set licenses or Adder AP Count Licenses. This command provides options to activate or deactivate any license supported on the platform.

```
license right-to-use  [activate|deactivate]  [ lanbase | ipbase | ipservices |
ap-count]  {evaluation  | <count> } [ all | slot  <switch id>] {acceptEULA}
```

Ugrading an IP Base SKU to IP Services License

Step	Command	Purpose
1	license right-to-use activate ipservices slot <switch id>	Activate IP Services license. Pass the switch id. EULA will be prompted, accept the EULA by typing ‘yes’.
2	show license right-to-use summary	Check the reboot license level is ipservices.
3	reload	Reboot the switch to boot with ipservices.

Evaluating IP Services License on IP Base SKU

Step	Command	Purpose
1	license right-to-use activate ipservices evaluation slot <switch id>	Activate IP Services evaluation license. Pass the switch id. EULA will be prompted, accept the EULA by typing ‘yes’.
2	show license right-to-use summary	Check the reboot license level is ipservices eval.
3	reload	Reboot the switch to boot with ipservices eval.

Upgrading an LAN Base SKU to IP Services License Without Prompting EULA

Step	Command	Purpose
1	license right-to-use activate ipservices slot <switch id> acceptEULA	Activate IP Services license. Pass the switch id. EULA will be accepted automatically without being prompted.
2	Show license right-to-use summary	Check the reboot license level is ipservices.
3	Reload	Reboot the switch to boot with ipservices.

Deactivating Evaluation IP Services License on IP Base SKU

Step	Command	Purpose
1	license right-to-use deactivate ipservices evaluation slot <switch id>	Deactivates IP Services evaluation license.
2	Show license right-to-use summary	Check the reboot license level is ipbase.
3	Reload	Reboot the switch to boot with ipbase.

Upgrading LAN Base Stack to IP Base Stack

Step	Command	Purpose
1	license right-to-use activate ipbase all	Activate IP Base license on all the switches in the stack. EULA will be prompted, accept the EULA by typing ‘yes’.
2	Show license right-to-use	Check the reboot license level is ipbase for all the switches.
3	Reload	Reboot the switch to boot with ipbase.

Changing the License Level of License Mismatch Switch from Active’s Console

If the license mismatch switch has a lower license level than other switches in the stack, and the stack is running at IP Services and the mismatch switch is booted with IP Base license.

Step	Command	Purpose
1	show switch	Get the switch number in license mismatch state.
2	show license right-to-use mismatch	Check the license level of the license mismatch switch.

Step	Command	Purpose
3	license right-to-use activate ipservices slot <switch-id>	Activate IP Services license on all the mismatch switches in the stack. EULA will be prompted, accept the EULA by typing ‘yes’.
4	Reload slot <switch-id>	Reboot the license mismatch switch to boot with ipservices and join the stack.

If the license mismatch switch has a higher license level than other switches in the stack, and the stack is running at IP Base and the mismatch switch is booted with IP Services license.

Step	Command	Purpose
1	show switch	Get the switch number in license mismatch state.
2	show license right-to-use mismatch	Check the license level of the license mismatch switch.
3	license right-to-use activate ipbase slot <switch-id>	Activate IP Base license on the license mismatch switch. EULA will be prompted, accept the EULA by typing ‘yes’.

Adding Adder AP Count Licenses

Step	Command	Purpose
1	license right-to-use activate apcount <count> slot <switch id>	Pass the number of AP count licenses to add as count. Pass the switch-id on which the Adder AP count licenses are to be added. EULA is prompted, accept it by typing ‘yes’.
2	Show license right-to-use slot <switch-id>	Check the adder AP count licenses are incremented on the given switch.
3	Show license right-to-use summary	Check the total Adder AP count licenses are incremented and the Total available AP count are incremented.

Decrementing Adder AP Count licenses

Step	Command	Purpose
1	license right-to-use deactivate apcount <count> slot <switch id>	Pass the number of AP count licenses to be removed as count. Pass the switch-id on which the Adder AP count licenses are to be removed.

Step	Command	Purpose
2	Show license right-to-use slot <switch-id>	Check the adder AP count licenses are decremented on the given switch.
3	Show license right-to-use summary	Check the total Adder AP count licenses are reduced by count and the Total available AP Count are reduced.

Activating Evaluation AP Count License on the Stack

Step	Command	Purpose
1	license right-to-use activate apcount evaluation	Activated evaluation AP Count licenses on the stack. EULA will be prompted, accept it.
2	Show license right-to-use summary	Check the license type evaluation with maximum supported AP Count is displayed. Base and adder AP Count licenses are not seen.
3	Show license right-to-use	To check the base and adder apcount licenses, if any.

Deactivating Evaluation AP Count License

Step	Command	Purpose
1	license right-to-use deactivate apcount evaluation	Deactivates evaluation AP Count licenses on the stack.
2	Show license right-to-use summary	Base and Adder AP Count licenses are displayed. Total available AP Count is sum of Base and Adder AP Count.

Feature Sets

The Catalyst 3850 switch supports three different feature sets:

- LAN Base feature set—Provides basic Layer 2+ features, including access control lists (ACLs) and quality of service (QoS), and up to 255 VLANs.
- IP Base feature set—Provides Layer 2+ and basic Layer 3 features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, IP multicast routing, Routing Information Protocol (RIP), basic IPv6 management, the Open Shortest Path First (OSPF) Protocol (for routed access only), and support for wireless controller functionality. The license supports up to 4094 VLANs.

- IP Services feature set—Provides a richer set of enterprise-class intelligent services and full IPv6 support. It includes all IP Base features plus full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging for only IP traffic). The IP Services feature set includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP), the Open Shortest Path First (OSPF) Protocol, and support for wireless controller functionality. The license supports up to 4094 VLANs.

Note A separate access point count license is required to use the switch as a wireless controller.

For more information about the features, see the product data sheet at this URL:

http://www.cisco.com/en/US/products/ps12686/products_data_sheets_list.html

Interoperability with Other Client Devices

This section describes the interoperability of this version of the switch software release with other client devices.

Table 10 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	16.3.1
Controller	Cisco 3850 Controller
Access points	3802, 3502, 3602, 2602, 1702, 2702, 3702, 702W, 1852
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 5.3, ISE 1.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 11 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, and phones.

Table 11 Client Types

Client Type and Name	Version
Laptop	
Intel 5100/5300	v14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 1000/1030	v14.3.0.6
Intel 7260	18.33.0.2
Intel 7265	18.40.0.9

Table 11 Client Types

Intel 3160	18.33.0.2
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Asus AC56(USB)	1027.7.515.2015
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro	OSX 10.11.5
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.11.5
Macbook Pro with Retina Display	OSX 10.11.5
Macbook New 2015	OSX 10.11.5
Tablets	
Apple iPad2	iOS 9.3.1(13E238)
Apple iPad3	iOS 9.3.1(13E238)
Apple iPad mini with Retina display	iOS 9.3.1(13E238)
Apple iPad Air	iOS 9.3.1(13E238)
Apple iPad Air 2	iOS 9.3.1(13E238)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 – SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3073.151
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0

Table 11 Client Types

Google Nexus 7 2nd Gen	Android 5.0
Phones	
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Apple iPhone 4S	iOS 9.2(13C75)
Apple iPhone 5	iOS 9.3.1(13E238)
Apple iPhone 5s	iOS 9.3.1(13E238)
Apple iPhone 5c	iOS 9.3.1(13E238)
Apple iPhone 6	iOS 9.3.1(13E238)
Apple iPhone 6 Plus	iOS 9.3.1(13E238)
Apple iPhone SE	iOS 9.3.1(13E238)
HTC One	Android 5.0
OnePlusOne	Android 4.3
Samsung Galaxy S4 – GT-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.1
Nexus 6	Android 5.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.4.2
Google Nexus 9	Android 6.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S5	Android 5.0.1
Xiaomi Mi 4i	Android 5.1.1
Samsung Galaxy S7	Android 6.0.1

Scaling Guidelines

Table 12 Scaling Guidelines

System Feature	Maximum Limit
Number of HTTP session redirections system-wide	Up to 100 clients per second (wired/wireless)
Number of HTTPS session redirections system-wide	Up to 5 clients per second (wireless) Up to 20 clients per second (wired)

Limitations and Restrictions

- Limitations for YANG data modeling—A maximum of 20 simultaneous NETCONF sessions are supported.
- Limitations for RF Profiles—Configuration with Cisco Prime Infrastructure is not supported. You must use the CLI to configure the feature.
- Limitations for Wired AVC:
  - NBAR2 (QOS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
  - NBAR2 attributes based QOS is not supported (‘match protocol attribute’).
  - NBAR2 and Netflow cannot be configured together at the same time 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 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale—Able to handle up to 5000 bi-directional flows per 24 access ports.
- Restrictions for QoS:
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
- Starting with Cisco IOS XE Denali 16.3.1, Centralized Management Mode (CMM) is no longer supported.
- MSE 8.x is not supported with Cisco IOS XE Denali 16.x.x.

- WIPs is not supported with Cisco IOS XE Denali 16.x.x since the CMX WIPs solution is not available.
- You cannot configure NetFlow export using the Ethernet Management port (g0/0).
- The maximum committed information rate (CIR) for voice traffic on a wireless port is 132 Mb/sec.
- On WS-C3850-48 switches, if the cable plugged into port 1 has a long cable boot, the boot may stay in contact with the mode button and cause the switch to reload and reset the configuration. To workaround this issue, use the **no setup express** command to disable Express Setup, or remove the cable boot from the cable in port 1.
- Flex Links are not supported. We recommend that you use spanning tree protocol (STP) as the alternative.
- Outdoor access points are supported only when they are in Local mode.
- Restrictions for Cisco TrustSec:
  - Dynamic SGACL download is limited to 6KB per destination group tag (DGT).
  - Cisco TrustSec 802.1x is not supported.
  - Cisco TrustSec Critical Auth is not supported.
  - Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
  - Cisco TrustSec for IPv6 is not supported.
  - Cisco TrustSec cannot be configured on a pure bridging domain with IPSG feature enabled. You must either enable IP routing or disable the IPSG feature in the bridging domain.
- 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 crash. As a workaround, disable the logging discriminator on the device.
- For the WS-C3850-12X48U-L, WS-C3850-12X48U-S and WS-C3850-12X48U-E switch models, a maximum of 28 ports are available for UPoE connections.

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

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The 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 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:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats in Cisco IOS XE Everest 16.4.1

The following are the open caveats in Cisco IOS XE Everest 16.4.1. Click on the identifier to view the details of a caveat in the BST.

Identifier	Description
CSCvc24786	16.4.1 - Mobility tunnel down due to PKI failure
CSCvb99047	Webauth fails after fallback from MAB
CSCvc26183	Install mode job error message requires change
CSCvb95950	Crash observed on 3-member mixed stack with 3850XS and 3850
CSCvc14776	[16.4.1 prd6]Image size significantly increased ~110MB, which is not inline with 16.3.2 CCO
CSCvb93503	[16.4.1]Software install/expand fails on latest build - 20161030_174118
CSCva47999	AP2800: spectrum mgmt bit is off in beacon
CSCvb70028	Unable to Access internal-webauth login page when client associated with AIR-AP2802I-B-K9 AP
CSCva75218	Barbados AP print '0' in statics output for fields TxData TxUC
CSCvc28298	Device crashed after reload:mips64_linux_iosd_ngwc-universalk9-ms_3638
CSCvb09930	"show plat soft fed switch 1 ac cou hardware" Egress frame count is 0
CSCvb36961	FIPS: Asymmetric MACsec POST KAT required for Doppler ASIC (3650/3850)
CSCvb53110	Smart CLI: vlan/gw config not handled for brownfield deployment
CSCvb54210	~30 sec traffic loss observed w. SSO on a port-channel w. multiple links (A,S,M)
CSCvb61864	The shut/noshut cmd with cisco powered pd cause pd to not power up
CSCvb67861	Image downgrade from 16.3.2 to 3.6.5E[Fips enabled]
CSCvb70239	16.3.2:1008:CTS: Standby crashed while unconfiguring a CTS link in down state
CSCvb70291	Power devices lose power upon switch reload with poe-ha enabled
CSCvb75523	FED crash durig overnight reload test
CSCvb75803	Netconf: Energywise activitycheck leaf not available under the interface through netconf-yang
CSCvb79124	Incorrect stack-power is budgeted after power stack cable OIR
CSCvb88345	16.3.2: Netflow timestamp is wrong on CSR and impact wired avc feature severely
CSCvb90042	g24 forwarding issues with Lisp decap
CSCvb91970	FED crash at dev_macsec_get_tx_sa_nextpn upon reload
CSCvb93706	[Cat3k] Trafic drops are seen on fabric edge node when MS/MR is offline
CSCvc06025	REP opened-non-neigbour didn't work properly

CSCvc08098	EEE status and capabilities output are not as expected with "power efficient-ethernet auto"
CSCvc10889	Dropped packers counters from portchannel are not seen
CSCvc12944	3.6.5: IOSd Crash Process = EW Main
CSCvc15252	Speed nonegotiate turns the interface duplex to half on 3850 1G uplink
CSCvc15365	Silent roll: "Package missing critical package information when determining build\" in bundle mode
CSCvc16268	WDAVC: Punt fails for short IPG packets
CSCvc18133	Sanity: AP failed to join ctlr, DTLS-3-PKI_ERROR, intermittent, very low reproduce rate
CSCvc18245	Stack merge due to incompatiblity reload 3850 8M half-ring stack
CSCvc19086	AP connected to Cat3k switch with 16.3.2 is unable to join centralized 8510 WLC
CSCvc20807	MPLS over Macsec is not working
CSCvc24786	16.4.1 - Mobility tunnel down due to PKI failure
CSCuy70833	Observing issue with packet counters in accounting record
CSCuy82690	Mcast data traffic is enforced by Trustsec
CSCuz12602	Cleanup autoinstall logging
CSCva91816	SF- Multicast convergence very high with RLOC Shut /no shut trigger
CSCvb56122	PM-3-INTERNALERROR: Port Manager Internal Software Error on no shut 40G
CSCvb66249	Traffic fails with ipv6 acl for tcp estabilished
CSCvb66917	Tracebacks seen during standby reload
CSCvb73310	SF:Netflow vrf input data should update segment information but shows "UNKOWN\"
CSCvb74369	AVB: pDelay values are high with 1G ports configured to 100Mbps.
CSCvb90280	Tengig Port in Etherchannel goes down after bootup on WS-C3850-12X48U
CSCvb91221	Found Traceback %PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT: during boot
CSCvb98994	Mac count not removed after disabling "no switchport port-security mac-address"
CSCvb99239	Used Values for "Directly or indirectly connected route" field is not as expected
CSCvc01596	shr_irq_signal_interrupt:865 no ip for irq 31:3
CSCvc24401	Downlink port LEDs display green without plugging anything in the port
CSCvc26412	Standby removed after configuring "ipv6 snooping" .

Resolved Caveats in Cisco IOS XE Everest 16.4.1

None.

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 IOS XE Denali 16.x.x documentation at this URL:

  http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html
- Catalyst 3850 switch documentation at this URL:

  http://www.cisco.com/go/cat3850_docs
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes at this URL:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents at this URL:

  http://www.cisco.com/go/designzone
- Error Message Decoder at this URL:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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.
