



Release Notes for the Catalyst 3850 Series Switches, Cisco IOS XE Release 3.3.xSE

First Published: October 7, 2013

Last Updated: January 30, 2015

OL-30562-05

This release note describes the features and caveats for the Cisco IOS XE 3.3.xSE software on the Catalyst 3850 series switch. Unless otherwise noted, the terms *switch* and *device* refer to a standalone switch and to a switch stack.

Contents

- [Introduction, page 2](#)
- [What's New, page 2](#)
- [Supported Hardware, page 9](#)
- [Wired Web UI \(Device Manager\) System Requirements, page 17](#)
- [Wireless Web UI Software Requirements, page 17](#)
- [Finding the Software Version and Feature Set, page 17](#)
- [Software Compatibility Matrix, page 18](#)
- [Interoperability with Other Client Devices, page 19](#)
- [Upgrading the Switch Software, page 20](#)
- [Features, page 20](#)
- [Important Notes, page 21](#)
- [Limitations and Restrictions, page 23](#)
- [Caveats, page 23](#)
- [Documentation Updates, page 31](#)



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

- [Troubleshooting, page 32](#)
- [Related Documentation, page 32](#)
- [Obtaining Documentation and Submitting a Service Request, page 33](#)

Introduction

The Catalyst 3850 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 application visibility and control are natively built into the switch.

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

The Cisco IOS XE software 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.

For more information about the Cisco IOS XE software, see

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps9442/ps11192/ps11194/QA_C67-622903.html

What's New

- [“What's New in Cisco IOS XE Release 3.3.5SE” section on page 2](#)
- [“What's New in Cisco IOS XE Release 3.3.4SE” section on page 2](#)
- [“What's New in Cisco IOS XE Release 3.3.3SE” section on page 3](#)
- [“What's New in Cisco IOS XE Release 3.3.2SE” section on page 6](#)
- [“What's New in Cisco IOS XE Release 3.3.1SE” section on page 6](#)
- [“What's New in Cisco IOS XE Release 3.3.0SE” section on page 6](#)

What's New in Cisco IOS XE Release 3.3.5SE

- Behavior change—When using PAP authentication, the MAC address of the client is presented in upper case characters as credential information to the AAA server. In previous releases, the MAC address was presented in lower case characters.

No features were added or enhanced for this release. For more information about other updates in this release, see the [“Caveats” section on page 23](#).

What's New in Cisco IOS XE Release 3.3.4SE

No features were added or enhanced for this release. For more information about updates in this release, see the [“Caveats” section on page 23](#).

What's New in Cisco IOS XE Release 3.3.3SE

- “New Hardware Support” section on page 3
- “CPP-Related Commands” section on page 3

New Hardware Support

- Catalyst 3850-12S and Catalyst 3850-24S switches that support SFP+ module slots. For more details, see the “[Catalyst 3650 Switch Models](#)” section on page 11.



Note These switches are supported by Cisco IOS XE Release 3.3.3SE or later.

- Support for DWDM SFP+ and 10G ZR SFP+ modules. For a list of all supported SFP+ modules, see http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6974.html.

CPP-Related Commands

- `cpp [all | disable | system-default | traffic-type]`
- `show platform qos queue stats internal cpu policer`

`cpp [all | disable | system-default | traffic-type]`

The `cpp [all | disable | system-default | traffic-type]` global configuration command for configuring Control Plane Policing (CPP) has been updated to include keywords for modifying CPP policer settings on CPU queues and for controlling the policer rate based on traffic types.

`cpp [all | disable | system-default | traffic-type [traffic-type {disable}]]`

all	(Optional) Enable policing on all CPU bound traffic.
disable	(Optional) Disable all CPU policing.

system-default	(Optional) Reset all CPU queues to system default policer rate values. Use the show platform qos queue stats internal cpu policer privileged EXEC command to display the system default values.
traffic-type [<i>traffic-type</i> { disable }]	(Optional) Set the CPU traffic type to police. <ul style="list-style-type: none"> • disable—Disable policing on the specified traffic type. Traffic types: <ul style="list-style-type: none"> • broadcast—Police broadcast traffic. • dot1x—Police IEEE 802.1x traffic. • forus-packet—Police forus packet traffic. Forus (or for-us) packets are packets destined to the router. • icmp-redirect—Police Internet Control Message Protocol (ICMP) redirect traffic. • layer2-control—Police Layer-2 control traffic. • multicast-control—Police multicast control traffic. • multicast-data—Police multicast data traffic. • routing-control—Police routing control traffic. • snooping—Police snooping traffic. • software-forward—Police software forward traffic. • system-data—Police system data traffic such as learning cache, RPF failure, GOLD, NFL sample. • topology-control—Police STP and STP topology control traffic. • webauth {<i>pps</i>}—Police web authentication traffic. <ul style="list-style-type: none"> – <i>pps</i>: The range is 100 pps to 13000 pps. • wireless-iapp—Police Cisco Inter Access Point Protocol (IAPP) traffic. • wireless-mgmt—Police wireless RFID, radio resource management (RRM), and probe management. • wireless-mobility—Police Control And Provisioning of Wireless Access Points (CAPWAP) mobility data and control traffic.

This example shows how to enable CPU queue policing on web authentication traffic at 1400 pps:

```
Switch(config)# cpp traffic-type webauth 1400
```

You can verify your setting by entering the **show platform qos queue stats internal cpu policer** privileged EXEC command. For information about this show command, see the [“show platform qos queue stats internal cpu policer” section on page 5](#).

show platform qos queue stats internal cpu policer

The **show platform qos queue stats internal cpu policer** privileged EXEC command is a new command to display the configured Control Plane Policing (CPP) CPU queue and corresponding traffic TYPES.

Table 1 CPP CPU Queue Mapping in FED with Corresponding Traffic Types

CPU Queue	Traffic Type
WK_CPU_Q_L2_CONTROL	layer2-control
WK_CPU_Q_ROUTING_CONTROL	routing-control
WK_CPU_Q_MCAST_DATA	multicast-data
WK_CPU_Q_PROTO_SNOOPING	snooping
WK_CPU_Q_PUNT_WEBAUTH	webauth
WK_CPU_Q_SW_FORWARDING_Q	sw-fwd
WK_CPU_Q_WIRELESS_PRIO_1	capwap-control
WK_CPU_Q_WIRELESS_PRIO_3	wireless-iapp
WK_CPU_Q_WIRELESS_PRIO_4, WK_CPU_Q_WIRELESS_PRIO_5	wireless-misc
WK_CPU_Q_TOPOLOGY_CONTROL	topology-control
WK_CPU_Q_MCAST_END_STATION_SERVICE	multicast-snooping
WK_CPU_Q_LEARNING_CACHE_OVFL, WK_CPU_Q_EXCEPTION, WK_CPU_Q_CRYPTO_CONTROL, WK_CPU_Q_EGR_EXCEPTION, WK_CPU_Q_NFL_SAMPLED_DATA, WK_CPU_Q_SGT_CACHE_FULL, WK_CPU_Q_GOLD_PKT, WK_CPU_Q_RPF_FAILED	system-data
WK_CPU_Q_ICMP_REDIRECT	icmp-redirect
WK_CPU_Q_DOT1X_AUTH	dot1x
WK_CPU_Q_BROADCAST	broadcast
WK_CPU_Q_FORUS_TRAFFIC	forus

The **show platform qos queue stats internal cpu policer** command output shows the CPP policer settings (such as traffic types and CPP rates) on the CPU queues.

```
Switch# sh platform qos queue stats internal cpu policer
```

```
For Asic 0
Queue           Enabled  Rate(default)  Rate(set)  Drop
-----
DOT1X Auth      No       1000           1000      0
L2 Control      No       500            500       0
Forus traffic   No       1000           1000      0
ICMP GEN        Yes      200            200       0
Routing Control No       500            500       0
Forus Address resolution No      1000           1000      0
ICMP Redirect   No       500            500       0
WLESS PRI-5     No       1000           1000      0
WLESS PRI-1     No       1000           1000      0
```

WLESS PRI-2	No	1000	1000	0
WLESS PRI-3	No	1000	1000	0
WLESS PRI-4	No	1000	1000	0
BROADCAST	Yes	200	200	0
Learning cache ovfl	Yes	100	100	0
Sw forwarding	Yes	1000	1000	0
Topology Control	No	13000	13000	0
Proto Snooping	No	500	500	0
BFD Low Latency	No	500	500	0
Transit Traffic	Yes	500	500	0
RPF Failed	Yes	100	100	0
MCAST END STATION	Yes	2000	2000	0
LOGGING	Yes	1000	1000	0
Punt Webauth	No	1000	1000	0
Crypto Control	Yes	100	100	0
Exception	Yes	100	100	0
General Punt	No	500	500	0
NFL SAMPLED DATA	Yes	100	100	0
SGT Cache Full	Yes	100	100	0
EGR Exception	Yes	100	100	0
Show frwd	No	1000	1000	0
MCAST Data	Yes	500	500	0
Gold Pkt	Yes	100	100	0

What's New in Cisco IOS XE Release 3.3.2SE

No features were added or enhanced for this release.

What's New in Cisco IOS XE Release 3.3.1SE

- Support added for Cisco Aironet 3700 Series Access Points—The Cisco Aironet 3700 Series Access Points with the 802.11ac module is supported in this release. For more information about the AP, see <http://www.cisco.com/en/US/products/ps13367/index.html>.
- For information about open and resolved caveats, see “Caveats” section on page 23.

What's New in Cisco IOS XE Release 3.3.0SE

- Wired Web UI (Device Manager)—An easy-to-use web interface that offers quick configuration and monitoring capabilities. Using a web browser, you can access Device Manager from anywhere in your network.
- Nine-member stacks—Up to nine switches can participate in a switch stack. All switches must be running the same feature set.
- Cisco Universal Power Over Ethernet (Cisco UPOE) feature—Sources up to 60 W of power (2X 30W) over both signal and spare pairs of the RJ-45 Ethernet cable based on IEEE 802.3at standards. It automatically detects Cisco UPOE-compliant power devices and negotiates power up to 60 W by using Layer 2 power negotiation protocols, such as Link Layer Discovery Protocol (LLDP). (Catalyst 3850 UPOE switches).
- Wireshark—A packet analyzer program that supports multiple protocols and presents information in a text-based user interface. Wireshark analyzes wired traffic and wireless traffic.

- HSRP version 2 support for IPv4 and IPv6—Improves management and troubleshooting of IP multicast addresses. Also addresses the restrictions in HSRP version 1, such as:
 - Group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.
 - Multicast address 224.0.0.2 is used to send HSRP hello messages. This address can conflict with Cisco Group Management Protocol (CGMP) leave processing. HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2.



Note HSRP is supported in the IP Base and IP Services feature sets. It is not supported in the LAN Base feature set.

- Wired Guest Access—Uses Ethernet in IP (RFC3378) within the centralized architecture to create a tunnel across a Layer 3 topology between two WLC endpoints. No additional protocols or segmentation techniques are needed to isolate guest traffic from the enterprise.
- Service Discovery Gateway feature—Enables multicast Domain Name System (mDNS) to operate across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain to another. This feature enhances Bring Your Own Device (BYOD).
- Captive Portal Bypassing for Local Web Authentication—Support for Apple devices that need to resolve Wireless Internet Service Provider roaming (WISPr) and have support for captive portal bypass.
- Critical Voice VLAN support—Puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.
- Multicast Fast Convergence with Flex Links Failover feature—Reduces the convergence time of multicast traffic after a Flex Links failure.
- Client Count per WLAN—You can configure client limits per WLAN, per AP per WLAN, and per AP per Radio. The number of clients that you can configure for each WLAN depends on the platform that you are using.
- 802.11w support—Support for the 802.11w standard as defined by the Management Frame Protection (MFP) service. Disassociation, Deauthentication, and Robust Action frames increase Wi-Fi network security by protecting the management frames from being spoofed.
- 802.11r support in local mode—Support for IEEE Standard for fast roaming allows the handshake with the new access point before the client roams to the target access point. Allows clients to move between access points without breaking a session.
- Wi-Fi Direct Client Policy—Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.
- Assisted Roaming—The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning. The assisted roaming feature is based on an intelligent and client-optimized neighbor list.
- Support for IPv6 wireless clients—Client policies can have IPv4 and IPv6 filters.
- Support for 802.11ac module—The 802.11ac radio module, which is based on the IEEE 802.11ac Wave 1 standard, is available on the Cisco lightweight access points.

The 802.11ac module provides enterprise-class reliability and wired-network-like performance. The 802.11ac module supports three spatial streams and 80 MHz-wide channels for a maximum data rate of 1.3 Gbps. The 802.11ac standard is a 5-GHz-only technology, which is faster and a more scalable version of the 802.11n standard.

- Application Visibility and Control—Classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR2) engine and provides application-level visibility into Wi-Fi networks.



Note The capability of dropping or marking the data traffic (control part) is not supported in the Cisco IOS XE 3.3.0SE.

- Security Enhancements
 - Manage Rogue devices—The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. For more information about managing rogue devices, see the “Managing Rogue Devices” section in the *System Management Configuration Guide*.
 - Classify rogue access points—The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified. For more information about classifying rogue access points, see the “Classifying Rogue Access Points” section in the *System Management Configuration Guide*.
 - wIPS—The Cisco Adaptive wireless intrusion prevention system (wIPS) continually monitors wireless traffic on both the wired and wireless networks and uses network intelligence to analyze attacks and more accurately pinpoint and proactively prevent attacks in the future. You can configure an access point to work in wIPS mode if the access point is in the Monitor or Local mode.
 - Radio Frequency Grouping—A radio frequency (RF) group is a logical collection of switches that coordinate to perform radio resource management (RRM) in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering switches into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single switch.
- Security Group Tag/Security Group ACL (SG/SGACL)—a set of features that improves the deployment of the overall Cisco TrustSec solution, including:
 - Cisco TrustSec VLAN to SGT mapping— enables deployment of SGT on devices that are not capable of SGT tagging but are VLAN-capable.
 - IP address to SGT mapping—enables deployment of SGT on resources with static IP addresses.
 - Port to SGT mapping—enables SGT tagging of all traffic from a particular port.
- Lightweight Directory Access Protocol Server mode—Operates as the backend database for web authentication to retrieve user credentials and authenticate the user.
- Wireless Flexible NetFlow—Enables flow monitoring and control of wireless traffic.
- Enhanced QoS support for wireless IPv6 clients—Support for IPv6 ACLs and DSCP-matching of IPv6 packets.
- Cisco Express Forwarding (CEF)—Supported in the LAN Base feature set.
- Protocol-independent multicast (PIM) for IPv4 traffic—Supported in the IP Base feature set.
- Policy-based routing (PBR) for IPv4 traffic—Supported in the IP Base feature set.
- OSPF enhancements—Support for up to 1000 routes.

Supported Hardware

Catalyst 3850 Switch Models

Table 2 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-C3850-24T-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
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set
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

Table 2 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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
Catalyst 3850-12S-S	IP Base	12 SFP+ module slots, 1 network module slot, 350-W power supply
Catalyst 3850-24S-S	IP Base	24 SFP+ module slots, 1 network module slot, 350-W power supply
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-3850-24U-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply
WS-3850-48U-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply
Catalyst 3850-12S-E	IP Services	12 SFP+ module slots, 1 network module slot, 350-W power supply
Catalyst 3850-24S-E	IP Services	24 SFP+ module slots, 1 network module slot, 350-W power supply

Network Modules

Table 3 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 3 Supported Network Modules

Network Module	Description
C3850-NM-4-1G	Four 1-Gigabit small form-factor pluggable (SFP) module slots. Any combination of standard SFP modules are supported. SFP+ modules are not supported.
C3850-NM-2-10G	Four SFP module slots: <ul style="list-style-type: none"> Two slots (left side) support only 1-Gigabit SFP modules and two slots (right side) support either 1-Gigabit SFP or 10-Gigabit SFP+ modules. Supported combinations of SFP and SFP+ modules: <ul style="list-style-type: none"> Slots 1, 2, 3, and 4 populated with 1-Gigabit SFP modules. Slots 1 and 2 populated with 1-Gigabit SFP modules and Slot 3 and 4 populated with 10-Gigabit SFP+ module.
C3850-NM-4-10G	Four 10-Gigabit slots or four 1-Gigabit slots. Note The module is supported only on the 48-port models.
C3850-NM-BLANK	No uplink ports.

Catalyst 3650 Switch Models

Table 4 Catalyst 3650 Switch Models

Switch Model	Cisco IOS Image	Description
Catalyst 3650-24TS-L	LAN Base	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP (small form-factor pluggable) uplink ports, 250-W power supply
Catalyst 3650-48TS-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-24PS-L	LAN Base	Stackable 24 10/100/1000 PoE+ ¹ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48PS-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48FS-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
Catalyst 3650-24US-L	LAN Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3650-48US-L	LAN Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-24TD-L	LAN Base	Stackable 24 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-48TD-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24PD-L	LAN Base	Stackable 24 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48PD-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48FD-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-24UD-L	LAN Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48UD-L	LAN Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48FQ-L	LAN Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-48PQ-L	LAN Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48TQ-L	LAN Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24TS-S	IP Base	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-48TS-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-24PS-S	IP Base	Stackable 24 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48PS-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3650-48FS-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
Catalyst 3650-24US-S	IP Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-48US-S	IP Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-24TD-S	IP Base	Stackable 24 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-48TD-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24PD-S	IP Base	Stackable 24 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48PD-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48FD-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-24UD-S	IP Base	Stackable 24 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48UD-S	IP Base	Stackable 48 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48FQ-S	IP Base	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-48PQ-S	IP Base	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48TQ-S	IP Base	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24TS-E	IP Services	Stackable 24 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply
Catalyst 3650-48TS-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, four 1-Gigabit SFP uplink ports, 250-W power supply

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3650-24PS-E	IP Services	Stackable 24 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48PS-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, four 1-Gigabit SFP uplink ports, 640-W power supply
Catalyst 3650-48FS-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, four 1-Gigabit SFP uplink ports, 1025-W power supply
Catalyst 3650-24US-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-48US-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE downlink ports and four 1-Gigabit uplink ports
Catalyst 3650-24TD-E	IP Services	Stackable 24 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-48TD-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 250-W power supply
Catalyst 3650-24PD-E	IP Services	Stackable 24 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48PD-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48FD-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-24UD-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48UD-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE downlink ports, and two 1-Gigabit SFP and two 10-Gigabit SFP+ uplink ports
Catalyst 3650-48FQ-E	IP Services	Stackable 48 10/100/1000 Full PoE downlink ports, four 10-Gigabit SFP+ uplink ports, 1025-W power supply
Catalyst 3650-48PQ-E	IP Services	Stackable 48 10/100/1000 PoE+ downlink ports, four 10-Gigabit SFP+ uplink ports, 640-W power supply
Catalyst 3650-48TQ-E	IP Services	Stackable 48 10/100/1000 Ethernet downlink ports, four 10-Gigabit SFP+ uplink ports, 250-W power supply

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
Catalyst 3850-24U-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE ports, one network module slot, 1100-W power supply
Catalyst 3850-48U-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE ports, one network module slot, 1100-W power supply

1. PoE+ = Power over Ethernet plus (provides up to 30 W per port).

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

Cisco Wireless LAN Controller Models

Table 5 Cisco WLC 5700 Models

Part Number	Description
AIR-CT5760-25-K9	Cisco 5760 Wireless Controller for up to 25 Cisco access points
AIR-CT5760-50-K9	Cisco 5760 Wireless Controller for up to 50 Cisco access points
AIR-CT5760-100-K9	Cisco 5760 Wireless Controller for up to 100 Cisco access points
AIR-CT5760-250-K9	Cisco 5760 Wireless Controller for up to 250 Cisco access points
AIR-CT5760-500-K9	Cisco 5760 Wireless Controller for up to 500 Cisco access points
AIR-CT5760-1K-K9	Cisco 5760 Wireless Controller for up to 1000 Cisco access points
AIR-CT5760-HA-K9	Cisco 5760 Series Wireless Controller for High Availability

Access Points and Mobility Services Engine

Table 6 lists the supported products of the Catalyst 3850 switch.

Table 6 Catalyst 3850 Switch Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 1040, 1140, 1260, 1600, 2600, 3500, 3600, 3700
Mobility Services Engine	3355, Virtual Appliance

Table 7 lists the specific supported Cisco access points.

Table 7 *Supported Access Points*

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 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I
Cisco Aironet 3500 Series	AIR-CAP3501E
	AIR-CAP3501I
	AIR-CAP3501P
	AIR-CAP3502E
	AIR-CAP3502I
	AIR-CAP3502P
Cisco Aironet 3600 Series	AIR-CAP3602E
	AIR-CAP3602I
Cisco Aironet 3700 Series	AIR-CAP3702I
	AIR-CAP3702E
	AIR-CAP3702P

Wired Web UI (Device Manager) System Requirements

Hardware Requirements

Table 8 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

- Windows 2000, Windows 2003, Windows XP, Windows Vista, or Windows 7
- With JavaScript enabled: Internet Explorer 6.0 and 7.0, or Firefox 26.0

Wireless Web UI Software Requirements

- Operating Systems
 - Windows XP
 - Windows 7
 - Mac OS X
- Browsers
 - Google Chrome
 - Microsoft Internet Explorer
 - Mozilla Firefox

Finding the Software Version and Feature Set

[Table 9](#) shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 9 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
03.03.05SE	15.1(0)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

Table 9 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
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.

Software Compatibility Matrix

Table 10 lists the software compatibility matrix.

Table 10 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2	MSE	ISE	ACS	Cisco PI
03.03.05SE	03.03.05SE	7.6	7.6	1.2	5.2, 5.3	2.1.2
03.03.04SE	03.03.04SE	7.6	7.6	1.2	5.2, 5.3	2.1.2
03.03.03SE	03.03.03SE	7.5	7.5			
03.03.02SE	03.03.02SE	7.6 ¹	7.6	1.2	5.2, 5.3	2.1.1 ³
03.03.01SE	03.03.01SE	7.5 ²	7.5			2.0
03.03.00SE	03.03.00SE					

1. Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.
2. 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.
3. Prime Infrastructure 2.1.1 allows you to manage Cisco WLC Releases 7.5.102.0 and 7.6.x with the features of Cisco WLC 7.4.121.0 and earlier releases. Prime Infrastructure 2.1.1 does not support any features that are introduced in Cisco WLC Releases 7.5.102.0 and 7.6.x except the new access point platforms and the new mobility feature.

Interoperability with Other Client Devices

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

[Table 11](#) lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 11 Client Types

Client Type and Name	Version
Laptop	
Intel 4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/6300	v14.3.0.6
Intel 6205	v14.3.0.6
Dell 1395/1397	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
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)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0.1
Apple iPad3	iOS 7.1.1(11D201)
Apple iPad Mini	iOS 7.1.1(11D201)
Samsung Galaxy Tab	Android 3.2
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 5	iOS 7.1.1(11D201)
Apple iPhone 5s	iOS 7.1.1(11D201)

Table 11 Client Types (continued)

Client Type and Name	Version
Apple iPhone 5c	iOS 7.1.1(11D201)
Apple iPhone 4	iOS 6.0.1
Apple iPhone 4S	iOS 6.0.1
Apple iPhone 5	iOS 6.0.1
Ascom i62	2.5.7
HTC Sensation	Android 2.3.3
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus	Android 4.0.2

Upgrading the Switch Software

For information about how to upgrade the switch software, see the *System Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/system_management/configuration_guide/b_sm_3se_3850_cg.html

Features

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 4094 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), ACLs, QoS, static routing, EIGRP stub routing, IP multicast routing, Routing Information Protocol (RIP), basic IPv6 management, the Open Shortest Path First (OSPF) Protocol, and support for wireless controller functionality.
- IP Services feature set—Provides a richer set of enterprise-class intelligent services and full IPv6 support. It includes IP Base features plus Layer 3 routing (IP unicast routing and IP multicast routing). 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.



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

Important Notes

- Although visible in the CLI, the following commands are not supported:
 - **switchport mode dot1qtunnel**
 - **collect flow username**
 - **authorize-lsc-ap** (CSCui93659)
 - **show platform qos xxx** (CSCug09112)
- WCCPv2 is supported for egress IPv4 traffic with the following limitations and restrictions:
 - Load balancing using only mask assignments; no support for hash assignments in hardware.
 - No VRF-aware WCCP support.
 - No IPv6 WCCP support.
 - Either PBR or WCCP configuration is supported on an interface.
 - Maximum number of service groups is eight for ingress and eight for egress.
- The following features are not supported in Cisco IOS XE Release 3.3.0SE:
 - Outdoor Access Points
 - Mesh, FlexConnect, and Office Extend Access Point deployment
 - Wireless Guest Anchor Controller (The Catalyst 3850 switch can be configured as a foreign controller.)
 - IPv6 Multicast Routing
 - Resilient Ethernet Protocol
 - Virtual Router Redundancy Protocol (VRRP)
 - Private VLANs
 - Device Sensor
 - MVR (Multicast VLAN Registration)
 - EnergyWise
 - IPv6 routing - OSPFv3 Authentication
 - Call Home
 - DVMRP Tunneling
 - Port Security on EtherChannel
 - 802.1x Configurable username and password for MAB
 - Government Certificates: Common Criteria & FIPS
 - Link State Tracking (L2 Trunk Failover)
 - Disable Per VLAN MAC Learning
 - IEEE 802.1X-2010 with 802.1AE support
 - IEEE 802.1AE MACsec (MKA & SAP)
 - Command Switch Redundancy
 - CNS Config Agent
 - Dynamic Access Ports
 - IPv6 Ready Logo phase II - Host

- IPv6 IKEv2 / IPSecv3
- OSPFv3 Graceful Restart (RFC 5187)
- Fallback bridging for non-IP traffic between VLANs
- DHCP snooping ASCII circuit ID
- Protocol Storm Protection
- 802.1x NEAT
- 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
- Mediatrace
- Passive Monitoring
- Performance Monitor (Phase 1)
- AAA: RADIUS over IPv6 transport
- 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
- IEEE 802.1Q Tunnel (Q-in-Q)
- Layer 2 Tunneling Protocol Enhancements
- UniDirectional Link Routing (UDLR)
- Pragmatic General Multicast (PGM)
- PVLAN, DAI, IPSG Interoperability
- Ingress Rate Limiting
- Ingress Strict Priority Queuing (Expedite)
- Weighted Random Early Detect (WRED)
- Improvements in QoS policing rates
- Fast SSID support for guest access WLANs

Limitations and Restrictions

- You cannot configure NetFlow export using the Ethernet Management port (g0/0).
- The switch does not support CDP bypass.
- 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.
- Restrictions for Cisco TrustSec:
 - Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
 - Cisco TrustSec for IPv6 is not supported.
 - Dynamic binding of IP-SGT is not supported for hosts on Layer 3 physical routed interfaces because the IP Device Tracking feature for Layer 3 physical interfaces 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.
 - Cisco TrustSec on the switch supports up to 255 security group destination tags for enforcing security group ACLs.

Caveats

- [Cisco Bug Search Tool, page 23](#)
- [Open Caveats, page 24](#)
- [Resolved Caveats in Cisco IOS XE Release 3.3.5SE, page 24](#)
- [Resolved Caveats in Cisco IOS XE Release 3.3.4SE, page 24](#)
- [Resolved Caveats in Cisco IOS XE Release 3.3.3SE, page 26](#)
- [Resolved Caveats in Cisco IOS XE Release 3.3.2SE, page 27](#)
- [Resolved Caveats in Cisco IOS XE Release 3.3.1SE, page 28](#)
- [Resolved Caveats in Cisco IOS XE Release 3.3.0SE, page 29](#)

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 listed in this document:

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

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool” section on page 23](#).

Bug ID	Severity	Headline
CSCuj92028	2	WCCP Crash @edison_wccp_cam_write_event_handler
CSCup12631	2	WebGUI displays WSMA errors on some pages after TACACS authentication
CSCup49704	2	3850 FED Crash - Waiting for SPI channels FED_SPI_FLCD,FED_SPI_FAST
CSCuq48800	2	Low throughput due to UAPSD for Intel 7260 WiFi chipset
CSCur24801	2	DUT Fails to hit (SGT, DGT) in the absence of inline/SXP and IPDT entry
CSCur07909	3	Stack merge due to active and standby lost connectivity

Resolved Caveats in Cisco IOS XE Release 3.3.5SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool” section on page 23](#).

Bug ID	Severity	Headline
CSCul46957	3	9M stack:Traceback@%OSAPI-5-MUTEX_UNLOCK_FAILED during switchover
CSCuo66526	2	wcm restart observed on 5760 with 3600 AP module
CSCup39353	2	IOSd reboots at @ ios_syncmgr_lock_pop_errmsg
CSCup86496	2	unicast ARP replies not destined to 3850 are forwarded to ARP module
CSCuq22460	3	COMMON-1-WDOG_CPUHOG: 1 fed: CPU usage time exceeded
CSCuq79546	1	IOSd reboots on 5760 running 3.3.4 at be_epm_redirect_cache_entry_get
CSCuq91035	3	5760 MIB support AP3700P AP model

Resolved Caveats in Cisco IOS XE Release 3.3.4SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool” section on page 23](#).

Bug ID	Severity	Headline
CSCuc12774	3	FA1 routes unicast flood traffic back out FA1
CSCuc21859	2	Memory leak seen due to ESM (Embedded Syslog manager)
CSCug51974	2	eEdge:Authen Failed page not thrown on Webauth with concurrent MAB login
CSCuh88726	3	SNMP High CPU when polling lldpXMedLocMediaPolicy
CSCui65914	2	DATA CORRUPTION-SP-1-DATA INCONSISTENCY copy error / 12.2(33)SRE6
CSCui69119	2	IPDT: rejected channel conf&Standby failed to boot up
CSCuj17317	3	XE: Certain snagless cables may press on the mode button causing reload
CSCul43158	2	Random mobile disassociation with PEM unknown timeout

Bug ID	Severity	Headline
CSCum45713	2	C2k_Scale: UUT crashed for scale session
CSCum66082	2	IRCM:Client able to pass traffic in CWA_RE
CSCum66129	2	3850 not forwarding multicast traffic in layer 2 when PIM enabled on SVI
CSCum91301	1	IPDT: Standby crashes due to host table corruption
CSCun39810	2	Iosd Crash due to snmpProxy
CSCun68485	2	Router ACL (RACL) on SVI in output direction applied to bridged traffic
CSCun78227	2	Incorrect temperature thresholds reported via SNMP
CSCun92928	2	Must reboot controller for HotSpot WLAN to advertise IW IE; AP crashes
CSCun97765	2	3850/03.03.02SE/Unable to disable IPDT
CSCuo14901	2	Crash/High CPU when enabling nbar for Flexible Netflow
CSCuo26294	2	WS-X45-SUP7-E crash with Process ffm: terminated abnormally
CSCuo47903	1	No CWA redirect for client in case it roamed in webauth-reqd state
CSCuo52701	2	slproc crash on 3850 switch stack
CSCuo55022	2	3850 hosts not getting DHCP addresses when Port-security is enabled
CSCuo63950	2	WCM crash on customer production network
CSCuo83872	5	Power Controller reports Short detected when non PoE device connected
CSCuo84770	2	3850/3.3.2SE/Not forwarding double dot1Q tagged packets
CSCuo86406	2	-D regulatory domain not supported with India (IN) country code in NGWC
CSCuo91792	2	IPDT:Wired stale entries learned via ARP not clearing out
CSCuo98789	2	ARP broadcast for vlan which is not SVI punted to CPU incase of Layer 2
CSCuo98816	2	Delete Payload not sent to previous AP when roaming to new AP
CSCup04121	2	Redirection loop when WCCP \ "OUTV" enabled on SVI on Cat-3850
CSCup09246	2	Catalyst3850 NetFlow export invalid packet
CSCup22590	2	Multiple Vulnerabilities in IOS/IOSd OpenSSL - June 2014
CSCup43034	2	WCM crash running 03.03.03
CSCup52101	2	EnergyWise Denial of Service vulnerabilty
CSCup53338	2	3850 IOSD crash Signal=SIGSEGV(11) @ pm_port_data_from_swidb
CSCup63909	2	Roaming fails when Anchored phone roams back from foreign.
CSCup73590	2	WCM crash in Mobility code.
CSCup76790	2	FNF flow doesn't age out after 50 days
CSCup76944	2	HSRP dual Active at 3850 after port-channel down/up
CSCup91453	2	SNMP query cportQosStatsEntry with invalid ifindex prints hwidb is null
CSCup92246	2	NG3K: Default deny SGACL policy dropping management traffic
CSCup92808	2	No CWA redirect for client in case it roamed in webauth-reqd state
CSCuq09690	2	"no parameter-map" causes crash on 3.3.3 : auth_proxy_cache_redirect_url
CSCuq25195	2	Adjust AFD for every client and BSSID add/del.
CSCuq29232	2	No CWA redirect for client if it roamed in webauth-reqd state

Bug ID	Severity	Headline
CSCuq32016	2	Incorrect AFD client ssid association
CSCuq38516	2	iosd crash at emweb_http_process

Resolved Caveats in Cisco IOS XE Release 3.3.3SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool”](#) section on page 23.

Bug ID	Severity	Headline
CSCui69681	3	3850 Switch Crash During Route Lookup on Self-Generated ICMP Packet
CSCtk68692	3	kron-initiated 'write mem' locks nvram indefinitely
CSCug75425	3	4500-Sup7E NTP synchronized but clock behind 5-8 seconds
CSCug92629	4	show tech-support inc Sunil includes names
CSCuh56465	3	Span: Multiple SPAN source ports on the same switch not monitored
CSCuh59075	2	member switch crashed with tracebacks due to MEMBLK CORRUPTION
CSCui94876	3	Serviceability enhancement needed to identify the AVL tree getting full
CSCuj31712	3	certain Vendor Sfp force ports to err-disable upon OIR
CSCui94876	3	Serviceability enhancement needed to identify the AVL tree getting full
CSCuj31712	3	certain Vendor Sfp force ports to err-disable upon OIR
CSCuj51019	2	Alpha: FFM crash on member switch
CSCuj52086	3	SSID name does not get updated with fast ssid change in access-request.
CSCul25757	2	CLI- port speed 10, 100, 1000 configuration fails on SFP interface
CSCul44461	2	System failed to bootup due to initializationfailure + IOSd crash
CSCul47224	2	Traceback @ ngwc_dot1x_control_rcv when dot1x authentication starts
CSCul66509	3	WLC 5760 GUI webpage error at first launch
CSCum07541	3	BYOD Guest client not joining the serving wlan sometimes.
CSCum09063	2	IOS system crash @ http_process
CSCum47451	2	3850 dACL is not applied on the stack member switch > 4
CSCum70737	2	3850 :: ACL definitions not consistent between stack master and members
CSCum81233	3	Config long vlan name cause tracback wcm_cs_debug_api + 780
CSCun10948	3	3850: Segfault with Process = ACL Logging Process
CSCun14712	3	5760 session timeout defaults and range are not shown properly in WebGUI
CSCun15859	2	Memory Leak ifm_send_ssid_update
CSCun21020	3	IP source guard causing packet drops
CSCun22639	3	ip source guard with mac-check prevents DHCP
CSCun26520	3	HA Not able to Sync on 5760
CSCun29753	1	Acl crash seen in darya mr1
CSCun31450	2	IOSD-WATCHDOG: Process = IP SLAs XOS Event Processor IOSd crash

Bug ID	Severity	Headline
CSCun32266	2	ACL label leak with large scale webauth
CSCun36781	2	3850 - Service config configuration causes boot loop
CSCun40246	3	Dot1x along with WEP fails authentication only during re-auth
CSCun44526	1	Katana 12K wireless clients application tuning for WVU
CSCun46486	1	Darya MR2 crash on SNMP engine
CSCun48219	2	Crash on 3850 stack with DHCP snooping
CSCun48721	2	3850 responds to GARP not destined to it
CSCun55391	2	FED crash on 5760 3.3.1SE
CSCun62776	3	3850 crash with FED service at fnf_ffm_cache_stats_send
CSCun84970	3	3850 Every time diff wrap occurs, packet counter mismatch by 1
CSCun87876	2	multicast entries not synced completely to standby on IGMP leave
CSCun92474	3	EAPOL version should not always be V2
CSCun94333	3	5760 may send account stop after successful authentication with CWA
CSCun96020	2	5760 Client stuck in idle state
CSCun97822	3	Numeric VLAN name causing issues in wlan configuration with WebGUI.
CSCun98131	2	NG3K: Persistent snmp instance values for entity-mib
CSCuo01232	2	Clients not getting IP address at times when CPU utilization is high
CSCuo01236	2	CPU utilization is high with un-authenticated HTTPS redirected traffic
CSCuo14829	2	3850/03.03.02SE/Stuck Routing Control Q due to IPV6 MLD
CSCul31038	3	CSCul31038 NG3K: SNMP MAU-MIB support
CSCuo54486	3	AmurEdison:Clients on dropped APs cannot reconnect after switchover

Resolved Caveats in Cisco IOS XE Release 3.3.2SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool”](#) section on page 23.

Bug ID	Severity	Headline
CSCtq21722	1	SNMP crash forced due to an invalid memory block
CSCuc50127	3	mcast traffic loss when SVI is shut/no shut
CSCud17778	2	memory leak in middle buffers due to snmp traps
CSCui40588	2	GUI is not accesible after aaa authentication for http/s
CSCui60565	3	Lost saved "queue-limit dscp vlaues" configuration after reload
CSCui75983	3	ingress policy match to wrong class-map after reboot
CSCui97487	2	3850: Reload of all member Switches cause Active SWitch to reload
CSCuj58616	2	Katana memory leak in IOSd - ppcp_to_ppm_policy
CSCuj61051	2	wcm crash in process_spi_job_incoming () at ios_services
CSCuj73087	2	Darya:QoS:1-2 ports of uplink module in 24 ports sw shaper 1/10

Bug ID	Severity	Headline
CSCuj81941	2	Katana-HA:PI template for 802.11a radio config pushed but failed to sync
CSCul19814	2	SCHED-3-tHRASHING at fnf-rpc_context_wait_for_completion
CSCul21515	2	Client policing behaviour is unexpected for TCP traffic
CSCul26646	2	Scheduler data structure cleanup issue "process_watch_watched_message"
CSCul30304	2	Failed to allocate hardware resource(REP RI)
CSCul30792	2	SNMP memory leak when heavy polling is done continuously
CSCul31225	2	QoS:svi set policy not work
CSCul37521	2	duplex configuration is lost upon a reload when using the GLC-GE-100FX.
CSCul54414	2	Unable to configure anything after adding few SNMP communities/host
CSCul54484	2	Memory leak in eicored
CSCul54561	2	Memory leak in iosd
CSCul66968	2	Crash after bringing up a port-channel configured with mode on
CSCul79858	2	Darya:SNMP pulling 3-4 days cause the switch crash
CSCul84467	2	C3850:Stack:Port-Channel:Active Mem Switch Power Shut cause Traffic Loss
CSCum11385	2	Amur: FED process crashed on the member switch
CSCum21662	2	Darya:SNMP pulling 3-4 days cause the switch crash
CSCum40660	2	3850 dot1x multi-host - client roaming between ports does not work
CSCum43727	2	DHCP snooping database not being created
CSCum59496	2	5760 reboots in openssl_dtls_server_setup
CSCum66933	2	Iosd crash observed on customer setup

Resolved Caveats in Cisco IOS XE Release 3.3.1SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool”](#) section on page 23.

Bug ID	Severity	Headline
CSCsl45701	3	TACACS+ per VRF authen failing: Address already in use
CSCuc63146	2	Port-channel interface flap when changing vlan allowed list
CSCud08538	2	WNBU-ALPHA: WCM crash on 2M at pthread_mutex_lock
CSCue49527	2	WLC should delete the session ID from PMK cache when client is removed
CSCue93229	3	crash when polling ipMRouteEntry during "clear ip mroute"
CSCug18767	6	LWA Captive Portal Bypass + Consent logout popup blocker support
CSCug29756	1	Cat3850: FRU_PS_OIR messages and/or PoE not updated with available power
CSCui36499	3	%PLATFORM_THERMAL-1-FRU_FAN_FAILURE:
CSCui69999	2	3850 crashes when switches in the stack have different images
CSCui80121	3	NGWC: AP's BVI MTU 1728 Bytes Triggering Input Errors on Neighbor Switch
CSCuj21417	2	AID leak causing Stale Client entries on WLC

Bug ID	Severity	Headline
CSCuj34025	2	HCA: AUP PDF page does not display in PDF format
CSCuj48089	2	3850 Stuck Broadcast Queue
CSCuj51372	2	MacLearning not occurring for a group of 24 ports on 3850
CSCuj57007	2	HCA: DHCPACK with no DHCP_OPT_LEASE_TIME option field should trigger IPDT
CSCuj65910	3	3850 03.02.02.SE wrong data for 1.3.6.1.4.1.9.9.656.1.4.1.1.14 OID
CSCuj78610	2	High cpu issue dueto process Auth-proxy HTTP, Web Auth client issue
CSCul03186	2	HCA: HotSpot Error intermittently on iPad
CSCul06456	3	Bowdoin cust requirement: need snmp OID support to create local net user
CSCul06619	2	Stale IPDT entries causing client to be stuck in DHCP reqd state.
CSCul13504	3	web-auth logout pop-up window disable support
CSCul27659	3	DHCP NAK sent as broadcast is causing issues in Guest (F-A) scenarios
CSCul27717	2	APs disassociate in large scale setup when debug commands are executed
CSCul30051	2	Clients failing auth (psk/dot1x) due to uncreated dot1x interface for AP

Resolved Caveats in Cisco IOS XE Release 3.3.0SE

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the [“Cisco Bug Search Tool”](#) section on page 23.

Bug ID	Severity	Headline
CSCua75283	2	%DATACORRUPTION-1-DATAINCONSISTENCY and router hang with Codenomicon
CSCub21979	2	Duplicated pkt on RSPAN destination as vlan filter enabled
CSCuc09296	3	CSCuc09296After switchover Full Reconciliation takes 15 secs
CSCuc12774	3	FA1 routes unicast flood traffic back out FA1
CSCuc24608	3	flow records exported to default table other than VRF table
CSCuc45552	2	RAs from wireless clients not blocked with Ether channel
CSCuc56470	3	Correct chaining behavior, prevent activation as “child” policy
CSCuc95293	1	All external communications cease
CSCud03402	3	switch logs “i2c-octeon i2c-octeon.1: broken irq connection detected”
CSCud11467	3	Apply in and out PV HQOS policy/remove input policy/output policy fails
CSCud11552	3	Change int BW/speed when HQOS policy is attached causes policy to detach
CSCud13091	2	Member crashes on boot up if previous l3 intf del is stuck
CSCud13283	2	After switchover unconfig takes several minutes
CSCud17361	3	Upon switchover, show int status shows unknown for uplink sfp
CSCud27939	2	Fail to update channel/power 4member 3850 stack
CSCud33835	3	show boot shows junk and boot on next reload value incorrect
CSCud51031	3	mac-address table updated with BPDU SA from Neighbor switch
CSCud54501	3	'show policy-map interface wireless ap' counters not updating

Bug ID	Severity	Headline
CSCud54725	3	policy stops working after remove class from policy-map attached to intf
CSCud55333	3	port-shape not reaching shape rate for 10gig port
CSCud56426	2	webauth does not unbind logout ACLs in use once virtual ip is removed
CSCud60008	3	with Priority+policer change on fly cause some policy to be uninstalle
CSCud60070	3	”increase range for “”prio+ abs rate”” from 2G to 10G”
CSCud62982	3	PV with same child policy don’t work properly on some uplink ports
CSCud63110	3	Table-map set still present after remove agg-policing with table child
CSCud63823	3	Delete share policy on 4x10G uplink port share policy on 1G stop work
CSCud65034	3	classification not work under parent user-defined class
CSCud71747	3	SNMP Issues in MO MC client tables
CSCud72626	2	per vlan policy failed to be removed with certain sequence
CSCud84240	3	snmp-server group CLI does not allow both IPv6 and IPv4 ACLs
CSCud90586	2	With passwd key zeroize config upon switchover active crashed
CSCuf86171	2	DHCP snooping database agent fails to start
CSCuf93185	3	Newton Uplink 1-G only port up even force change state to admin down
CSCug38523	2	WebUI: home screen takes 10-15 sec to load
CSCug41165	3	Copy-paste of wireless config drops characters from beginning of line
CSCug58178	3	wireless multicast traffic not sent to vlan defined by AP group on 3850
CSCuh17479	2	2M-Stack: WCM crash@eicore_ipc after 1 day 19 hours; 03.10.05.EXP
CSCuh20848	3	3850 shows %IPC-5-WATERMARK log messages repeatedly
CSCuh44542	2	Crash as multi data/voice clients auth followed by host-mode change
CSCuh66931	3	3850 SW crash due to process watchdog loop with NGWC Learning Process
CSCui51050	3	3850 not pulling right correct OID for stack port change
CSCui59004	2	iosd crash while configuring no ntp server

Documentation Updates

Catalyst 3850 Switch Hardware Installation Guide

Network Modules

- The description of the network module is incorrect. It should read:

C3850-NM-2-10G	<p>Four-slot SFP module:</p> <ul style="list-style-type: none"> Two slots (left side) support only 1-Gigabit SFP modules and two slots (right side) support either 1-Gigabit SFP or 10-Gigabit SFP modules. <p>Supported combinations of SFP and SFP+ modules:</p> <ul style="list-style-type: none"> Slots 1, 2, 3, and 4 populated with 1-Gigabit SFP modules. Slots 1 and 2 populated with 1-Gigabit SFP modules and Slot 3 and 4 populated with 10-Gigabit SFP+ module.
----------------	--

Hardware Guide (French Version)

The French version of the *Catalyst 3850 Switch Hardware Guide* does not include information about the Catalyst 3850-12S and Catalyst 3850-24S switches. For information on these switches, see the English hardware guide at:

http://www.cisco.com/go/cat3850_hw

Regulatory Compliance and Safety Information for the Catalyst 3850 Switch

- In the French RCSI guide, statement warning 1044 is erroneously included. It does not apply to the switches.

Security Configuration Guides

Refer to this document for Cisco TrustSec support on the switch:

<http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html>.

These documentation links provide incorrect information about Cisco TrustSec on the switch:

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/configuration_guide/b_consolidated_3850_3se_cg/b_consolidated_3850_3se_cg_chapter_01000010.html
- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/security/configuration_guide/b_sec_3se_3850_cg/b_sec_3se_3850_cg_chapter_010011.html

System Management Configuration Guide, Cisco IOS XE Release 3SE

- The name of the Cisco IOS software bundle and the names of the Cisco IOS package files are incorrect. The correct filenames are:
 - cat3k_caa-universalk9.SPA.03.03.00.SE.150-1.EZ.bin
 - cat3k_caa-base.SPA.03.03.00SE.pkg
 - cat3k_caa-drivers.SPA.03.03.00SE.pkg
 - cat3k_caa-infra.SPA.03.03.00SE.pkg
 - cat3k_caa-iosd-universalk9.SPA.150-1.EZ.pkg
 - cat3k_caa-platform.SPA.03.03.00SE.pkg
 - cat3k_caa-wcm.SPA.10.1.100.0.pkg

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

- 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.

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.

© 2013-2015 Cisco Systems, Inc. All rights reserved.

