



Release Notes for Catalyst 3650 Series Switch, Cisco IOS XE Release 3.7.xE

First Published: December 10, 2014

Last Updated: Feb 16, 2017

This release note gives an overview of the features for the Cisco IOS XE 3.7.xE software on the Catalyst 3650 series switch.

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

Contents

- [Introduction, page 2](#)
- [New Features, page 2](#)
- [Supported Hardware, page 7](#)
- [OpenFlow Version and Cisco IOS Release Support, page 16](#)
- [Wireless Web UI Software Requirements, page 17](#)
- [Finding the Software Version and Feature Set, page 17](#)
- [Upgrading the Switch Software, page 18](#)
- [Features, page 19](#)
- [Interoperability with Other Client Devices, page 20](#)
- [Important Notes, page 21](#)
- [Limitations and Restrictions, page 23](#)
- [Caveats, page 24](#)
- [Troubleshooting, page 30](#)
- [Related Documentation, page 30](#)
- [Obtaining Documentation and Submitting a Service Request, page 31](#)



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

Introduction

The Catalyst 3650 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 160-Gbps StackWise-160. Wired and wireless security and application visibility and control are natively built into the switch.

The Catalyst 3650 switches also support full IEEE 802.3 at Power over Ethernet Plus (PoE+), and offer modular and field replaceable redundant fans and power supplies. The Catalyst 3650 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 preminent 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

Revision History

Table 1 **Revision History**

Modification Date	Modification Details
April 27, 2017	<ul style="list-style-type: none"> • Resolved Caveats in Cisco IOS XE Release 3.7.5E, page 25 <ul style="list-style-type: none"> – Added: CSCus83638


New Features

- [What's New in Cisco IOS XE Release 3.7.5E, page 2](#)
- [What's New in Cisco IOS XE Release 3.7.4E, page 3](#)
- [What's New in Cisco IOS XE Release 3.7.3E, page 3](#)
- [What's New in Cisco IOS XE Release 3.7.2E, page 3](#)
- [What's New in Cisco IOS XE Release 3.7.1E, page 4](#)
- [What's New in Cisco IOS XE Release 3.7.0E, page 4](#)

What's New in Cisco IOS XE Release 3.7.5E

There are no new features in this release.

What's New in Cisco IOS XE Release 3.7.4E

Feature Name	Description
Support for –B Domain	<p>The FCC (USA) rule making on 5 GHz released on April 1, 2014 (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. Cisco APs and Cisco WLCs will comply with the new rules by supporting the new regulatory domain (– for the US and will create new AP SKUs that are certified under the new rules. Examples of new rules include new 5-GHz band channels permitted for outdoor use, and transmission (Tx) power level increased to 1W for indoor, outdoor, and point-to-point transmissions.</p> <p> Note Cisco APs and Cisco WLCs that are in the –A domain category can continue to operate and even coexist with –B domain devices without any issues.</p> <p>We recommend that you upgrade Cisco APs and Cisco WLCs to the appropriate software release that supports –B domain.</p> <p>–B Domain Compliant Cisco APs starting with Cisco IOS XE Release 3.7.4E are: Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 2600, 2700, 3500, 3600, 3700.</p>

What's New in Cisco IOS XE Release 3.7.3E

Feature Name	Description
Enhancement to Web-auth configuration	<p>Commands under global parameter-map to enable non SVI and VRF aware Web-auth configuration.</p> <p>(LAN Base, IP Base and IP Services/Enterprise Services)</p>
Mobility Controller managing Mobility Agent (MCMA)	<p>The Mobility Controller managing Mobility Agent feature allows you to push the wireless and common configurations from the MC to the MAs.</p> <p>(IP Base, IP Services/Enterprise Services)</p>
OpenFlow 1.0 and OpenFlow 1.3	<p>The OpenFlow feature defines a flow-based forwarding infrastructure (L2-L4 Ethernet switch model) and a standardized application programmatic interface to allow traffic flows on a device to be added or removed. OpenFlow allows a controller to direct the forwarding functions of a switch through a secure channel.</p> <p>(LAN Base, IP Base, IP Services)</p>
Support is added for these access points:	<ul style="list-style-type: none"> • Cisco Aironet 1850 Series Access Points • Cisco Aironet 1830 Series Access Points

What's New in Cisco IOS XE Release 3.7.2E

- LACP Rate Fast—Support for the new **lACP rate** command, to set the rate at which Link Aggregation Control Packets (LACP) packets are sent to LACP-supported interfaces.
- GRE tunneled packets switched on hardware—Support for forwarding GRE tunneled packets on the switch hardware.

What's New in Cisco IOS XE Release 3.7.1E

- New parameter **call-station-id** added to the **wireless security dot1x radius mac-authentication** command. The **call-station-id** parameter configures Call Station ID type for MAC authentication.
- SFP BiDirectional (BiDi) Optics—SFP BiDirectional (BiDi) optical transceivers are used to transmit and receive optical signals through only one single fiber. These make use of single strand of SMF. The deployment of BiDi optical transceivers instantly doubles the bandwidth capacity of the existing optical fiber infrastructure.
- Enhancement to port security configuration—Specify a MAC address that is forbidden by port security on all interfaces.
- Support for Media Access Control Security (MACsec). The switch supports 802.1AE encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between the switch and host devices.
- Increased scale on Catalyst 3650 Switches to support up to 50 access points. Previously, support was up to 25 access points.

What's New in Cisco IOS XE Release 3.7.0E

- Wireless capability is added to [Catalyst 4500E Series Switch Supervisor Engine 8-E](#).
- Support is added for the following access points:
 - [Cisco Aironet 1700 Series Access Point](#)
 - [Cisco Aironet 1570 Series Access Point](#) (supported only in Local mode)
- VLAN tagging is supported on [Cisco Aironet 700W Series Access Points](#)
- mDNS Service Discovery Gateway Phase 3—The Service Discovery Gateway feature enables multicast Domain Name System (mDNS) to operate across Layer 3 (L3) boundaries. In this phase, features such as de-congestion of incoming mDNS traffic, redistribution of service withdrawal messages, a filter criterion for learning services available on a specific interface, and the periodic browsing of services on specific interfaces are introduced.
- AVC top 'N' users per application—This feature enables you to know network usage information on a per user basis within an application. This feature is enabled by default and is available if AVC is enabled.
- AN Infra—Autonomic networking makes network devices intelligent by introducing self-management concepts that simplify network management for the network operator.
- CDP Bypass—The sessions are established in single and multi-host modes for IP Phones. However, if voice VLAN and 802.1x on an interface port is enabled, then the CDP Bypass is enabled when the host mode is set to single or multi host mode.



Note By default the host mode is set to single mode in <legacy> mode and multi-authentication in the edge mode.

Use the following commands to configure CDP bypass:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface <interface-id>
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan <vlan-id>
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode single | multi-host
Switch(config-if)# dot1x pae authenticator
```

- VRRPv3 for IPv4 and IPv6—Enables a group of devices to form a single virtual device, to eliminate the single point of failure, which is inherent to a static default routed environment.
- WebAuth sleeping client—Allows successfully authenticated devices to stay logged in for a configured period without reauthentication.

The following CLI is added under the webauth parameter map:

sleeping-client timeout *timeout-in-minutes*

Restrictions:

- There is one-to-one mapping between device MAC and username/password. Once an entry is added to sleeping-client cache, the device/user gets policies for the user stored in the cache. Therefore, any other user using the device also gets the same policies as the user stored in the sleeping-client cache. The user can force normal authentication by logging out. To do that, the user must explicitly enter the following URL:

```
http[s]://<Virtual IP/Virtual Host>/logout.html
```
- Mobility is not supported. If the client roams from one controller to another, the client undergoes normal authentication on the foreign controller.
- Regulatory domains for India (-D), Indonesia (-F), Brazil (-Z), Honk Kong (-S) are supported.
- New Flexible NetFlow Collect parameters:
 - **collect wireless afd drop bytes**—Collects the fields for wireless approximate fair drop (AFD) drop bytes
 - **collect wireless afd accept bytes**—Collects the fields for AFD accept bytes
- New CLI is added to view AFD statistics information:

```
Switch# show platform qos wireless stats ssid {ssid-value | all} client all
```

 This CLI lists client MAC address, WLAN ID, BSSID, accept byte, and drop byte details.
- New CLI is added to check whether an access point model is supported or not:

```
Switch# show ap is-supported ap-model-part-number
```
- AutoQoS is supported for wireless.
- MC managing MA is supported.
- Private VLAN support is introduced.
- AutoQoS Compact: This feature hides the auto-QoS-generated commands from the running configuration.
- Netflow IPv6 Exporter/IPv6 Extended Host Mode: This feature enables FNF Export over IPv6.
- MACSec Encryption: Support for CTS (Cisco Trusted Security), which uses MACSec and SAP for securing links between Cisco Catalyst switches. It uses either 802.1x protocol or manual configuration for authentication and authorization between the peers, followed by the Cisco proprietary protocol SAP (Security Association Protocol) for key agreement to encrypt and decrypt traffic.

- IPv6 Source Guard: IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works in conjunction with IPv6 neighbor discovery (ND) inspection or IPv6 address glean, both of which detect existing addresses on the link and store them into the binding table. IPv6 source guard is an interface between the populated binding table and data traffic filtering, and the binding table must be populated with IPv6 prefixes for IPv6 source guard to work.
- IPv6 Prefix Guard: The IPv6 Prefix Guard feature works within the IPv6 Source Guard feature, enabling the device to deny traffic originated from non-topologically correct addresses. IPv6 prefix guard is often used when IPv6 prefixes are delegated to devices (for example, home gateways) using DHCP prefix delegation. The feature discovers ranges of addresses assigned to the link and blocks any traffic sourced with an address outside this range.
- IPv6 Destination Guard: The IPv6 Destination Guard feature works with IPv6 neighbor discovery to ensure that the device performs address resolution only for those addresses that are known to be active on the link. It relies on the address glean functionality to populate all destinations active on the link into the binding table and then blocks resolutions before they happen when the destination is not found in the binding table.
- IPv6 First Hop Security support on Etherchannels: The IPv6 FHS policies can be attached to EtherChannel interfaces (Port Channels).
- IPv6 ACL Wild Card Masking: Support for IPv6 wild card masking when specifying the Layer 3 address of a IPv6 ACL entry.
- VLAN name extension: Maximum characters allowed for a VLAN name has been increased from 32 to 128.
- LDAP source interface and VRF support: Allows you to configure a dedicated LDAP source interface IP address and virtual routing and forwarding (VRF).
- VRF aware DHCPv6 Server/Relay for Prefix Delegation: Ensures that the DHCPv6 server and relay involved in delegating prefixes are VRF aware.
- Webauth Sleeping Client (Webauth remember me): Allows successfully authenticated devices to stay logged in for a configured period without re-authentication.
- VLAN RADIUS Attributes in Access Requests
- Enhances the security for access switches with the use of VLAN RADIUS attributes (VLAN name and ID) in the access requests and with an extended VLAN name length of 128 characters.
- Copy Aware VRF: Enables copying of files to and from a VRF via the **copy** command.
- CWDM SFP+ 10-Gigabit optics are supported.

Supported Hardware

Catalyst 3850 Switch Models

Table 2 Catalyst 3850 Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-L	LAN Base	Stackable 24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply
WS-C3850-48T-L	LAN Base	Stackable 48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply
WS-C3850-24P-L	LAN Base	Stackable 24 10/100/1000 PoE+ ports, 1 network module slot, 715 W power supply
WS-C3850-48P-L	LAN Base	Stackable 48 10/100/1000 PoE+ ports, 1 network module slot, 715 W power supply
WS-C3850-48F-L	LAN Base	Stackable 48 10/100/1000 PoE+ ports, 1 network module slot, 1100 W power supply
WS-C3850-24U-L	LAN Base	Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-48U-L	LAN Base	Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
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 power supply
WS-C3850-24T-S	IP Base	Stackable 24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply
WS-C3850-48T-S	IP Base	Stackable 48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply
WS-C3850-24P-S	IP Base	Stackable 24 10/100/1000 PoE+ ports, 1 network module slot, 715 W power supply
WS-C3850-48P-S	IP Base	Stackable 48 10/100/1000 PoE+ ports, 1 network module slot, 715 W power supply
WS-C3850-48F-S	IP Base	Stackable 48 10/100/1000 PoE+ ports, 1 network module slot, 1100 W power supply
WS-C3850-24U-S	IP Base	Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-48U-S	IP Base	Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-24PW-S	IP Base	Stackable, 24-port PoE IP Base with 5-access point license

Table 2 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-48PW-S	IP Base	Stackable, 48-port PoE IP Base with 5-access point license
WS-C3850-12S-S	IP Base	Stackable 12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-S	IP Base	Stackable 24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-S	IP Base	Stackable, 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	Stackable, 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	Stackable, 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	Stackable, 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	Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.
WS-C3850-48XS-F-S	IP Base	Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.
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 power supply
WS-C3850-24T-E	IP Services	Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply
WS-C3850-48T-E	IP Services	Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply
WS-C3850-24P-E	IP Services	Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply

Table 2 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-48P-E	IP Services	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply
WS-C3850-48F-E	IP Services	Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply
WS-C3850-24U-E	IP Services	Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply
WS-C3850-48U-E	IP Services	Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply
WS-C3850-12S-E	IP Services	Stackable, 2 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-E	IP Services	Stackable, 24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-E	IP Services	Stackable, 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	Stackable, 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	Stackable, 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	Stackable, 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-E switch.
WS-C3850-48XS-E	IP Services	Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.
WS-C3850-48XS-F-E	IP Services	Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.
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 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 3650-24TD-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

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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 3650-48FQ-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
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 3650-24TD-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

Table 4 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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 3650-48FQ-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
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 3650-24TD-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

Table 4 *Catalyst 3650 Switch Models (continued)*

Switch Model	Cisco IOS Image	Description
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 3650-48FQ-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

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 3650 Switch.


Note

On platforms that run Cisco IOS XE releases, the WSSI/3G modules on access points are not supported.

Table 6 Catalyst 3650 Switch Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 700, 700W, 1040, 1140, 1260, 1530, 1570, 1600, 1700, 2600, 2700, 3500, 3600, 3700
Mobility Services Engine	3355, Virtual Appliance

Table 6 lists the specific supported Cisco access points.

Supported Access Points

Access Points	
Cisco Aironet 700 Series	AIR-CAP702W-x-K9
	AIR-CAP702I-x-K9
	AIR-CAP702I-xK910
Cisco Aironet 700W Series	AIR-CAP702Wx-K9
	AIR-CAP702W-xK910
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

Supported Access Points (continued)

Access Points	
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 1700 Series	AIR-CAP1702I-x-K9
	AIR-CAP1702I-xK910
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I
Cisco Aironet 2700 Series	AIR-CAP2702I-x-K9
	AIR-CAP2702E-x-K9
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

Compatibility Matrix

[Table 7](#) lists the software compatibility matrix.

Table 7 **Software Compatibility Matrix**

Catalyst 3650	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE	ISE	ACS	Cisco PI
03.07.00E	03.07.00E	8.0 7.6	8.0 ¹	1.3	5.2 5.3	2.2

Table 7 Software Compatibility Matrix

Catalyst 3650	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE	ISE	ACS	Cisco PI
03.06.01E 03.06.00E	03.06.01E 03.06.00E	8.0 7.6	8.0 ²	1.2	5.2 5.3	2.2, 2.1.2, or 2.1.1 if MSE is also deployed ³ 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	7.5 ⁴	7.5	1.2	5.2 5.3	2.0

1. 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.
2. 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.
3. If MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.
4. Prime Infrastructure 2.0 enables you to manage Cisco WLC c7.5.102.0 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 Software Compatibility Matrix](#).

OpenFlow Version and Cisco IOS Release Support

The OVA package is available for download in the same location as your system image (.bin) file, on [cisco.com](#)



Note

The OVA package is compatible only with its corresponding system image file name - as listed in the table below. Do not use an older version of the OVA package with a newer system image file, or a newer OVA package with an older system image file.

Cisco IOS Release	Cisco OpenFlow Plug-In Version	Cisco OpenFlow Plug-In	Image Name
IOS XE 3.7.3E	2.0.4	ofa-2.0.4-r3-cat3000-SPA-k9.ova	cat3k_caa-universalk9.SPA.03.07.03.E.152-3.E3.bin

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 7
 - Windows 8
 - Mac OS X 10.8
- Browsers
 - Google Chrome—Version 35
 - Microsoft Internet Explorer—Versions 10 or 11
 - Mozilla Firefox—Version 30
 - Safari—Version 6.1

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
03.07.00E	15.2(3)E	10.3.100.0	15.3(3)JNB
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

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
03.03.03SE	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

For information about how to upgrade the switch software, see the *System Management Configuration Guide, Cisco IOS XE Release 3E (Catalyst 3650 Switches)* at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3e/system_management/configuration_guide/b_sm_3e_3650_cg.html

Table 10 Software Images

Image	File Name
Universal	cat3k_caa-universalk9.SPA.03.07.00.E.152-3.E1.bin
Universal without DTLS	cat3k_caa-universalk9ldpe.SPA.03.07.00.E.152-3.E1.bin

Important Upgrade Note

After you upgrade to Cisco IOS XE Release 3.7E, the WebAuth success page behavior is different from the behavior seen in Cisco IOS XE Release 3.3.X SE. After a successful authentication on the WebAuth login page, the original requested URL opens in a pop-up window and not on the parent page. Therefore, we recommend that you upgrade the Web Authentication bundle so that the bundle is in the format that is used by the AireOS Wireless LAN Controllers.

To download a sample Web Authentication bundle, follow these steps:

-
- Step 1** Browse to <http://software.cisco.com/download/navigator.html>.
- Step 2** Navigate to **Products > Switches > Campus LAN Switches - Access > Cisco Catalyst 3650 Series Switches**.
- Step 3** Click a switch model.
- Step 4** Click **Wireless Lan Controller Web Authentication Bundle**.
- Step 5** Choose Release 3.7.0 and click **Download**.
- Step 6** After the download, follow the instructions provided in the Read Me file that is attached in the bundle.

**Note**

When you upgrade to Cisco IOS XE Release 3.7.5E the SSH access is lost, because it cannot use the CISCO_IDEVID_SUDI_LEGACY RSA server key. Before upgrade, generate the server key using the **crypto key generate rsa** command in global configuration mode. To verify whether the RSA server key is available on your device, run the **show crypto key** command.

**Note**

In a High Availability scenario, if you download the Web Authentication bundle to the active controller, the bundle cannot be synchronized with the standby controller. Therefore, we recommend that you also manually download the Web Authentication bundle to the standby controller.

**Note**

During an IOS image upgrade or downgrade on a PoE 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 Cisco IOS 3.7E and later releases, the process takes approximately 1 minute to complete. The microcode update occurs only during an image upgrade or downgrade on PoE switches. It does not occur during switch reloads or on non-PoE switches.

Features

The Catalyst 3650 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), 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. 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 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. 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/ps13133/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 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	v15.10.5.1
Intel 6235	V15.10.5.1
Intel 6300	v15.10.4.2
Intel 7260(11AC)	17.0.0.34, Windows 8.1
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
Broadcom 4360(11AC)	6.30.163.2005
Macbook Air (11AC)	10.9.3
Macbook Air	10.9.3
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0.1
Apple iPad3	8.0.2(12A405)
Apple iPad Air	8.0.2(12A405)
Apple iPad Mini	8.0.2(12A405)
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

Table 11 *Client Types (continued)*

Client Type and Name	Version
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 4	iOS 6.0.1
Apple iPhone 4S	8.0.2(12A405)
Apple iPhone 5s	8.0.2(12A405)
Apple iPhone 5c	8.0.2(12A405)
Apple iPhone 6	8.0.2(12A405)
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
Samsung Galaxy S4 (GT-I9500)	4.4.2
Samsung Galaxy Note (SM-900)	4.4.2

Important Notes

- A switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches is not supported.
- With Cisco Prime Infrastructure 2.1.1, the refresh config and inventory collection tasks from the switch might take anywhere from 20 minutes to 40 minutes. For more information, see CSCum62747 on the Bug Search Tool.
- Sometimes a delay is seen in the handling of ICMP reply packets when the packet timer is set to milliseconds (if the value is under 1 second). This is an expected behavior.
- Although visible in the CLI, the following commands are not supported:
 - **collect flow username**
 - **authorize-lsc-ap** (CSCui93659)
- The following features are not supported in Cisco IOS XE Release 3.7E:
 - Mesh, FlexConnect, and OfficeExtend access point deployment
 - IP-in-IP (IPIP) Tunneling

- Wireless Guest Anchor Controller (The Catalyst 3850 switch can be configured as a foreign controller.)
- Resilient Ethernet Protocol
- MVR (Multicast VLAN Registration)
- IPv6 routing - OSPFv3 Authentication
- Call Home
- DVMRP Tunneling
- Port Security on EtherChannel
- 802.1x Configurable username and password for MAB
- Link State Tracking (L2 Trunk Failover)
- Disable Per VLAN MAC Learning
- 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
- 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
- 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
- Layer 2 Tunneling Protocol Enhancements
- UniDirectional Link Routing (UDLR)
- Pragmatic General Multicast (PGM)
- 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

Scaling Guidelines

Table 12 **Scaling Guidelines**

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

Limitations and Restrictions

- 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.
- MACSec Key Agreement (MKA) encryption is not supported between switches and host devices.
- Outdoor access points are supported only when they are in Local mode.
- VRRPv3 for IPv4 and IPv6 is not supported.
- 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.
- 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.
- Cisco TrustSec VLAN-to-SGT binding cannot be enabled in pure bridging domain. You have to either manually enable IP device tracking on the ports in the VLAN, or enable SVI interface for the VLAN.
- For Cisco IOS Release 3.7E and later, Cisco TrustSec VLAN-to-SGT binding cannot be enabled in pure bridging domain. You have to either manually enable IP device tracking on the ports in the VLAN, or enable SVI interface for the VLAN.
- 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.
- Restrictions for Cisco Plug-in for OpenFlow:
 - STRIP VLAN cannot work for L2 packets that do not have a payload.
- The switch supports only physical ports in access and trunk modes. It does not support Etherchannel ports in access and trunk modes.

Caveats

- [Cisco Bug Search Tool, page 24](#)
- [Open Caveats, page 25](#)
- [Resolved Caveats in Cisco IOS XE Release 3.7.5E, page 25](#)
- [Resolved Caveats in Cisco IOS XE Release 3.7.4E, page 27](#)
- [Resolved Caveats in Cisco IOS XE Release 3.7.3E, page 28](#)
- [Resolved Caveats in Cisco IOS XE Release 3.7.2E, page 29](#)
- [Resolved Caveats in Cisco IOS XE Release 3.7.1E, page 30](#)
- [Resolved Caveats in Cisco IOS XE Release 3.7.0E, page 30](#)

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

Bug ID	Headline
CSCuo75037	High Priority Access Point Keeps Flapping when License Count is Exceeded
CSCuu13106	Traffic not recovered over cts link after hot swap of uplink
CSCuu86712	FED Process Traceback @al_lookup_add_generic_entry while enabling IPSG
CSCuz19779	ENH. DHCP malformed Offer packets get dropped (as per RFC) on 3850 CPU
CSCuz75030	license feature display issue after IOS upgrade
CSCva28133	3650 stack generates IPSG messages: %EM-4-AGED:
CSCvb26404	8 port group showing as not connect on code 3.7.3
CSCvb30329	WS-C3850-48XS/3.7.4E POST: Thermal, Fan Tests : End, Status Failed
CSCvb39796	SNMP Trap is not include entPhysicalDescr and entPhysicalName on C3850
CSCvb61022	LACP is not negotiated via Q in Q tunnel
CSCvc47165	SFP port detect link-flap error and it's in error-disabled state on 3650
CSCvc63975	Ping fails when RSPAN is configured and SRC port/vlan are in same trunk as the DEST remote-span vlan
CSCvc73079	"Speed nonegotiate" disappeared after a couple of ORI'ing SFP cables on back-to-back switch
CSCvd17125	Traceback seen after switchover with SPAN configuration

Resolved Caveats in Cisco IOS XE Release 3.7.5E

Bug ID	Headline
CSCud22987	STANDBY wcm: %OSAPI-4-TIME_SHIFT_DETECTED: Detected backward time shift
CSCun71347	Catalyst 3850 crash in Cisco Express Forwarding: IPv4 process while processing ARP throttle elements.
CSCup05919	3850 - Power given, but State Machine Power Good wait timer timed out
CSCus83638	5-GHz radio on Cisco AP beaconing but not accepting client associations
CSCuv65173	Scrubs Delta FEP Supply not responding in slot B
CSCuw17864	3650 will not forward 5246 with ip helper
CSCuw41152	'%NGWC_PLATFORM_FEP-1-FRU_PS_SIGNAL_FAULTY' message is not output

Bug ID	Headline
CSCuy67349	3650/3850 IPv6 ND RAGUARD drops RS packets (ICMPv6 type 133)
CSCuy83302	Catalyst 3850 - Port-security may interfere with spantree bpdu guard
CSCuy99151	3850 failing Inline Power Controller Tests
CSCuz06686	Port-channel no drops although member port drops on C3650/C3850
CSCuz08086	PD's not getting PoE on multiple interfaces in 3850 stack
CSCuz24063	Storm-control configured on port-channel cannot reflect to member link
CSCuz28295	TCN generate late and mac learn issue on 3650 stack after RSTP TCN
CSCuz54670	WS-C3850-24XS: Local port still up when TX fiber removed from 10G SFP
CSCuz57493	High CPU observed in punjectrx fed-ots-main thread
CSCuz60141	SDP drops causing stack issues.
CSCuz87489	breelay: No crashinfo generated since core resource was not set
CSCuz89095	3850 switch at Provisioned state after a random reload/power outage
CSCuz98375	OSPF flaps on Cat3850 with 1s/3s timers with 03.07.03E
CSCva02227	C3850s in stack don't return ports 45-48 when polled through SNMP
CSCva13231	CRC/Corrupted packets after a link failure with MACSEC and 802.1q (3850)
CSCva21500	Cat3650 interface don't up when "speed nonegotiate" is applied
CSCva22528	3850:Traffic only flowing between ports on Port Asic
CSCva22545	LACP with mode active doesn't come up in 3.7.4 .
CSCva25359	NOVA: Evaluation of glibc vulnerabilities on IOS/IOS-XE
CSCva40478	ip dhcp snooping trust on port-channel does not reflect on member link
CSCva43372	Interoperability - remote side CRC error
CSCva55550	incorrect CDP/LACP/UDLD neighbor information on 3850 - 3.7.3 and 3.7.4
CSCva76630	BENI MR5: RSPAN traffic is not encrypted on CTS MACSEC SAP link
CSCva92074	%PLATFORM_PM-6-MODULE_ERRDISABLE output when inserting SFP
CSCva98034	EICORE_GET_NEXT_MC: end of items / Error using the collection / Cat3850
CSCvb22505	Port security mac address not aging out when relearned from a Channel
CSCvb26637	IGMPv2 leave messages sent back to ingress interface

Bug ID	Headline
CSCvb34556	Cat3850 - 10G member of Ether-channel with LACP is continuously flapping
CSCvb56934	commit to 3.7.x and 16.3.x Zero RX counters on te1/1/3 port on bootup
CSCvb60511	SSH doesn't work with MACSEC configured between 3850 and 4500
CSCvb65304	Output drops and Output errors increment simultaneously in show interfaces
CSCvb97732	3850/3650 Switch Crashes Following "network-policy" Configuration Change on Interface
CSCvc26787	%LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/1/4, changed state to down
CSCvc62241	SGACL enforcement under VRF unexpectedly blocking traffic

Resolved Caveats in Cisco IOS XE Release 3.7.4E

Bug ID	Headline
CSCUw23090	3650 trunk interface malfunction issue when speed nonegotiate is applied
CSCUw59595	Cannot get expected packet rate for PQ in output QoS policy
CSCUw66770	udld err-disbale on remote device on reloading 3650
CSCUw88823	Traceback on 3650 during reload
CSCUw95074	3650 Packets with fragment offset bit hit wrong class-map
CSCUx16194	3650 does not change to link down on removing SFP Tx cable
CSCUx16628	Without IPv6 enabled, IPv6 traffic to FF02::2 and FF02::3 is send to CPU
CSCUx28536	Interface stays in down state after link flap on the neighbor
CSCUx41556	QoS cannot behave normally on 3650 with S/W ver.3.7.2E, 100M/full
CSCUx56459	Stack reload due to doubLast Updated: Feb 16, 2017Last Updated: Feb 16, 2017le free (FREEFREE)
CSCUx64558	Inline power stops on the port in err-disabled state.
CSCUx71386	After clear counters is issued, the Xmit-err shows a very huge number
CSCUx77360	Cat3650-24TS-S connection issue with FUJITSU switch SR-S324TL2
CSCUy21298	Performance Monitoring not working on 3650
CSCUy44807	Switch crashes with Segmentation fault(11), Process = NGWC DOT1X Process
CSCUy46096	Uncabling SFP port up/up when "speed nonegotiate" is configured

Resolved Caveats in Cisco IOS XE Release 3.7.3E

Bug ID	Headline
CSCum06547	NG3K standalone crashed after removed energywise domain
CSCus17795	Same port name displays in lower and upper case during OpenFlow configuration
CSCus84849	ipdt difference in config and default configuration
CSCus99269	MCMA: dACL should not be synced to MA & should be allowed on MA as well
CSCut14397	Bad parsing when keyword is truncated during OpenFlow LXC configuration
CSCut25533	PnPA: non-vlan CLI should only apply to newly bootup devices
CSCut87285	MAC address being learnt on an individual Port-channel member interface
CSCut88813	WLAN cannot be configured with a space in psk shared key on NGWC 3.7
CSCuu09331	CTS link not passing traffic after SSO
CSCuu15831	Switch reboots when SPAN configured under "cts manual"
CSCuu34717	3850 cts enforcement for multicast traffic
CSCuu36487	Cat3k: OF: Vlan strip action doesnot work for ipv6 packets
CSCuu49195	Access session cache entries not getting updated
CSCuu56466	"Total output drops" counter of a certain ports does not increment
CSCuu56511	OutDiscards counter does not increment
CSCuu66503	HTTPS: IOS HTTPS client not enforcing subject-name verification
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuu85807	Switch returns wrong OID when standalone
CSCuu87659	CpmCPUTotal5minRev average value of stack switch 2 on 3850 is incorrect.
CSCuu97048	Traffic is dropped due to static mac entry on foreign interface
CSCuu97550	4500X - SNMP dot1dTpFdbPort retuning incorrect value
CSCuv02964	Memory leak with dot1x on IOS-XE switch
CSCuv07427	TCP connection cannot be established with Openflow agent due to
CSCuv13351	MAC address is learned on RSPAN vlan after stack switchover
CSCuv14890	DHCPv6 solicit frame (IPv6 multicast) frame replication issues
CSCuv19160	Config lock mode during redundancy prevents PnP redirection.
CSCuv19204	NTP Server take 15 - 18 minutes to sync with API-EM clock
CSCuv19773	"nmsp attach suppress" not being added into run-config on WS-C3850-24P
CSCuv20618	3650 - Port goes down when 'no mdix auto' is configured, POE works fine

Bug ID	Headline
CSCuv20921	mac address-table learning command should not be allowed for RSPAN vlan
CSCuv22736	After reload, C3850-NM-4-10G/GLC-SX-MM not linkup with speed nonegotiate
CSCuv36348	management port can be added to OpenFlow config
CSCuv42533	Flow addition failing with wildcard match
CSCuv62574	GRE tunnel in up/down state when tunnel source configured via interface
CSCuv78424	Unicast ARP packets are duplicated
CSCuv85232	openflow exclusive config not cleared on standby
CSCuv88334	mismatch in the rf parameters mode between cli/gui
CSCuw06386	Flows are not prgrmd in PD after consecutive clearopenflow switch1 cntrl
CSCuw19798	GRE Tunnel not working on Catalyst 3850
CSCuw21694	Invalid flow count increasing in PD when i remove and add OF ports
CSCuw22050	Switch reports Power device detected when non device is connected
CSCuw28638	3650 Rebooting during EAP-TLS authentication
CSCuw36865	L2 switched traffic matched by L3 SVI VACL in the output direction
CSCuw38233	Mobility tunnel between MA/MC drops when default egress policy is deny
CSCuw39020	access-session vlan-assignment ignore-errors breaks dynamic vlan assign
CSCuw55669	Crash is seen in iosd on switch and auth-mgr
CSCuw67734	CFD CSCun37216 entAliasMappingIdentifier broken on 03.07.02E...
CSCuw73525	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr
CSCuw82216	Catalyst3850: Upgrade in install mode corrupts the flash - EXT2-fs error
CSCuw98232	Fixing build breakage for 15.2(3)E/3.7.3E which happened with CSCuv62574

Resolved Caveats in Cisco IOS XE Release 3.7.2E

Bug ID	Headline
CSCup55828	Need error message when using a wrong image to do software install
CSCuq44139	Need to disable Macsec for half-duplex mode on downlink ports
CSCus69196	After overnight ping traffic on active, standby sw#6 crashes at iosd

Bug ID	Headline
CSCus89656	Trust, DSCP transparency, COPP not working when a member comes up
CSCut26365	Packet drop on 3850 by an unrelated ACL entry
CSCut49440	3850 class-map "match" doesn't work correctly

Resolved Caveats in Cisco IOS XE Release 3.7.1E

There are no caveats to list here.

Resolved Caveats in Cisco IOS XE Release 3.7.0E

Bug ID	Headline
CSCun29064	Show switch details show false stack linkdown
CSCun54503	No QoS Per Port Per VLAN configuration option 3650 & 3850
CSCuo00561	Switch unusable for 8 minutes after ?default interface? w/ L3 CTS config
CSCup40892	Wireless clients may be stuck in idle state when FQDN feature is enabled
CSCup62150	After Inter-Switch Roam, QoS policy is not applied to Client
CSCuq02810	STP check bypassed for data traffic sent to switch mac address

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 3E Release documentation at this URL:
<http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/tsd-products-support-series-home.html>
- Catalyst 3650 switch documentation at this URL:
http://www.cisco.com/go/cat3650_docs
- 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.

© 2014-2016 Cisco Systems, Inc. All rights reserved.

