Release Notes for Catalyst 3650 Series Switch, Cisco IOS XE Release 3.3.xSE

First Published: October 10, 2013
Last Updated: January 15, 2014

OL-30563-02

This release note describes the features and caveats for the Cisco IOS XE 3.3.xSE 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
- What's New in Cisco IOS XE Release 3.3.1SE, page 2
- Supported Hardware, page 2
- Device Manager System Requirements, page 7
- Web UI Software Requirements, page 7
- Finding the Software Version and Feature Set, page 8
- Upgrading the Switch Software, page 8
- Features, page 8
- Interoperability with Other Client Devices, page 9
- Important Notes, page 10
- Limitations and Restrictions, page 12
- Caveats, page 12
- Documentation Updates, page 22
- Troubleshooting, page 22
- Related Documentation, page 22
- Obtaining Documentation and Submitting a Service Request, page 23

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 and Cisco StackPower. 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+), modular and field replaceable network modules, 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 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 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 12.

Supported Hardware

Switch Models

Table 1 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

Table 1 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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
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

Table 1 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 3650-24TD-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 3650-48FQ-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

Table 1 Catalyst 3650 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
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 3650-48FQ-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

Other Supported Products

Table 2 lists the supported products of the Catalyst 3650 switch.

Table 2 Catalyst 3650 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 3 lists the specific supported Cisco access points.

Table 3 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

Compatibility Matrix

Table 4 lists the software compatibility matrix.

Table 4 Software Compatibility Matrix

Catalyst 3650	Cisco 5700 WLC	Cisco 5508 or WiSM2	MSE	ISE	ACS	Cisco PI
03.03.01SE	03.03.01SE	7.5[1]	7.5	1.2	5.2, 5.3	2.0.1[2]

1. 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.
2. Available Q4 CY13.

Device Manager System Requirements

Hardware Requirements

Table 5 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, XP, Vista, or Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox 1.5, 2.0 or later with JavaScript enabled.

Web UI Software Requirements

- Operating Systems
  - Windows XP
  - Windows 7
  - Mac OS X 10.7.5
- Browsers
  - Google Chrome—Version 23.x
  - Microsoft Internet Explorer—Versions 10.x
  - Mozilla Firefox—Version 22.x

Finding the Software Version and Feature Set

Table 6 shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 6 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
03.03.01SE	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 3SE (Catalyst 3650 Switches)* at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3650/software/release/3se/system_management/configuration_guide/b_sm_3se_3650_cg.html

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 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, 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 all IP Base features plus full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). The IP Services feature set includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and 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/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 7 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 7 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 6.0.1
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

Table 7 Client Types (continued)

Client Type and Name	Version
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	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

Important Notes

- A switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches is not supported.
- Although visible in the CLI, the following commands are not supported:
  - **switchport mode dot1qtunnel**
  - **collect flow username**
- Although visible in the CLI, the **authorize-lsc-ap** command is not supported. (CSCui93659)
- 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.

Caveats

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

https://tools.cisco.com/bugsearch/search

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

- Open Caveats, page 12
- Resolved Caveats in Cisco IOS XE Release 3.3.0SE, page 16
- Resolved Caveats in Cisco IOS XE Release 3.3.1SE, page 20

Open Caveats

- CSCug52286

  After FlexLink load balancing is removed from an active interface, all packets are dropped.

  The workaround is to remove the FlexLink configuration from the interface and then reconfigure FlexLinks on the interface.

- CSCug63412

  When an IPv6 Multicast Listener Discovery (MLD) group entry is programmed in the overflow ternary content-addressable memory (TCAM), multicast traffic to this group is flooded across all ports in the same VLAN instead of sending the multicast traffic to the interested multicast client.

  There is no workaround.

- CSCug87984

  When you boot the switch with the factory default configuration, the system configuration dialog prompts are interrupted by the following message:

  ```
  % Generating 1024 bit RSA keys, keys will be non-exportable...
  ```

  The workaround is to ignore the message and type yes or no to the dialog prompts.

- CSCuh25601

  ARP traffic is occasionally dropped. The ARP loss corresponds with buffer counter under “failures” incrementing in the output of **show platform punt client**.

  If IP device tracking is not required and neither dot1x or DAI is used, then the workaround is to add the **nmsp attachment suppress** command at the interface level of all switch ports. This stops ARP snooping from being enabled on the ports.

- CSCuh10592

  When a power supply is inserted into the chassis without a power cord, the **show environment power** command displays the status of Sys Pwr and PoE Pwr as Good. This is a reporting issue and has no functional impact.

  There is no workaround.

- CSCuh56417

  The **clear counters d2** command does not clear the 802.11ac (d2) counters on AP. This could result in an issue when a debug operation is being performed and the fresh counters for the 802.11ac radio are needed to be checked.

  The workaround is to reboot the AP.

- CSCuh73828

  During an SSO and shutdown of interfaces on which APs are connected, the following error message is displayed:

  ```
  FED_QOS_ERRMSG-3-TABLEMAP_INGRESS_HW_ERROR
  ```

  There is no workaround. There is no functional impact.

- CSCuh97237

  The Wireless Guest Access feature does not support wireless clients configured with a static IP address that are trying to join the foreign controller.

  The workaround is to ensure that all clients joining the wireless guest access WLAN on the foreign controller are configured to acquire their IP address from the DHCP server.

- CSCui00072

  Some VLANs may not be able to learn the multicast router or querier by IGMP snooping.

  The workaround is to use the static IGMP querier and static mrouter.

- CSCui07364

  In a cross-stack EtherChannel with trunk configured, port flapping occurs when a VLAN is added or removed from the list of allowed VLANs. This problem occurs with both static and dynamic trunk port configurations.

  There is no workaround.

- CSCui12012

  You cannot modify the type set table-map action in a policy-map when the policy-map is attached to an interface.

  The workaround is to remove the policy from the interface, remove the action, and add the new action.

- CSCui23689

  When the startup configuration in a switch stack includes IPv6 first-hop security (FHS) configuration information (that is, default IPv6 snooping policy and default IPv6 nd suppress policy have been applied to one or more VLANs), some switched virtual interfaces (SVIs) are in the stalled state after the switch stack is rebooted and the stalled SVIs have no FHS configuration.

  The workaround is to used the **shutdown** and **no shutdown commands** on the affected SVIs.

- CSCui28803

  In PIM Sparse Dense mode, when the scaled number of Mcast Groups/Clients present (500 Groups), IGMP traffic is not received on a few groups.

  The workaround is to reboot the switch.

- CSCui36531

  During boot up or after a power supply is removed and reinserted, the following error message is displayed:

  ```
  %NGWC_PLATFORM_FEP-1-FRU_PS_SIGNAL_FAULTY
  ```

  There is no workaround. There is no functional impact.

- CSCui40588

  After a TACACS authentication, the wireless GUI is not available on the switch.

  The workaround is to use CLI interface (Telnet, Console, SSH) and configure the device.

- CSCui56229

  When configuring the shaper policy, the uplink 1G port follows the uplink 10G port, which causes the uplink 1G port shaper accuracy issue.

  The workaround is to use the downlink 1G port instead of the uplink 1G port when you need accurate shaper policy.

- CSCui56842

  When Flexible NetFlow is configured on wireless SSID, multicast traffic received or sent by wireless clients is not reported.

  There is no workaround.

- CSCui57827

  When a fiber interface is configured with the default configuration, the following error message is displayed:

  ```
  ETHCNTR-3-LOOP_BACK_DETECTED
  ```

  and the interface is placed in the error-disabled state.

  The workaround is to configure the interface with the **no keepalive** command.

- CSCui59068

  On a switch stack, 2000 802.1X/MAC Authentication Bypass sessions are authorized with security group tags (SGT) downloaded from the ISE and authentication timer enabled. After some period of time, the active IOSd process stops running for some time.

  There is no workaround.

- CSCui65778

  When the standby switch reboots with a line-by-line configuration, synchronization failure.

  The workaround is to manually remove the LACP configuration from under the interface.

- CSCui67207

  On booting a switch with a QoS policy attached to one or more Etherchannel members, a warning message is displayed for each member in the channel starting from the second member.

  There is no workaround.

- CSCui67856

  Traffic drops in the process when HSRP on the interface of a switch comes up and preempts the HSRP switch that is active.

  This occurs when HSRP preemption is enabled on the switches that are part of the same HSRP group. When the HSRP active switch with higher priority becomes nonoperational, the HSRP standby switch becomes active and starts to forward traffic. If the old active switch, which is nonoperational, becomes operational again and preempts the new active switch, traffic is dropped. This issue is observed when a user with administrative privileges does a shut down/no shut down on the HSRP active switch interface.

  There is no workaround.

- CSCui69907

  Policing does not work as expected when a class map contains multiple match VLAN statements.

  The workaround is to create a class map with multiple VLANs in a single match; for example:

  ```
  class-map VLAN
  match vlan3, 4
  ```

- CSCui69984

  The output of the **show int transceiver supported-list** command does not show the complete list of supported 10G optics modules.

  The workaround is to view the compatibility tables at this URL:

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

- CSCui75983

  After rebooting the switch stack, ingress traffic matching a policy with multiple class maps of different ACLs might match the wrong class map.

  The workaround is to remove the policy and reapply the policy on the affected interface.

- CSCui78313

  On an input policer policy, the classification counter does not accurately reflect matches on a class map with a ACL or DSCP clauses.

  The workaround is to monitor the police counter instead of the classification counter.

- CSCui83014

  During an SSO, when traffic from an egress port on the active switch is forwarded to an egress port on a member switch using alternate path, traffic is dropped.

  There is no workaround.

- CSCui84577

  When a 10G interface is configured with the unidirectional link detection (UDLD) message time equal to 7 and the switch on the other end of the 10G link is rebooted, the 10G interface goes into a UDLD error-disabled state.

  The workaround is to configure the UDLD message time as 15 or more.

- CSCui88474

  QoS policies created through Web UI are not listed on the Web UI page.

  There is no workaround.

- CSCuj10024

  After an SSO on the 5760 controller with HA, some clients fail to rejoin.

  The workaround is to decrease the number of clients connecting to the controller.

- CSCuj27803

  When a policy contains multiple match statements in a class, the classification counter displays incorrect results.

  There is no workaround.

- CSCuj31712

  Removing and reinserting SFP modules causes the port to go into an error-disabled state.

  The workaround is to use the **shutdown/no shutdown** commands on the port.

- CSCuj42801

  When the **snmp-server enable traps stackwise** command is used to set SNMP traps for the CISCO-STACKWISE MIB, the only trap set is for port status; traps are not set for the other MIB objects.

  There is no workaround.

- CSCui84582

  Bcast queue is full when IGMP is disabled.

  There is no workaround.

Resolved Caveats in Cisco IOS XE Release 3.3.0SE

- CSCua75283

  The following tracebacks are noticed on normal setup:

  ```
  DATACORRUPTION-1-DATAINCONSISTENCY: strstr_s: dmax exceeds max,  -PC= 0x240BE60Cz
  -Traceback= 190BA74z 182D4C8z 5E68CD5z 5E68B63z 55817EBz 55815D7z 558154Dz 5580E60z
  5580444z 55802CAz
  ```

  There is no workaround. There is no functional impact.

- CSCuc12774

  When the Ethernet management port receives a frame whose destination MAC address is not FA1, it does not drop the traffic. Instead, the port uses the vrf mgmtVrf routing table to route the traffic back.

  There is no workaround.

- CSCuc95293

  In very rare cases, all traffic to and from the switch ceases; all access points and LAG links disconnect as the switch fails to transmit the LACP PDUs; however, the management interfaces function.

- CSCud11467

  When the same PV HQOS policies are applied to both directions of an interface, the output policy stops working when the input policy is removed.

  The workaround is to detach the output policy and reapply it to the interface.

- CSCud11552

  After a HQOS policy is attached to interface and the interface speed or bandwidth is changed while the policy is attached, the HQOS policy gets detached from the interface.

  The workaround is to detach the policy, change the bandwidth or speed of the interface, and reattach the policy.

- CSCud54501

  The class video counters for the AP port policy appear as zero when you use the **show policy-map interface wireless ap** command.

  There is no workaround.

- CSCud54725

  When a class is removed from a queuing policy map that is attached to a wired port, the queue programming in the hardware is removed.

  The workaround is to remove the policy from the port before making modifications.

- CSCud55333

  When the incoming rate is far beyond the rate configured in a policy map through policing, the traffic is not properly shaped.

  The workaround is to configure the policy map with priority level 1 percent and priority level 2 percent instead of configuring the policy with priority level x and policing.

- CSCud56426

  When you modify the webauth virtual IP while there are active webauth sessions, the session stays in the pending-delete state and you cannot create a new session.

  The workaround is to not make CLI changes when authorized webauth sessions are in use.

- CSCud60008

  When a policy with priority and a policer is attached to a range of interfaces on an uplink, in some scenarios, any change made to the policer rate causes the policy to be unprogrammed on one or more ports.

  The workaround is to remove the policy from the affected ports and reattach it.

- CSCud60070

  When configuring policy maps using absolute values, the maximum rate is limited to 2G/second.

  The workaround is to configure policy maps using the **priority level 1 percent *x*** command instead of configuring absolute values with the **priority level 1 *x*** command.

- CSCud62982

  When policers are attached to uplink interfaces using the **range** command, the policers do not always work.

  The workaround is to attach the policy to each port, one by one.

- CSCud63110

  In a hierarchical queueing policy, a table map under the child policy continues to mark traffic after the policy is detached from an interface.

  The workaround is to attach a default policy, for example:

  ```
  policy-map trust-cos
       class class-default
       set cos cos table default
  ```

  You then detach it.

- CSCud63823

  After a queuing policy is deleted from one uplink port (10 G), the queueing policy on the other 1-G uplink stops working.

  The workaround is to detach the policy and reattach it.

- CSCud65034

  When using hierarchical policies, the child classification does not work properly when its matching value is a subset of the parent class's matching values for COS, DSCP, UP, and PREC classes.

  The workaround is to configure hierarchical policies to achieve one of these results:

  - The parent class has only class-default and the child class has user-defined classes.
  - The parent class has user-defined classes and the child has only class-default.

- CSCud71747

  The **snmp get** command on cLMobilityExtMoMcLinkStatus for a given mobility controller (MC) and on cLMobilityExtMcAssocTime for a given mobility controller's client returns incorrect values.

  The workaround is to use the following commands:

  - **show wireless mobility oracle summary** to display the link status between the mobility oracle and the mobility controller
  - **show wireless mobility controller client summary** to display the client association time.

- CSCud72626

  After a per-VLAN policy is removed from a port, the policer stays active. The VLAN has an SVI with a policy attached that is performing a set.

  The workaround is to remove the policy from the SVI before removing it from the port.

- CSCuf86171

  The DHCP snooping database agent fails to start while changing the DNS entry that the URL pointed to or when restarting the DHCP server. To avoid this issue, use another file transport mechanism like SCP or TFTP.

  The workaround is to reload the switch.

- CSCuf93185

  When a 1-G port on a Catalyst 3850 switch is connected to a 10-G port on a 5760 controller with a 1-G SFP module, the 10-G controller port stays up even when the switch port is shut down.

  There is no workaround.

- CSCug38523

  In WebUI, it takes up to 10 to 15 seconds for the home page to load.

  There is no workaround.

- CSCug41165

  If you copy and paste several wireless configuration lines into the configuration, the system drops the first few characters from every other line. The number of characters dropped appears to be related to how long the command takes to execute. The issue does not occur on non-wireless configuration lines.

  The workaround is to copy and paste line by line.

- CSCug58178

  Multicast traffic travels on the WLAN-mapped VLAN rather than on the AP-group mapped VLAN when an AP is placed in an AP group where VLAN is overridden for the SSID and a client associates with the AP that is broadcasting this SSID.

  There is no workaround.

- CSCuh20848

  The console displays %IPC-5-WATERMARK log messages repeatedly.

  There is no workaround. There is no functional impact.

- CSCui57827

  When a fiber interface is configured with the default configuration, the following error message is displayed:

  ```
  ETHCNTR-3-LOOP_BACK_DETECTED
  ```

  and the interface is placed in the error-disabled state.

  The workaround is to configure the interface with the **no keepalive** command.

- CSCui59004

  When the Network Time Protocol (NTP) configuration is removed from the switch, the Cisco IOS software unexpectedly halts.

  There is no workaround.

Resolved Caveats in Cisco IOS XE Release 3.3.1SE

- CSCsl45701

  The TACACS+ per VRF feature is not working and authentication fails.

  The workaround is to use the TACACS+ source interface from the global routing table, not VRF.

- CSCuc63146

  Port-channel interface flap when changing vlan allowed list.

- CSCud08538

  WCM unresponsive on 2M at pthread_mutex_lock.

- CSCue49527

  Controller should use a new session ID for every fresh authentication.

  There is no workaround.

- CSCug18767

  Apple devices are unable to login to WEB authentication.

  The workaround is to connect to the WEB authentication SSID, open a WEB browser, close the browser, change the device's SSID settings to disable Auto-login, and then re-open the browser. The client should then WEB authenticate successfully.

- CSCui36499

  %PLATFORM_THERMAL-1-FRU_FAN_FAILURE

  When the ambient temperature of the switch changes and the fan has to adjust accordingly, the RMP fan values programmed in the MCU may be different than those read from the fan. As a result, this intermittent error message occurs.

  There is no workaround.

- CSCui69999

  Switches with different images in the same stack are not supported.

  The workaround is to ensure that all switches in the same stack are running the same image.

- CSCuj21417

  AID leak causing stale client entries on WLC

  The workaround is to disconnect and reconnect AP to clear stale clients.

- CSCuj34025

  AUP PDF page does not display in PDF format.

- CSCuj48089

  The switch is stuck in a broadcast queue that prevents packets to enter the queue.

  The workaround for ARP is to re-enable NMSP (no nmsp attachment suppress). This action will allow ARP traffic to be processed. A reload will also clear this state.

- CSCuj51372

  In rare cases, Mac Learning does not occur for either ports 1-24 or ports 25-48 on one stack member in a switch stack. The other stack members are not affected.

  The workaround is to reload the affected stack member.

- CSCuj57007

  DHCPACK with no DHCPOPT_LEASE_TIME option field should trigger IPDT.

  The workaround is to release and then renew the IP address on the Lenovo W520.

- CSCuj78610

  High cpu issue at TUD on 03.12.19.EZP for process Auth-proxy HTTP dae.

  There is no workaround.

- CSCul03186

  Hotspot error occurs intermittently on iPad.

- CSCul06456

  There is no SNMP MIB object available to add a local netuser or guest user.

  The workaround is to use the CLI to add the user.

- CSCul06619

  Stale IPDT entries causing client to be stuck in DHCP reqd state.

- CSCul13504

  Web authentication logout pop-up window is not disabled.

  There is no workaround.

- CSCul27659

  The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned one Layer 2 MGID.

  L2 MGID is not sent to AP for Guest WLANs. So if DHCP NAK (which is broadcast as per current code) is received by AP it gets dropped and never reaches end client.

- CSCul27717

  Cisco APs are disassociated in a large scale setup (500 or more APs) when the **debug capwap** or **debug dtls** command is enabled (even with a MAC filter in place).

  The workaround is to disable these debug commands.

- CSCul30051

  Clients fail authentication (psk/dot1x) due to uncreated dot1x interface for the AP.

  The workaround is to reboot the AP on the client that cannot authenticate.

Documentation Updates

Catalyst 3650 Switch Getting Started Guide

- The “Managing the Switch” section erroneously includes information about Cisco Network Assistant (CNA). CNA is not supported in this release.

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 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/en/US/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.
