Release Notes for Catalyst 3850 Series Switch, Cisco IOS XE Release 3.2.xSE

First Published: January 29, 2013
Last Modified: November 14, 2013
OL-28114-04

This release note describes the features and caveats for the Cisco IOS XE 3.2.xSE software on the Catalyst 3850 series switch.

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

Contents

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

Introduction

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

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

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

For more information about the Cisco IOS XE software, see
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps9442/ps11192/ps11194/QA_C67-622903.html

What's New in Cisco IOS XE Release 3.2.3SE

Cisco Prime Infrastructure (PI) 2.0

Cisco PI 2.0 manages both wired and wireless LAN devices such as Catalyst 3850 switches, Cisco 5760 controllers, Cisco 5500 series wireless controllers, and access points. PI 2.0 provides unified management for the features that are common to both switches and wireless controllers. After your devices are added to Prime Infrastructure, you can use the Initial Device Setup workflow to configure the wired and wireless features on switches and controllers.

For more details on PI 2.0, see the documents at this URL:

http://www.cisco.com/en/US/products/ps12239/tsd_products_support_series_home.html

Captive Portal Bypassing for Local Web Authentication

In Cisco IOS XE Release 3.2.2SE, Apple devices that need to resolve Wireless Internet Service Provider roaming (WISPr) and have support for captive portal bypass could not get local web authentication. This issue is resolved in Cisco IOS XE Release 3.2.3SE.

If you have configured virtual IP resulting in a successful web authentication, but when you log out, you receive a popup window prompting you to click a link to log out, you can disable this popup by following these steps:

	Command	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *map-name* **Example:** `Switch(config)# parameter-map type webauth named`	Configures a name for the parameter map and enters the parameter map configuration mode.
Step 3	**type consent** **Example:** `Switch(config-params-parameter-map)# type consent`	Configures the parameter type as consent. **Note** You can disable the popup window only if the parameter map type is configured as consent.
Step 4	**logout-window-disabled** **Example:** `Switch(config-params-parameter-map)# logout-window-disabled`	Disables the web authentication logout popup window.
Step 5	**end** **Example:** `Switch(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

For more information about captive portal bypassing, see http://www.cisco.com/en/US/docs/wireless/controller/7.5/config_guide/b_cg75_chapter_01010001.html

What's New in Cisco IOS XE Release 3.2.2SE

New and Enhanced GUI Features

In the earlier releases, the controller web user interface is accessed by entering http://*ipaddress* (the *ipaddress* is the controller IP address) in the browser. Now, you can enter http://*ipaddress*/wireless in the browser, which will also allow you to access the web user interface.

The controller web user interface is enhanced to support the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- NMP System Summary
- Management Port
- Wireless Management

- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of controller, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification—friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the controller for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.

Enhanced Bring Your Own Device (BYOD) Support

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users and their devices. A Cisco Identity Services Engine (ISE) Advanced License provides the tools that you need to allow employees to securely use personal devices on a corporate network.

- Device Profiling—When a client device tries to associate with a WLAN, the switch collects information related to DHCP, RADIUS, HTTP, and so on and sends that information in the form of RADIUS packets to the Cisco Identity Services Engine (ISE). As a result, the client type can be determined.
- Single SSID and Dual SSID support—In the single SSID scenario, one SSID is used for certificate enrollment, provisioning, and network access. In the dual SSID scenario, one SSID provides certificate enrollment and provisioning and a second SSID provides secure network access. This certificate is used by the client to authenticate with the ISE EAPTLS protocols after it is provisioned in the first SSID (open). For more details, see the *Cisco Identity Services Engine User Guide* at this URL:

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_user_guide.html

Fast SSID Changing

Fast SSID changing allows wireless clients to move from one SSID to another without delay. For more information, see Configuring Fast SSID Changing, page 47.

Supported Hardware

Switch Models

Table 1 Catalyst 3850 Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48T-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24P-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48P-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48F-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24T-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set
WS-C3850-48T-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Base feature set
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Base feature set
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Base feature set

Table 1 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC power supply 1 RU, IP Base feature set
WS-C3850-24T-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-48T-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350WAC power supply 1 RU, IP Services feature set
WS-C3850-24P-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Services feature set
WS-C3850-48P-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715WAC power supply 1 RU, IP Services feature set
WS-C3850-48F-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100WAC power supply 1 RU, IP Services feature set
WS-C3850-24PW-S	IP Base	Cisco Catalyst 3850 24-port PoE IP Base with 5 access point license
WS-C3850-48PW-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base with 5 access point license

Network Modules

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

Table 2 Supported Network Modules

Network Module	Description
C3850-NM-4-1G	Four 1-Gigabit SFP module slots. Any combination of standard SFP modules are supported. SFP+ modules are not supported.
C3850-NM-2-10G	Four SFP module slots: • 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: • 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.

Table 2 Supported Network Modules (continued)

Network Module	Description
C3850-NM-4-10G	Four 10-Gigabit slots or four 1-Gigabit slots. **Note** This is only supported on the 48-port models.
C3850-NM-BLANK	No uplink ports.

Optics Modules

The Catalyst 3850 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 3 lists the supported products of the Catalyst 3850 switch.

Supported Access Points

Table 3 Catalyst 3850 Switch Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 1040, 1140, 1260, 1600[1], 2600, 3500, 3600
Mobility Services Engine	3310, 3350, 3355, Virtual Appliance
Identity Services Engines (ISE)	ISE 1.1.1 on 3315, 3355, 3395 and Virtual Instance
Cisco Prime Infrastructure	Cisco Prime Infrastructure 2.0

1. AP 1600 will not work with 5508/WiSM2 as MC in converged access mode.

Table 4 lists the specific supported Cisco access points.

Table 4 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

Table 4 Supported Access Points (continued)

Access Points	
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

Compatibility Matrix

Table 5 lists the software compatibility matrix.

Table 5 Software Compatibility Matrix

Catalyst 3850	5760	5508 or WiSM2	MSE	ISE	ACS	Cisco PI
3.2.0SE	3.2.0SE	7.3.112.0	—	1.1.1MR	5.2	NA
3.2.1SE	3.2.1SE	7.3.112.0[1]	—	1.1.3, 1.1.2	5.2, 5.3	NA
3.2.2SE	3.2.2SE	7.3.112.0 and the 7.5 Release	—	1.1.3, 1.1.2	5.2, 5.3	NA
3.2.3SE	3.2.3SE	7.3.112.0 and the 7.5 Release	—	1.1.3, 1.1.2	5.2, 5.3	2.0

1. IRCM Feature: Seamless roam between 5760 / 3850 and 5508 / WiSM2 with 7.3 MR1 running new mobility.

Express Setup System Requirements

Hardware Requirements

Table 6 Minimum Hardware Requirements

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

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

Software Requirements

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox 1.5, 2.0 or later with JavaScript enabled.

Web UI System Requirements

Software Requirements

- Supported Browsers
  - Google Chrome—Version 26.x
  - Microsoft Internet Explorer—Versions 8.x, 9.x and 10.x
  - Mozilla—Version 20.x

Finding the Software Version and Feature Set

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

Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
03.02.00SE	15.0(1)EX	10.0.100.0	152-2.JN
03.02.01SE	15.0(1)EX1	10.0.101.0	152-2.JN
03.02.02SE	15.0(1)EX2	10.0.111.0	152-2.JN
03.02.03SE	15.0(1)EX3	10.0.120.0	152-2.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 *Cisco IOS File System, Configuration Files, and Bundle Files Appendix* at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/system_management/appendix/swiosfs.html#wp1311040

Note If you are upgrading from Cisco IOS XE Release 3.2.1 or earlier and you configured auto QoS on the switch, you must remove all auto QoS configurations maps, class maps, and access lists before you reboot the switch with the new software. Follow these steps to remove the auto QoS configurations.

Step 1 In privileged EXEC mode, record all current auto QoS configurations by entering this command:

show auto qos

Step 2 In interface configuration mode, run the appropriate **no auto qos** command on each interface that has an auto QoS configuration.

Step 3 Return to privileged EXEC mode, and record any remaining auto QoS maps class maps, policy maps, access lists, table maps, or other configurations by entering this command:

show running-config | i AutoQos

Step 4 In global configuration mode, remove the QoS class maps, policy maps, table maps, and any other auto QoS configurations by entering these commands:

a. **no policy-map** *policy-map-name*

b. **no class-map** *class-map-name*

c. **no ip access-list extended** *Auto-QoS-x*

d. **no table-map** *table-map-name*

e. **no table-map policed-dscp**

Step 5 Return to privileged EXEC mode, and verify that all auto QoS configurations have been removed by entering the following commands:

a. **show running-config | i AutoQos**

b. **show auto qos**

Step 6 Write the changes to the auto QoS configuration to NV memory by entering the **write memory** command.

Step 7 Reboot the switch with the new or upgraded software image.

Step 8 Reconfigure auto QoS for the interfaces recorded in Step 1.

Features

The Catalyst 3850 switch supports three different feature sets:

- LAN Base feature set—Provides basic Layer 2+ features, including access control lists (ACLs) and quality of service (QoS) and up to 4094 VLANs.
- IP Base feature set—Provides Layer 2+ and basic Layer 3 features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), ACLs, QoS, static routing, EIGRP stub routing, PIM stub 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 AP count license is required to use the Catalyst 3850 switch as a wireless controller.

The device has these features:

- Security, page 12
- Ease of Operations, page 14
- Deployment and Control Features, page 14
- High Availability, page 16
- High-Performance IP Routing, page 17
- Quality of Service, page 17
- Wireless Features, page 18

Security

- IEEE 802.1x, DHCP snooping, IP Source Guard, Control Plane Protection, and Wireless Intrusion Prevention Systems (wIPS) security features are available. With a variety of wired and wireless users connecting to the network, the switch supports session-based networking, where each device connected to the network is identified as one session.
- Port security secures access based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.
- DHCP snooping filters untrusted DHCP messages between untrusted hosts and DHCP servers.
- IP source guard restricts traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings.

- Dynamic ARP inspection (DAI) prevents malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.
- Flexible authentication supports multiple authentication mechanisms including 802.1X, MAC Authentication Bypass and web authentication using a single, consistent configuration.
- Open mode creates a user friendly environment for 802.1X operations.
- Comprehensive new RADIUS Change of Authorization capability provides for asynchronous policy management.
- Private VLANs restricts traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a non-broadcast, multiaccess-like segment.
- Private VLAN Edge provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.
- Unicast Reverse Path Forwarding (RPF) feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.
- Multidomain Authentication allows an IP phone and a PC to authenticate on the same switch port while placing them on appropriate voice and data VLAN.
- Cisco security VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs.
- Cisco standard and extended IP security router ACLs define security policies on routed interfaces for control-plane and data-plane traffic. IPv6 ACLs can be applied to filter IPv6 traffic.
- Port-based ACLs for Layer 2 interfaces allow security policies to be applied on individual switch ports.
- Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3.
- (SNMPv3) provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH Protocol, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.
- Bidirectional data support on the Switched Port Analyzer (SPAN) port allows Cisco Intrusion Detection.
- System (IDS) enables taking action when an intruder is detected.
- TACACS+ and RADIUS authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
- MAC address notification allows administrators to be notified of users added to or removed from the network.
- Multilevel security on console access prevents unauthorized users from altering the switch configuration.
- Bridge protocol data unit (BPDU) Guard shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- Spanning Tree Root Guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
- IGMP filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.
- Wireless end-to-end security offers control and provisioning of wireless access points (CAPWAP)-compliant DTLS encryption to ensure encryption between access points and controllers.

- Mobility and security provides secure, reliable wireless connectivity and a consistent end-user experience.
- Increased network availability is achieved through proactive blocking of known threats.

Ease of Operations

- Cisco Catalyst Smart Operations is a comprehensive set of capabilities that simplify LAN deployment, configuration, and troubleshooting. In addition to adaptive, always on technologies such as StackWise-480 and StackPower, Catalyst Smart Operations enable zero touch installation and replacement of switches and fast upgrade, as well as ease of troubleshooting with reduced operational cost. Catalyst Smart Operations is a set of features that includes Smart Install, Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:
  - Cisco Smart Install is a transparent plug and play technology used to configure the Cisco IOS software image and switch configuration without user intervention. Smart Install utilizes dynamic IP address allocation and the assistance of other switches to facilitate installation providing transparent network plug and play.
  - Cisco Auto Smartports provide automatic configuration as devices connect to the switch port, allowing auto detection and plug and play of the device onto the network.
  - Cisco Smart Configuration provides a single point of management for a group of switches and in addition adds the ability to archive and back up configuration files to a file server or switch allowing seamless zero touch switch replacement.
  - Cisco Smart Troubleshooting is an extensive array of debug diagnostic commands and system health checks within the switch, including Generic Online Diagnostics (GOLD) and Onboard Failure Logging (OBFL).
- Embedded Event Manager (EEM) is a powerful and flexible feature that provides real-time network event detection and onboard automation. Using EEM, customers can adapt the behavior of their network devices to align with their business needs. This feature requires the IP Base feature set.

Deployment and Control Features

- Consistent quality of service (QoS) and security for wired and wireless traffic.
  - Modular QoS CLI (MQC) for defining and applying QoS common policies.
  - Granular QoS policies per access point (AP), radio, SSID, and client.
  - Session-based networking provides better control on devices connecting to the network. ACLs and QoS policies can be applied through the Identity Services Engine (ISE) to each session.
- Improved scale and bandwidth using the converged wired plus wireless functionality:
  - Each 48-port Catalyst 3850 switch provides 40 Gbps of wireless throughput (20 Gbps for the 24 port model). This wireless capacity increases with the number of members in the stack.
  - Mobility Agent—In this mode, the switch terminates the CAPWAP tunnels from access points and provides wireless connectivity to wireless clients. The switch enforces security and QoS policies for wireless clients and access points.
  - Mobility Controller—In this mode, the switch performs all Mobility Agent tasks as well as Mobility coordination, Radio Resource Management (RRM), and clean air coordination.

- Cisco StackWise-480 technology creates a resilient single unified system (a stack) of up to four switches. With a stack bandwidth of 480 Gbps, the stack functions as a single switching unit that is managed by the active switch. If the active switch fails, the standby switch assumes the role of the active switch, keeping the stack operational. Access points connected to operational switches in the stack remain connected during an active to standby switchover.
- Cisco Stack Power technology unifies the individual power supplies installed in the switches in a stack and allows them to be shared as a common resource. Up to four switches can be configured in a StackPower stack with the special connector at the back of the switch using the StackPower cable. StackPower can be deployed in either power sharing mode or redundancy mode. In power-sharing mode, the power of all the power supplies in the stack is aggregated and distributed among the switches in the stack. In redundant mode, some power is held in reserve and used to maintain power to switches and attached devices when one power supply fails, enabling the network to operate without interruption.
- Express Setup for quickly configuring a switch for the first time with basic IP information, contact information, switch and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program.
- IP service-level agreements (SLAs) enable customers to assure new business-critical IP applications, as well as IP services that utilize data, voice, and video, in an IP network. This feature requires IP Services feature set.
- Dynamic Host Configuration Protocol (DHCP) Auto-configuration of multiple switches through a boot server eases switch deployment.
- Automatic QoS (AutoQoS) simplifies QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect Cisco IP phones, classify traffic, and help enable egress queue configuration.
- Cisco StackWise-480 technology helps ensure that all switches are automatically upgraded when the master switch receives a new software version. Automatic software version checking and updating help ensure that all stack members have the same software version.
- Auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
- Dynamic Trunking Protocol (DTP) facilitates dynamic trunk configuration across all switch ports.
- Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel groups and Gigabit groups.
- EtherChannel groups to link to another switch, router, or server.
- Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This feature is similar to Cisco EtherChannel technology and PAgP.
- Automatic media-dependent interface crossover (MDIX) automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.
- Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
- Switching Database Manager (SDM) templates—VLAN template (specific to LAN Base license level) and Advanced template allow the administrator to automatically optimize the TCAM memory allocation to the desired features based on deployment-specific requirements.
- Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.
- Optimized multicast for wired and wireless traffic.

- Internet Group Management Protocol (IGMP) v1, v2, v3 Snooping for IPv4. MLD v1 and v2 Snooping provide fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors.
- Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.
- Cisco VLAN Trunking Protocol (VTP) version 3 supports dynamic VLANs and dynamic trunk configuration across all switches.
- Remote Switch Port Analyzer (RSPAN) allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.
- The Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis.
- Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from source to destination.
- Wireless RF management provides both real-time and historical information about RF interference impacting network performance across controllers, via system-wide Cisco CleanAir technology integration.
- Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location.
- Network Time Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches.

High Availability

- Cross-Stack EtherChannel provides the ability to configure Cisco EtherChannel technology across different members of the stack for high resiliency.
- FlexLink provides link redundancy with convergence time less than 100 ms.
- IEEE 802.1s/w Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) provide rapid spanning-tree convergence independent of spanning-tree timers and also offers the benefit of Layer 2 load balancing and distributed processing. Stacked units behave as a single spanning-tree node.
- Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances.
- Switch-port auto-recovery (Err-disable) automatically attempts to reactivate a link that is disabled because of a network error.
- StackWise-480 provides switch redundancy based on the resilient Cisco IOS Stateful Switchover (SSO) mechanism.
- StackPower provides power supply redundancy across the stack without an external RPS.
- Resilient wireless deployment which is a hierarchical deployment model using the mobility controller and mobility.

High-Performance IP Routing

- IP unicast routing protocols (Static, Routing Information Protocol Version 1 [RIPv1], and RIPv2, RIPng, EIGRP stub) are supported for small-network routing applications with IP Base feature set.
- Advanced IP unicast routing protocols (OSPF, EIGRP, BGPv4, and IS-ISv4) are supported for load balancing and constructing scalable LANs. IPv6 routing (OSPFv3, EIGRPv6) is supported in hardware for maximum performance. OSPF for routed access is included in the IP Base image. The IP Services feature set is required for full OSPF, EIGRP, BGPv4, and IS-ISv4.
- Equal-cost routing facilitates Layer 3 load balancing and redundancy across the stack.
- Policy-based routing (PBR) allows superior control by facilitating flow redirection regardless of the routing protocol configured. The IP Services feature set is required.
- Protocol Independent Multicast (PIM) for IP multicast routing is supported, including PIM sparse mode (PIM- SM), PIM dense mode (PIM-DM), PIM sparse-dense mode and Source Specific Multicast (SSM). The IP Services feature set is required.
- Virtual routing and forwarding (VRF)-Lite enables a service provider to support two or more VPNs, with overlapping IP addresses. IP Services feature set is required.
- IPv6 addressing is supported on interfaces with appropriate **show** commands for monitoring and troubleshooting.

Quality of Service

- Granular wireless bandwidth management to provide hierarchical bandwidth management at line rate. Policies can be configured at the AP, radio, SSID, and client levels.
- Approximate Fair Drop (AFD) to enable fair sharing across users within an SSID.
- Cross-stack QoS to enable QoS configuration across the entire stack.
- 802.1p class of service (CoS) and differentiated services code point (DSCP) field classification are provided, using marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number.
- Data-plane QoS ACLs on all ports to ensure proper marking on a per-packet basis.
- Eight egress queues per port for wired traffic and four egress queues for wireless to enable differentiated management of different traffic types across the stack for wired traffic.
- Shaped Round Robin (SRR) scheduling to ensure differential prioritization of packet flows.
- Weighted Tail Drop (WTD) to minimize congestion at the ingress and egress queues before a disruption occurs.
- Strict priority queuing to ensure that the highest-priority packets are serviced ahead of all other traffic.
- The Cisco committed information rate (CIR) function provides bandwidth in increments as low as 8 Kbps.
- Rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.
- Up to 2000 aggregate policers available per switch.

Wireless Features

Table 8 is a detailed list of wireless features supported on the device.

Table 8 Wireless Features

Feature	Description
Scalability	Supports up to 50 access points per stack and 2,000 wireless clients for business-critical wireless services.
High Performance	• Optimized for 802.11ac standard. • Hardware assisted processing to provide up to 40 Gbps* throughput with services such as downloadable ACL, Granular QoS queues, fairness algorithm, NetFlow-v9 processing, and so on. *48-port Catalyst 3850 switch
Cisco IOS-based Controller	• Security-hardened Cisco IOS operating system. • Well-known Cisco IOS CLI allows users to leverage existing management tools for operations. • The NetFlow eco-system allows users to leverage reporting, monitoring, traffic analysis, and troubleshooting tools for wireless network.
RF Management	Provides both real-time and historical information about RF interference impacting network performance across controllers, via system wide Cisco CleanAir technology integration.
Comprehensive End-to-End Security	Offers control and provisioning of wireless access points (CAPWAP)-compliant DTLS encryption to ensure encryption between access points and controllers or between controllers.
High Performance Video	• Optimized video delivery via a single stream for wireless clients. • Supports Cisco VideoStream technology to optimize the delivery of business-critical multicast video applications across the WLAN.
End-to-End Voice	• Supports Unified Communications for improved collaboration through messaging, presence, and conferencing. • Supports all Cisco Unified Communications Wireless IP Phones for cost-effective, real-time voice services.

Table 8 Wireless Features (continued)

Feature	Description
Mobility and Security	• Secure, reliable wireless connectivity and consistent end-user experience. • Increased network availability through proactive blocking of known threats.
Layer 3 Mobility	Layer 3 roaming occurs when a station roams to a controller where the same VLAN or subnet is not available.
RRM	The Radio Resource Management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network.
Videostream	The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the broadcast frame over the air to a unicast frame.
WMM call admission control (CAC)	CAC enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, to maintain QoS under differing network loads, CAC in CCXv4 is required.
Guest Services Internal Webauth	When a WLAN is configured to use the web policy, either for authentication or pass-through, the internal web server is invoked by default.
Guest Services External Webauth Centrally Switched	If an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. The user database for the guest users can either be stored on the Wireless LAN Controller's local database, or might be stored external of the controller.
ACLs—dynamic on controller	ACLs on the WLC are meant to restrict or permit wireless clients to services on its WLAN.
ACLs—downloadable	You can create ACLs on the controller that can be assigned to groups and individual users based on the RADIUS authorization. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols and more.
Data DTLS	Datagram Transport Layer Security (DTLS) is required to encrypt the data plane traffic.

Table 8 Wireless Features (continued)

Feature	Description
Adaptive wIPS	The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) is an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.
Enhanced Local Mode (ELM)	Local mode access points with a subset of wIPS capabilities is referred to as Enhanced Local Mode (ELM) access point or just ELM AP.
Rich RF (Clean Air, Client Link)	Cisco CleanAir technology, which provides proactive, high-speed spectrum intelligence to combat performance problems due to wireless interference. Cisco ClientLink 2.0 technology to improve downlink performance to all mobile devices including one, two, and three-spatial-stream devices on 802.11n while improving battery life on mobile devices such as smartphones and tablets.
Open/Static WEP	Controllers can control static WEP keys across access points.
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key (WPA-PSK) is a data encryption specification for a WLAN that does not require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase. You can configure WPA parameters on the controller and specify the ASCII or HEX format of the preshared key. This key is used as the Pairwise Master Key (PMK) between the clients and the authentication server.

Table 8 Wireless Features (continued)

Feature	Description
802.1x (WPA/WPA2)	Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA1 and WPA2 use 802.1X for authenticated key management by default.
MAC Authentication	You can configure the controller to start 802.1X authentication when MAC authentication with static WEP for the client fails. If MAC authentication is successful and the client requests for an 802.1X authentication, the client must pass the 802.1X authentication to be allowed to send data traffic.
CCKM Fast Roaming	Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature.
PMK Fast Roaming/OKC	In OKC (Opportunistic Active Key caching), the client and controller store one Pairwise Master Key Security Association (PMKSA). When the client roams, it calculates a new PMKID based on the PMKSA and sends the PMKID with the association request to the AP. The controller calculates the new PMKID based on PMKSA stored for the client. If both PMKIDs match, fast roaming is performed.

Table 8 Wireless Features (continued)

Feature	Description
MIC	Manufactured-installed certificate is a type of certificate installed on the access points.
TACACS Accounting	The process of recording user actions and changes.
LDAP	An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its backend database to retrieve user credentials.
Rogue Detection/Classification	The controller software enables you to create rules that can organize and display access points as Friendly, Malicious, or Unclassified.
MFP (Client, Infrastructure)	Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.
RLDP	The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.
QoS Markings	Quality of Service (QoS) Marking gives critical traffic preferential treatment to make sure it is delivered quickly and reliably.
QoS TCLAS, SIP	The controller can perform traffic classification (TCLAS) to ensure that voice streams are properly classified. As LWAPP/CAPWAP data packets always use the same ports, 16666 and 5247 respectively, and the AP uses the outside QoS marking to determine which queue the packets should be placed in, using port-based QoS policies is inadequate. With TCLAS, even if the LWAPP/CAPWAP AVVID IP DSCP markings are incorrect, the traffic is tagged correctly.

Table 8 Wireless Features (continued)

Feature	Description
Dot1p markings	You can configure 802.1p tagging for wired packets. Wireless packets are impacted only by the maximum priority level set for QoS. The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network. If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.
U-APSD	Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media.
TSPEC /CAC	Call Admission Control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion.
Voice Diagnostics	The controller allows you to perform voice diagnostics and view debug messages between a maximum of two 802.11 clients. You can view details like TSPEC, RSSI, QoS/DSCP mapping and packet statistics information sent from the clients.
Voice metrics	You can generate reports on Traffic Stream Metrics (TSM) using the controller. The report displays TSM metrics such as time QoS, packet loss ratio (uplink and downlink), average queuing delay (uplink and downlink), roaming delay, roaming count, and percentage of queuing delay packets.
Multicast-Unicast	Unicast option configures the controller to use the unicast method to send multicast packets.
Multicast-Multicast	Multicast option configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.
DFS/802.11h	The Cisco UWN solution complies with regulations that require radio devices to use dynamic frequency selection (DFS) to detect radar signals and avoid interfering with them.

Table 8 Wireless Features (continued)

Feature	Description
IPv6 (client mobility)	Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network.
IPv6 RA guard	IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 Router Advertisement (RA) packets. The RA Guard feature is similar to the RA guard feature of wired networks. RA Guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients.
IPv6 DHCP guard	The IPv6 DHCP server guard feature prevents wireless clients from handing out IPv6 addresses to other wireless clients upstream. In order to prevent DHCPv6 addresses from being handed out, any DHCPv6 advertise packets from wireless clients are dropped.
RA throttling/Rate limit	RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity.
IPv6 ACL	IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.
IPv6 Client Visbility	The addition of IPv6 client support to the Cisco Next Generation Wiring Closet (NGWC) feature maintains feature parity between IPv4 and IPv6 clients including mobility, security, guest access, quality of service, and endpoint visibility.
IPv6 Neighbor Discovery	IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.
Syslog	A syslog server can be configured to allow: • Receiving syslog messages through either TCP or UDP • Full reliability because messages can be sent through TCP

Table 8 Wireless Features (continued)

Feature	Description
CDP	The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.
WGB Support	A workgroup bridge (WGB) is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point.
VLAN pooling per group	With VLAN select and VLAN pooling, there is a possibility that you might increase duplicate packets.
Passive Clients	Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.
Band Select	Band Select addresses client distribution between the 2.4-GHz and 5-GHz bands by first understanding the client capabilities to verify whether a client can associate on both 2.4-GHz and 5-GHz spectrum. Enabling band select on a WLAN forces the AP to do probe suppression on the 2.4-GHz band that ultimately moves dual band clients to 5-GHz spectrum.
Peer-to-Peer blocking	Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. You also have more control over how traffic is directed.
Client load balancing (Aggressive load balancing)	Enabling aggressive load balancing on the controller allows the controller to load balance wireless clients across access points.
Client and RFID tag location (see Context aware)	The controller enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the mobility services engine.

Table 8 Wireless Features (continued)

Feature	Description
Efficient AP upgrade	When upgrading the image of an AP, you can use the pre-image download feature to reduce the amount of time the AP is unavailable to serve clients.
AAA override (VLAN and ACL)	When AAA Override option is set, the controller allows the RADIUS server to set VLAN or ACL on a per-MAC address basis and override the global values for the VLAN and ACL as configured on the WLAN.
Basic AAA functions	Authentication is used to ensure that the person attempting to use the device or service is authorized to use it according to the credentials configured. Authorization is used to configure the specific actions a user (or group of users) is allowed to perform on a device. Accounting is used for billing purposes to log the amount of packets or traffic forwarded through a device.
Posturing	A service that Cisco ISE provides is to scan endpoint compliancy; for example, AV/AS software installation and its definition file validity (known as Posture).
Extensible Authentication Protocol (EAP) Authentication	EAP is an authentication framework frequently used in wireless networks for providing transport and usage of keying material and parameters generated by EAP methods which include PEAP, EAP-FAST, TLS, and so on.
Accounting	Enables you to track the services that are accessed and the amount of network resources that are consumed.
Device Profiling	Provides the functionality in discovering and determining the capabilities of all the attached endpoints on your network, regardless of their device types, to ensure and maintain appropriate access to your network. It primarily collects an attribute or a set of attributes of all the endpoints on network and classifies them according to their profiles.
Central Guest access	Allows a guest user to connect to a designated WLAN and access the guest network as configured by the administrator after completing the configured authentication.

Table 8 Wireless Features (continued)

Feature	Description
Local Auth	Local auth is an authentication method that allows users and wireless clients to be authenticated locally on the switch/controller. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.
Internal DHCP Server	The controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The internal server provides DHCP addresses to wireless clients.
New Hierarchical Mobility	Allows a client to roam seamlessly between AireOS controllers running the maintenance Release 7.3.112.0 or Release 7.5 and Cisco controllers running Cisco IOS Release 3.2.xSE.
Web GUI	A web browser, or graphical user interface (GUI), is built into each controller. It allows multiple users to simultaneously browse into the controller HTTP or HTTPS (HTTP over SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points.
AP Priority	During installation, we recommend that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller. When sufficient controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, which allows the client device to immediately reassociate and reauthenticate.
AP Priming	If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point.

Interoperability with Other Client Devices

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

Table 9 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 9 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
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

Table 9 Client Types (continued)

Client Type and Name	Version
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

- When you upgrade the switch software from either Cisco IOS XE Release 3.2.0SE or XE Release 3.2.1SE to XE Release 3.2.2SE, a firmware upgrade occurs automatically. The following message is displayed on the console for about four minutes:

```
Front-end Microcode IMG MGR: Programming device
0...rwRrrrrrrwsssssssssssssssssspsssssssssssssssssspsssssss.......
Front-end Microcode IMG MGR: Programming device
0...rrrrrrwsssssssssssssssssspsssssssssssssssssspsssssssssss......
```

  Do not turn off the switch or reset the switch until the booting process is complete.

  The following features are not supported in Cisco IOS XE Release 3.2.xSE:

  - Outdoor Access Points
  - Mesh, FlexConnect, and OEAP deployment
  - Secure Group Access (SXP, SGT)
  - Wireless Guest Anchor Controller (The Catalyst 3850 switch can be configured as a foreign controller.)
  - IPv6 Multicast Routing
  - Resilient Ethernet Protocol
  - Hot Standby Router Protocol (HSRP)
  - Virtual Router Redundancy Protocol (VRRP)
  - Private VLANs
  - Device Sensor
  - MVR (Multicast VLAN Registration)
  - Secure Group Access - Security Group Tag (SGT) Secure Group Access List (SGACL)
  - Security Group Tag (SGT) Exchange Protocol (SXP)
  - EnergyWise
  - IPv6 routing - OSPFv3 Authentication
  - Call Home
  - Critical VLAN for voice devices

- IPv6 First Hop Security: IPv6 Source Guard
- 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
- Support for 16 static IPv4 routes in LAN Base
- 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
- Multicast Fast Convergence with Flex Links failover

Limitations and Restrictions

- You cannot configure NetFlow export using the Ethernet Management port (g0/0). (CSCuc51864)
- The switch does not support CDP bypass. (CSCud50335)
- The maximum committed information rate (CIR) for voice traffic on a wireless port is 132 Mb/sec. (CSCud59964)
- For wired QoS policy modifications, detach input and output service policies under the interfaces, modify the policies, and re-attach to the interface.
- Although visible in the CLI, the **show platform qos** commands are not supported. (CSCug09112)

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:

http://tools.cisco.com/Support/BugToolKit/

(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.)

The following sections lists Open Caveats and Resolved Caveats for the Catalyst 3850 switch, Cisco IOS XE Release 3.2.xSE.

Open Caveats

- 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.

- CSCub21979

  When a VLAN filter is configured on an RSPAN monitor session, duplicate packets are captured on the RSPAN destination port.

  There is no workaround.

- CSCuc09296

  Following a switchover in a four-member stack, full reconciliation of high availability (HA) services may be delayed by up to 15 seconds. The re-association of wireless clients is similarly delayed.

  There is no workaround.

- 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.

- CSCuc24608

  When the NetFlow collector address for the Flow Exporter is configured in the VRF route table, flow records are exported to the same IP address in the global route table.

  The workaround is to connect the NetFlow collector in the global route table instead of the VRF route table.

- CSCuc45552

  IPV6 first-hop security does not work with EtherChannel.

- CSCuc50127

  Layer 3 multicast traffic is not transmitted on a statically joined port after using the **shutdown** and **no shutdown** commands on an SVI.

  The workaround is to unconfigure the static join and configure it again.

- CSCuc56470

  When policy maps are PRE chained in conjunction with concurrent or sequential authentication sessions, events associated with each authentication method's chained policy are evaluated and executed instead of only those events associated with the method for which the session was authorized. For example, a policy specifies that sessions be authenticated using dot1x or mab, and upon success of either method, chain (attach) a child policy map. If both authentication methods succeed, the session, based on priority, is authorized with dot1x. Subsequent events are matched against both the MAB and dot1x chained policy maps instead of the dot1x chained policy map.

  The workaround is to avoid using PRE chaining with concurrently authenticated sessions.

- CSCuc95293

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

  Run the **sh platform punt statistics port-asic 0 cpuq -1 direction tx** command to verify whether the suspend/unsuspend count is stuck for any of the transmission queues. Run the command several times to make sure that the suspend/unsuspend counters are no longer incrementing, and the TX suspend count = TX unsuspend count + 1. If you see this problem on any of the transmission queues, open a case with the TAC, or contact your Cisco technical support representative.

  There is no workaround. Reboot the switch.

- CSCud03402

  The following message may appear in the switch logs:

```
process kernel: i2c-octeon i2c-octeon.1: broken irq connection detected, switching to polling mode
```

  There is no workaround. There is no functional impact.

- 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.

- CSCud13091

  When Layer 3 interfaces on the active switch in a switch stack are deleted and reapplied, the new member switch that joins the stack may reload.

  The workaround is to reload the stack.

- CSCud13283

  After a switchover, and a default to a Layer 3 interface, the CLI may not respond for several minutes.

  There is no workaround.

- CSCud17361

  After a switchover on a switch stack, the **show interface status** command displays the status of the Uplink SFP as unknown.

  The workaround is to use the **show inventory** command on the interface.

- CSCud27939

  When you update the power or channel on a four-member stack using the **snmp set** command, the operation fails on the standby switch, and the following error message is displayed:

```
%SNMP-3-SYNCFAIL: SNMP MIB Sync Failure: Failure on standby
```

  There is no workaround.

- CSCud33835

  When the switch stack is running in install mode and set to boot with the **boot system switch all flash:packages.conf** command**,** the **show boot system** command does not properly display the BOOT variable for the standby and member switches. The effect is only on the **show** commands; there is no effect on operations.

  There is no workaround.

- CSCud40163

  Rogue Location Discovery Protocol (RLDP) does not work when the AP is in local mode. This problem occurs when there is no WLAN configured in controller or monitor mode AP.

  The workaround is to ensure that you configure one SSID on the controller when AP is in local mode. RLDP does not work when the AP is in monitor mode and there is no workaround.

- CSCud51031

  The mac-address table is updated with BPDU SA from neighbor switch. This is a default behavior. The workaround is to use the **test matm ctrl_pkt_lrn** command in the enable mode to disable this feature.

- 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 user-defined class is **match vlan**.
  - 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.

- CSCud68142

  When the standby switch in a switch stack is reloaded and added back to the stack as a member, sometimes the Feature Forwarding Manager (FFM) process fails, causing a reload. This problem occurs in configurations with a combination of Layer-3 routing, PBR and ACL features.

  There is no workaround.

- 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.

- CSCud84240

  You cannot apply both IPv6 and IPv4 ACLs to an snmp-server group.

  The workaround is to use the **snmp-server user** command instead.

- CSCud90586

  During a configuration synchronization, the **passwd key zeroize** command can cause the standby switch in the stack to stop functioning.

  The workaround is to remove the **passwd key zeroize** command from the configuration and use the **crypto key zeroize rsa** command instead.

- 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.

- CSCug29756

  The **show power inline** command does not accurately reflect changes to the amount of available power.

  There is no workaround. There is no functional impact.

- 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.

- CSCuh17479

  In a switch stack, the Wireless Control Module (WCM) on the active switch stops working due to high CPU usage.

  There is no workaround.

- CSCuh20848

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

  There is no workaround. There is no functional impact.

- 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 switchports. This stops ARP snooping from being enabled on the ports.

- CSCuh44542

  When voice and data clients are authorized in multi authentication mode and the host-mode is subsequently changed to multi-domain authentication (MDA) mode, the switch unexpectedly reboots.

  There is no workaround.

- CSCuh66931

  In a switch stack, a member switch stops working due to a loop with the NGWC Learning Process. This loop can occur when multiple MAC addresses flap between ports, for example, after a wired to wireless MAC move.

  There is no workaround.

- CSCui51050

  Stack port change messages are not properly trapped and displayed with the SNMP trap **snmp-server enable traps stackwise**.

  The workaround is to configure an EEM script to pull the correct OID. For example:

  ```
  event manager applet snmp
  event snmp oid 1.3.6.1.4.1.9.9.500.1.2.2.1.1 get-type next entry-op eq entry-val "2"
  entry-type value poll-interval 5
  action 1.1      syslog msg "Success."
  action snmptrap snmp-trap strdata ""
  ```

- 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.

- CSCui84215

  A WLAN configured to authenticate users with the local webauth method uses the default network authorization method instead of the configured network authorization method. For example, with this global configuration:

  ```
  aaa authorization network default group radius
  aaa authorization network local_webauth local
  ```

and this WLAN configuration:

```
security web-auth
security web-auth authentication-list local_webauth
```

authentication goes through the RADIUS server and not through local authentication.

The workaround is to use the **aaa authorization network default local** command to configure the default network authorization method as local.

Resolved Caveats

Caveats Resolved in Cisco IOS XE Release 3.2.3SE

- CSCtu10646

  Inconsistencies are displayed or the switch unexpectedly resets when you try to remove an existing password from the console or a VTY (telnet port). Use the **show running | be line** command to verify. This problem occurs while the switch is used in a stack.

  The workaround is to avoid using a login password for VTY lines and minimize password configuration changes; the use of AAA for login is recommended. If you need to make password configuration changes, ensure that you save the configuration in a standalone switch, and then include the switch in the stack.

  Here is an example of AAA configuration using local username and password:

  ```
  aaa new-model username username privilege 15 password 0 mypassword aaa
  authentication login vty local line con 0 login authentication vty line vty 0 15
  login authentication vty
  ```

- CSCud06451

  During many simultaneous dot1x authentication operations, sessions may time out and fail to correctly authenticate. The console will continuously report authorization and authentication messages.

  There is no workaround.

- CSCue93229

  The router crashes when polling ipMRouteEntry while executing the **clear ip mroute** command.

  The workaround is to not query ipMRouteEntry and use the **clear ip mroute** command at the same time.

- CSCuf77489

  The switch can crash when there are concurrent sessions and you try remove an existing password from the console or VTY. Various inconsistencies can be seen in the running configuration that can result in a crash.

  The workaround is to minimize configuration changes to the password, and to use a standalone switch when making such changes.

- CSCug34943

  The switch fails to create extended VLANs on a 9-member switch stack.

  There is no workaround.

- CSCug75799

  All wireless clients become stuck in idle state. Once idle, the clients cannot reconnect to the wireless network. New clients can connect, but will become idle on disconnect.

  The workaround is to reload the affected device or stack and upgrade to release 3.3.0(SE) or greater.

- CSCug80708

  A port channel is in the “not connect” status when BPDU packets are received.

  There is no workaround.

- CSCug83616

  When sending traffic from two IXIA ports, the switch packet counter (InUcastPkts and OutUcastPkts) frame value is displayed incorrectly.

  There is no workaround.

- CSCug84023

  Active to backup conversion of FlexLink is slow when the network module C3850-NM-2-10G is used.

  There is no workaround.

- CSCug87540

  Layer 3 traffic routed on one switch or stack member fails for newly added devices.

  There is no direct workaround. Reload the impacted switch to recover.

- CSCug90789

  When the internal process takes more than 3 seconds to process the mobility state change request, the client can be stuck in local state on the foreign switch. As a result, traffic is not forwarded through the anchor; instead, traffic is forwarded through the foreign switch.

  There is no workaround.

- CSCuh08087

  You cannot use a Microsoft NLB deployment to assign a static ARP entry to a non-IPv4 multicast MAC address.

  There is no workaround.

- CSCuh09405

  When multiple activities such as the following are running in parallel, the switch may unexpectedly reboot.

  - multiple SSH sessions
  - multiple Telnet sessions
  - several invalid logins
  - multiple show-tech CLI commands executed

  There is no workaround.

- CSCuh09941

  There is an QoS ACL matching issue when multiple classes match in the ACL range.

  The workaround is to remove auto qos voip cisco-softphone from all attaching interfaces and then reattach the policy.

- CSCuh93075

  BW of the **show interfaces port-channel** privileged EXEC command does not display correctly.

  There is no workaround.

- CSCui05366

  The standby switch in a stack of Catalyst 3850 switches fails to boot up when the **speed nonegotiate** command is configured on an interface and a switch is either reset, or powered up after the command is configured. This may cause all the member switches to reset.

  The workaround is to remove speed nonegotiate from all interfaces using the **no speed nonegotiate** command, or to use the **redundancy config-sync ignore mismatched** privileged EXEC commands.

- CSCui12946

  Some WS-C3850-48T-S switches do not recognize GLC-T SFPs in the uplink module.

  The workaround is to use a downlink 1 Gbps copper port.

- CSCui21897

  Output sensor 1 or HotSpot sensor 2 has an incorrect yellow threshold. This can cause intermittent false SNMP alarms on the SNMP server. New threshold values are set to address the issue.

  There is no workaround.

- CSCui23050

  The external webauth page redirect stops working after some time.

  The workaround is to reboot the system.

- CSCui25555

  When a switch port detects a false short it never recovers to power an IEEE PD. This happens when a PoE port is connected to a PC that has no power and the cable is moved to connect IEEE PD devices.

  There are two workarounds. The first is to use the **shutdown** and **no shutdown** commands to restart the port. The second workaround is to connect the port to a powered on non-PD (like a PC) and wait for the link up. After removing the non-PD link, the port regains the PD detection capability. Then connect the port to the desired PD to get power.

- CSCui36124

  The input queue size counter may exceed the maximum defined threshold of 10, and does not increment any drops.

  There is no workaround.

- CSCui38959

  A Catalyst 3850 stack produces an FCS-Err on some ports. The counter is either 18446744073709551614 or 18446744073709551615.

  The **show interface** command does not show any CRC errors and functionality is not affected.

  The workaround is to bounce the interface to reset the counter to zero.

- CSCui39507

  One switch in a stack of three Catalyst 3850 switches reboots randomly when QoS is enabled.

  There is no workaround.

- 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.

- CSCui47662

  Segmentation fault crash in process cpf_msg_rcvq_process.

  There is no workaround.

- CSCuj48089

  The broadcast queue can become stuck and the switch drops all packets destined to that queue.

  The workaround is to reload the switch. In the case of ARP traffic, you can re-enable NMSP using the **no nmsp attachment suppress** command to enable ARP traffic to be processed.

- 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.

Caveats Resolved in Cisco IOS XE Release 3.2.2SE

- CSCud35278

  The results of the **snmp get** command entered on the SNMP MIB bsnMobileStationRssiData from bsnMobileStationRssiDataTableon are incorrect.

  The workaround is to use one of the following commands in the AP console:

  show wireless client mac-address *mac_address* **detail**

  show controller

- CSCud36670

  The ranges for cLQd11aRadioMaxStreams/cLQd11bRadioMaxStreams and cLQd11aClientMaxStreams/cLQd11aClientMaxStreams do not start at 0. This situation occurs when you perform an **snmp set** on cLQd11aRadioMaxStreams or cLQd11bRadioMaxStreams under cLQd11aCACConfig. The same situation exists for a Radio type.

  There is no workaround.

- CSCud37684

  The switch stack fails to generate a system report log when reloaded.

  The workaround is to manually delete older system reports in the crashinfo partition.

- CSCud47308

  In a four-member stack, large IPv6 RACLs are attached to an ingress port and QoS with policy rate is attached to egress port. When a change is made to the QoS policy map, the switch member unexpectedly reloads.

  There is no workaround.

- CSCud51806

  After reloading a member switch, the NetFlow configuration previously applied to an interface does not work.

  The workaround is to remove the NetFlow configuration from the interface and apply it again.

- CSCud53860

  The **snmp get** command returns an incorrect value on bsnMobileStationWepState from bsnMobileStationTable.

  The workaround is to use the **show wlan name** *profile-name* command.

- CSCud57372

  After a roam operation, when you enter the **show policy** command, the police-conformed rate state under a child policy is displayed incorrectly.

  There is no workaround.

- CSCud60212

  When LoopGuard is enabled globally, the edge access ports that do not have PortFast configured are moved to a blocking state due to loop inconsistency. This problem occurs when edge ports configured as Layer 2 ports without PortFast perform a switchover.

  The workaround is to enable PortFast on Layer 2 edge ports if LoopGuard is enabled.

- CSCud61298

  After a switchover on a switch stack running Rapid-PVST in which the root port goes down as part the switchover, uplink connectivity is lost.

  The workaround is to use the **shutdown** command followed by the **no shutdown** command to enable the new root port. Another option is to configure the root port as a Layer 2 port channel so that it will not go down as part of the switchover.

- CSCud68770

  When you perform a continuous SNMPWALK on the table's attributes, the output is inconsistent.

  When you perform a **set** on the cLD11ClientCalibTable, SNMPWALK gives the correct data for the first few minutes and then it does not return any data.

  There is no workaround.

- CSCud68775

  When you hotswap an FRU or hotswap a 10-G SFP with a 1-G SFP, uplink port traffic fails. In a standalone WS-3850 or a stack of WS-3850 switches, the following operations do not work:

  - Inserting a FRU for the first time when the switch is already in READY state
  - Replacing a FRU with another type of FRU
  - Replacing a 1-G SFP with a 10-G SFP or a 10-G SFP with a 1-G SFP on a FRU that supports 10-G interfaces.

  The workaround for the first two scenarios is to reload the switch where the FRU uplink was inserted or swapped. The workaround for the third scenario is to use the **clear errdisable interface** *interface* **recover-uplink** on the uplink where SFP module was inserted or swapped.

- CSCud84381

  The options under the **errdisable recovery cause ?** command are located on the right side of the display.

  There is no workaround.

- CSCud84155

  When wireless clients use downloadable ACLs with multiple RADIUS servers configured to authenticate clients, the switch reloads.

  The workaround is to use the named ACL with Filter-ID instead of downloadable ACLs when there are multiple RADIUS servers in the network.

- CSCud86601

  When the standby switch and a member switch are being reloaded while the active switch is up and running, the Table_manager process on the active switch fails, causing a reload.

  There is no workaround.

- CSCud88468

  When the startup configuration has the **exception dump device second usbflash0:** command configured and the stack undergoes a staggered boot, the standby switch is reset due to a bulk synchronization failure.

  The workaround is to boot all switches simultaneously. Another workaround is to remove the **exception dump device** command from the configuration and after all the switches are up and running, add the **exception dump device second usbflash0:** command to the configuration.

- CSCud88714

  When a nonhierarchical policy is installed on SSID output and when you try to overwrite it with a new policy which is in a hierarchical format, the policy change fails. This problem occurs only when a nonhierarchical policy is overwritten with a hierarchical policy.

  The workaround is to unconfigure the existing policy and apply the new policy.

- CSCud93812

  With an emergency install, the timestamp for the installed package files and the conf file is set to Dec 31 1969.

- CSCud93998

  After a switchover, when 500 or more clients are trying to join, a few clients do not reassociate.

  The workaround is to manually reassociate the failed clients.

- CSCud94109

  If a client is roaming from Mobility Agent (MA) to Mobility Controller (MC) and joins another MA in a different peer group before complete authentication to MC, and then tries to rejoin to MC, the client entry cannot be deleted from the database. The client will not be able to join on the AP connected to MC but can join anywhere else in the network.

  The workaround is to use the **test platform llm clear-database** *client_mac_address* **true** command to remove the client entry on MC.

- CSCue44402

  The switch displays the following message:

  ```
  FRU Power Supply is not responding
  ```

  There is no workaround.

- CSCue55762

  The switch crashes after about 200 days of uptime.

  There is no workaround

- CSCuf49309

  When UDLD aggressive is configured between two switches and the send port ID and receive port IDs are the same, UDLD detects an error.

  The workaround is to use a different port ID when connecting two switches with a fiber cable.

- CSCuf89784

  When you apply auto qos trust on a port on one of the expansion modules of a non-active switch in a switch stack, errors are displayed.

  There is no workaround.

- CSCug23120

  The **show environment power all** command randomly displays a power supply failure message and displays the wattage is displayed incorrectly as 235 W.

  There is no workaround.

- CSCug29704

  The Layer 2 or Layer 3 path is breaks, all SNMP packets are dropped, or all wireless clients are idle.

  The workaround is to reload the affected member switch and restore service.

- CSCug52183

  When significant traffic (~ 4 billion packets) has traversed the CPU, the switch reloads unexpectedly. Depending on the control traffic pattern, it can take days or weeks for CPU-bound traffic to reach 4 billion. To check for this condition use the **show platform punt stat port-asic 0 cpuq -1 direction rx** command.

  There is no workaround.

- CSCug65693

  A Macbook client bug causes connectivity problems with a recent OS X update. This problem is triggered by the client sending an out of sequence packet.

  The workaround is to disable A-MPDU.

- CSCug85580

  When the **auto qos voip cisco-phone** command is applied to a port, data traffic over 10 (or 20) Mb/s is dropped at ingress ports.

  The workaround is to remove the policer from the following class-map policy:

```
Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy
Class AutoQos-4.0-Default-Class
      set dscp default
     police cir 10000000 bc 8000 be 8000
       conform-action transmit
       exceed-action set-dscp-transmit dscp table policed-dscp
       violate-action drop
```

- CSCug87904

  Auto QoS policy maps, class maps, and access lists are incorrectly generated in Cisco IOS XE Release 3.2.0 and 3.2.1. If you are upgrading your system from Cisco IOS XE Release 3.2.1 or eariler, to Cisco IOS XE Release 3.2.2 or later, refer to the "Upgrading the Switch Software" section on page 11.

- CSCuh10007

  Phones that are connected to the switch does not register or get an IP address.

  There is no workaround.

- CSCuh21506

  When the switch is in VTP client mode, all broadcast traffic is blocked for a given VLAN when a vtp prune event is immediately followed by a re-join event. ARP does not complete and consequently MAC addresses on upstream devices are not learned.

  The workaround is to set the VTP mode to transparent.

Caveats Resolved in Cisco IOS XE Release 3.2.1SE

- CSCue76684

  In certain boot sequences, the BOOT variable is removed from the switch. At the next reboot attempt, the reboot fails, and the switch remains in the bootloader prompt.

  The workaround is to:

  – Boot the switch with **boot flash:***file_name* command.

    or

  – Set the BOOT variable explicitly in the bootloader using **BOOT=flash:***file_name* and, then boot the switch using boot command.

Documentation Updates

Catalyst 3850 Switch Hardware Installation Guide

Product Overview

- The hardware installation guide erroneously describes Cisco Expandable Power System (XPS) 2200 support. XPS 2200 is not supported in this release.
- This note was added to the “Front Panel and LEDs” section:

Note The Catalyst 3850 switches might have slight cosmetic differences on the bezels.

Switch Installation

- The rack-mounting bracket number shown in Figure 2-11 is incorrect. The correct number for the rack-mounting bracket is C3850-RACK-KIT.

Power Supply Installation

- The dual-hole ground lug is optional and is not included with the switch.

Switch Models

- "Table 1: Catalyst 3850 Switch Models" is incomplete. The following should be included:

Switch Model	Cisco IOS Image	Description
WS-C3850-24PW-S	IP Base	Cisco Catalyst 3850 24-port PoE IP Base with 5 access point license
WS-C3850-48PW-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base with 5 access point license

Network Modules

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

C3850-NM-2-10G	Four-slot SFP module: • 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: • 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.

SFP and SFP+ Modules

- The list of SFP modules supported on Catalyst 3850 switches is incomplete. It should include the SFP-GE-Z module.

Technical Specifications

- The dimension for the depth of the switch is incorrect. The correct dimension is 17.5 inches.
- The dimension for the height of the power supply is incorrect. The correct dimension is 1.58 inches.
- The note associated with the power supply dimension information should read:

  Dimensions shown exclude the extraction handle, which measures 1.55 in. (3.9 cm) and the keying feature which measures 0.44 in (1.1 cm).

Catalyst 3850 Switch Getting Started Guide

- In the "Running Express Setup" section, Step 8 contains an error. It should read:

Step 8	Start a browser session on the PC, and enter the IP address **https://10.0.0.1**. When prompted, enter the default password, **cisco**. **Note**: The switch ignores text in the username field. **Troubleshooting:** If the Express Setup window does not appear, make sure that any browser pop-up blockers or proxy settings are disabled and that any wireless client is disabled on your PC or laptop.

- In the "Running Express Setup" section, Step 11 erroneously implies that you need to enable IPv6. IPv6 is enabled by default.

System Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Configuring Fast SSID Changing

When the client sends a new association for a different SSID and fast SSID changing is disabled, the client entry in the controller connection table is cleared before the client is added to the new SSID. This means that the controller enforces a delay before clients are allowed to move to a new SSID. When fast SSID changing is enabled, there is no delay, and clients move more quickly from one SSID to another.

Beginning in privileged EXEC mode, follow these steps to configure fast SSID changing:

	Command	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless client fast-ssid-change** **Example:** `Switch(config)# wireless client fast-ssid-change`	Enables fast SSID change for wireless clients.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/en/US/support/index.html

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

Related Documentation

- Catalyst 3850 switch documentation at this URL:

  http://www.cisco.com/go/cat3850_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes at this URL:

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

- Cisco Validated Designs documents at this URL:

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *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 reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.