Release Notes for Cisco 5700 Series Wireless LAN Controller, Cisco IOS XE Release 3.3.xSE

First Published: October 7, 2013
Last Updated: January 15, 2014

OL-30703-02

This release note describes the features and caveats for the Cisco IOS XE 3.3.xSE software on the Cisco WLC 5700 Series.

Contents

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

Introduction

The Cisco 5700 Series Wireless LAN Controller (Cisco WLC 5700 Series) is designed for 802.11ac performance with maximum services, scalability, and high resiliency for mission-critical wireless networks. With an enhanced software programmable ASIC, the controller delivers wire-speed performance with services such as Advanced QoS, Flexible NetFlow Version 9, and downloadable ACLs enabled in a wireless network. The controller works with other controllers and access points to provide network managers with a robust wireless LAN solution. The Cisco WLC 5700 provides:

- Network traffic visibility through Flexible NetFlow Version 9
- Radio frequency (RF) visibility and protection
- Support for features such as CleanAir, ClientLink 2.0, and VideoStream

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

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

What's New in Cisco IOS XE Release 3.3.1SE

- Support added for Cisco Aironet 3700 Series Access Points—The Cisco Aironet 3700 Series Access Points with the 802.11ac module is supported in this release. For more information about the AP, see http://www.cisco.com/en/US/products/ps13367/index.html.
- Wired Guest Access—Uses Ethernet in IP (RFC3378) within the centralized architecture to create a tunnel across a Layer 3 topology between two WLC endpoints. No additional protocols or segmentation techniques are needed to isolate guest traffic from the enterprise.

Note Detailed documentation for this feature will be made available at a later date. In the meantime, see information about configuring Wired Guest Access on Catalyst 3850 Series Switches at http://www.cisco.com/en/US/docs/ios-xml/ios/ibns/configuration/xe-3se/3850/ibns-wired-guest-access.html.

- For information about open and resolved caveats, see "Caveats" section on page 10.

What's New in Cisco IOS XE Release 3.3.0SE

- Wireshark—A packet analyzer program that supports multiple protocols and presents information in a text-based user interface. Wireshark analyzes wired traffic and wireless traffic.
- Wired Guest Access—Uses Ethernet in IP (RFC3378) within the centralized architecture to create a tunnel across a Layer 3 topology between two WLC endpoints. No additional protocols or segmentation techniques are needed to isolate guest traffic from the enterprise.
- Service Discovery Gateway feature—Enables multicast Domain Name System (mDNS) to operate across Layer 3 boundaries by filtering, caching, and redistributing services from one Layer 3 domain to another. This feature enhances Bring Your Own Device (BYOD).

- Captive Portal Bypassing for Local Web Authentication—Support for Apple devices that need to resolve Wireless Internet Service Provider roaming (WISPr) and have support for captive portal bypass.
- Multicast Fast Convergence with Flex Links Failover feature—Reduces the convergence time of multicast traffic after a Flex Links failure.
- High Availability (HA)
  - Controller Stack—This release supports a stack of two controllers connected using the stack cable, working together using the Cisco StackWise-480 technology. The HA feature is enabled by default when the controllers are connected using the stack cable and the Cisco StackWise-480 technology is enabled.
  - Access Point Stateful Switchover—Controller supports 1000 access points and 12000 clients. When a switchover from the active controller to standby controller occurs, the access points continue to remain connected during the active-to-standby switchover. However, all the clients are deauthenticated and need to be reassociated with the new active controller.
- Client Count per WLAN—You can configure client limits per WLAN, per AP per WLAN, and per AP per Radio. The number of clients that you can configure for each WLAN depends on the platform that you are using.
- 802.11w support—Support for the 802.11w standard as defined by the Management Frame Protection (MFP) service. Disassociation, Deauthentication, and Robust Action frames increase Wi-Fi network security by protecting the management frames from being spoofed.
- 802.11r support in local mode—Support for IEEE Standard for fast roaming allows the handshake with the new access point before the client roams to the target access point. Allows clients to move between access points without breaking a session.
- Wi-Fi Direct Client Policy—Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.
- Assisted Roaming—The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning. The assisted roaming feature is based on an intelligent and client-optimized neighbor list.
- Support for IPv6 wireless clients—Client policies can have IPv4 and IPv6 filters.
- Support for 802.11ac module—The 802.11ac radio module, which is based on the IEEE 802.11ac Wave 1 standard, is available on the Cisco lightweight access points.

  The 802.11ac module provides enterprise-class reliability and wired-network-like performance. The 802.11ac module supports three spatial streams and 80 MHz-wide channels for a maximum data rate of 1.3 Gbps. The 802.11ac standard is a 5-GHz-only technology, which is faster and a more scalable version of the 802.11n standard.
- Application Visibility and Control—Classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR2) engine and provides application-level visibility into Wi-Fi networks.

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

- Security Enhancements
  - Manage Rogue devices—The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. For more information about managing rogue devices, see the "Managing Rogue Devices" section in the *System Management Configuration Guide*.
  - Classify rogue access points—The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, or Unclassified. For more information about classifying rogue access points, see the "Classifying Rogue Access Points" section in the *System Management Configuration Guide*.
  - wIPS—The Cisco Adaptive wireless intrusion prevention system (wIPS) continually monitors wireless traffic on both the wired and wireless networks and uses network intelligence to analyze attacks and more accurately pinpoint and proactively prevent attacks in the future. You can configure an access point to work in wIPS mode if the access point is in the Monitor or Local mode.
  - Radio Frequency Grouping—A radio frequency (RF) group is a logical collection of controllers that coordinate to perform radio resource management (RRM) in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering controllers into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single controller.
- Lightweight Directory Access Protocol Server mode—Operates as the backend database for web authentication to retrieve user credentials and authenticate the user.
- Wireless Flexible NetFlow—Enables flow monitoring and control of wireless traffic.
- Enhanced QoS support for wireless IPv6 clients—Support for IPv6 ACLs and DSCP-matching of IPv6 packets.

Supported Hardware

Controller Models

Table 1 Cisco WLC 5700 Models

Part Number	Description
AIR-CT5760-25-K9	Cisco 5760 Wireless Controller for up to 25 Cisco access points
AIR-CT5760-50-K9	Cisco 5760 Wireless Controller for up to 50 Cisco access points
AIR-CT5760-100-K9	Cisco 5760 Wireless Controller for up to 100 Cisco access points
AIR-CT5760-250-K9	Cisco 5760 Wireless Controller for up to 250 Cisco access points
AIR-CT5760-500-K9	Cisco 5760 Wireless Controller for up to 500 Cisco access points

Table 1 Cisco WLC 5700 Models (continued)

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

Other Supported Products

Table 2 lists the supported products of the Cisco 5700 Series WLC.

Table 2 Cisco 5700 Series WLC Supported Products

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

Table 3 lists the specific supported Cisco access points.

Table 3 Supported Access Points

Access Points	
Cisco Aironet 1040 Series	AIR-AP1041N
	AIR-AP1042N
	AIR-LAP1041N
	AIR-LAP1042N
Cisco Aironet 1140 Series	AIR-AP1141N
	AIR-AP1142N
	AIR-LAP1141N
	AIR-LAP1142N
Cisco Aironet 1260 Series	AIR-LAP1261N
	AIR-LAP1262N
	AIR-AP1261N
	AIR-AP1262N
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I

Table 3 Supported Access Points (continued)

Access Points	
Cisco Aironet 3500 Series	AIR-CAP3501E
	AIR-CAP3501I
	AIR-CAP3501P
	AIR-CAP3502E
	AIR-CAP3502I
	AIR-CAP3502P
Cisco Aironet 3600 Series	AIR-CAP3602E
	AIR-CAP3602I
Cisco Aironet 3700 Series	AIR-CAP3702I
	AIR-CAP3702E
	AIR-CAP3702P

Compatibility Matrix

Table 4 lists the software compatibility matrix.

Table 4 Software Compatibility Matrix

Cisco 5700 WLC	Catalyst 3850	Catalyst 3650	Cisco 5508 WLC or WiSM2	MSE	ISE	ACS	Cisco PI
03.03.01SE	03.03.00SE	03.03.00SE	7.5[1]	7.5	1.2	5.2, 5.3	2.0
03.03.00SE	03.03.01SE	03.03.01SE	7.5	7.5	1.2	5.2, 5.3	2.0

1. Prime Infrastructure 2.0 enables you to manage Cisco WLC 7.5.102.0 with the features of Cisco WLC 7.4.110.0 and earlier releases. Prime Infrastructure 2.0 does not support any features of Cisco WLC 7.5.102.0 including the new AP platforms.

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

Web UI Software Requirements

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

Software Version

Table 5 shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 5 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
03.03.01SE	15.0(1)EZ1	10.1.110.0	15.2(4)JB2
03.03.00SE	15.0(1)EZ	10.1.100.0	15.2(4)JN

Upgrading the Controller Software

To upgrade the Cisco IOS XE software, use the **software install** privileged EXEC command to install the packages from a new software bundle file. You can install the software bundle from the local storage media or it can be installed over the network using TFTP or FTP.

The **software instal**l command expands the package files from the specified source bundle file and copies them to the local flash: storage device. When the source bundle is specified as a tftp: or ftp: URL, the bundle file is first downloaded into the switch's memory (RAM); the bundle file is not copied to local storage media.

After the package files are expanded and copied to flash: the running provisioning file (flash:packages.conf) is updated to reflect the newly installed packages, and the controller displays a reload prompt.

```
MC#software install file
tftp://10.10.10.2/system1/ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin
Preparing install operation ...
[1]: Downloading file
tftp://10.10.10.2/system1/ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin to active
switch 1
[1]: Finished downloading file
tftp://172.19.26.230/kart/ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin to active
switch 1
[1]: Starting install operation
[1]: Expanding bundle ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle ct5760-ipservicesk9.SPA.03.03.00.SE.150-1.EZ.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
    Removed ct5760-base.SPA.03.02.03.SE.pkg
    Removed ct5760-drivers.SPA.03.02.03.SE.pkg
    Removed ct5760-infra.SPA.03.02.03.SE.pkg
    Removed ct5760-iosd-ipservicesk9.SPA.150-1.EX3.pkg
    Removed ct5760-platform.SPA.03.02.03.SE.pkg
    Removed ct5760-wcm.SPA.10.0.120.0.pkg
[1]: New files list:
    Added ct5760-base.SPA.03.03.00SE.pkg
    Added ct5760-drivers.SPA.03.03.00SE.pkg
```

```
    Added ct5760-infra.SPA.03.03.00SE.pkg
    Added ct5760-iosd-ipservicesk9.SPA.150-1.EZ.pkg
    Added ct5760-platform.SPA.03.03.00SE.pkg
    Added ct5760-wcm.SPA.10.1.100.0.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software. New software will load on reboot.
[1]: Committing provisioning file

[1]: Do you want to proceed with reload? [yes/no]:
```

Features

The Cisco 5700 Series WLC is the first Cisco IOS-based controller built with smart ASIC for next generation unified wireless architectures. The Cisco 5700 Series WLC can be deployed both as a Mobility Controller (MC) in Converged Access solutions and as a Centralized Controller.

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

http://www.cisco.com/en/US/products/ps12598/products_data_sheets_list.html

Interoperability with Other Client Devices

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

Table 6 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 6 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

Table 6 Client Types (continued)

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

Important Notes

- A switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches is not supported.
- Although visible in the CLI, the following commands are not supported:
  - **switchport mode dot1qtunnel**
  - **collect flow username**
- Although visible in the CLI, the **authorize-lsc-ap** command is not supported. (CSCui93659)
- The following features are not supported in Cisco IOS XE Release 3.3.0SE:
  - Outdoor Access Points
  - Wired Guest Access

Note Wired Guest Access is supported in the Cisco IOS XE Release 3.3.1SE.

  - Mesh, FlexConnect, and Office Extend Access Point deployment
  - Fast SSID support for guest access WLANs

Limitations and Restrictions

Caveats

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

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

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

Open Caveats

- CSCuf81658

  During an SSO when multicast traffic is flowing on the 5760 controller, spurious unicast packets are transmitted to the multicast client for few seconds.

  There is no workaround.

- CSCug52286

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

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

- CSCug87984

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

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

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

- CSCug90767

  In some circumstances, when the interface on the 5760 controller is in the “down” state, the corresponding port on the neighbor switch might be in the “up” state. This condition is observed when the controller is reloaded with the port being in “admin down” state, and when the switch comes up, the interface is shown as “down” but the port PHY is still “up.”

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

- CSCuh25601

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

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

- CSCuh10592

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

  There is no workaround.

- CSCuh56417

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

  The workaround is to reboot the AP.

- CSCuh64902

  When the 5760 controller with HA is heavily loaded, traceback messages are observed during an SSO.

  There is no workaround. There is no functional impact.

- CSCuh73828

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

  ```
  FED_QOS_ERRMSG-3-TABLEMAP_INGRESS_HW_ERROR
  ```

  There is no workaround. There is no functional impact.

- CSCuh97237

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

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

- CSCui00072

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

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

- CSCui07364

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

  There is no workaround.

- CSCui12012

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

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

- CSCui23689

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

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

- CSCui40588

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

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

- CSCui56229

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

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

- CSCui56842

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

  There is no workaround.

- CSCui57827

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

  ```
  ETHCNTR-3-LOOP_BACK_DETECTED
  ```

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

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

- CSCui67432

  Clients fail to rejoin after multiple switchovers in a Cisco WLC 5700 Series with High Availability environment and with a load of 1000 access points and 12000 wireless clients. Multiple manual switchovers are performed. The issue is intermittent. The scaled system may take more than nine switchovers to see the issue.

  There is no workaround.

- CSCui67756

  7925G phone on WPA2 CCKM WLAN displays a “Leaving Service Area” message during roaming between APs with 802.11ac modules because of forced full reauthentication. Key-cache roaming seems not to work as expected.

  The workaround is not to use 802.11ac modules when CCKM is a requirement for the client.

- CSCui69907

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

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

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

- CSCui88474

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

  There is no workaround.

- CSCuj10024

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

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

- CSCuj13219

  RF-CAC bandwidth is not released after a **shutdown/no shutdown** of a WLAN or a radio, resulting in limited CAC bandwidth for future calls.

  The workaround is to reload the controller.

- CSCuj27803

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

  There is no workaround.

- CSCuj66594

  The 802.11k feature is enabled by default in the Cisco IOS XE 3.3.0 software. If you have a 79xx phone-based VoWLAN solution, the phones need the 1.4.5.x or higher version of firmware to interoperate with 802.11k. A workaround is to disable 802.11k on the controller.

- CSCui84582

  Bcast queue is full when IGMP is disabled.

  There is no workaround.

Resolved Caveats in Cisco IOS XE Release 3.3.0SE

- CSCua75283

  The following tracebacks are noticed on normal setup:

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

  There is no workaround. There is no functional impact.

- CSCuc12774

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

  There is no workaround.

- CSCuc95293

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

- CSCud11467

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

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

- CSCud11552

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

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

- CSCud54501

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

  There is no workaround.

- CSCud54725

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

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

- CSCud55333

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

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

- CSCud56426

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

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

- CSCud60008

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

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

- CSCud60070

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

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

- CSCud62982

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

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

- CSCud63110

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

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

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

  You then detach it.

- CSCud63823

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

  The workaround is to detach the policy and reattach it.

- CSCud65034

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

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

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

- CSCud71747

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

  The workaround is to use the following commands:

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

- CSCud72626

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

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

- CSCuf86171

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

  The workaround is to reload the controller.

- CSCuf93185

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

  There is no workaround.

- CSCug38523

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

  There is no workaround.

- CSCug41165

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

  The workaround is to copy and paste line by line.

- CSCug58178

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

  There is no workaround.

- CSCuh20848

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

  There is no workaround. There is no functional impact.

- CSCui57827

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

  ```
  ETHCNTR-3-LOOP_BACK_DETECTED
  ```

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

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

- CSCui59004

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

  There is no workaround.

Resolved Caveats in Cisco IOS XE Release 3.3.1SE

- CSCsl45701

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

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

- CSCuc63146

  Port-channel interface flap when changing vlan allowed list.

- CSCud08538

  WCM unresponsive on 2M at pthread_mutex_lock.

- CSCue49527

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

  There is no workaround.

- CSCug18767

  Apple devices are unable to login to WEB authentication.

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

- CSCui69999

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

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

- CSCuj21417

  AID leak causing stale client entries on WLC

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

- CSCuj34025

  AUP PDF page does not display in PDF format.

- CSCuj48089

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

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

- CSCuj48889

  Crash due to eicore_ipc used up CPU.

- CSCuj51372

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

  The workaround is to reload the affected stack member.

- CSCuj57007

  DHCPACK with no DHCPOPT_LEASE_TIME option field should trigger IPDT.

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

- CSCuj78610

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

  There is no workaround.

- CSCuj81949

  WCM stopped responding on AAA authentication code. This issue occurs in a scale environment.

  There is no workaround.

- CSCuj91918

  Number of MA RF members is restricted to eight (8) on MC, but allowed limit is 20 members.

  There is no workaround.

- CSCul03186

  Hotspot error occurs intermittently on iPad.

- CSCul06456

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

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

- CSCul06619

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

- CSCul13504

  Web authentication logout pop-up window is not disabled.

  There is no workaround.

- CSCul27659

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

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

- CSCul27717

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

  The workaround is to disable these debug commands.

- CSCul30051

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

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

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

Related Documentation

- Cisco 5700 controller documentation at this URL:

  http://www.cisco.com/en/US/products/ps12598/tsd_products_support_series_home.html

- Cisco Validated Designs documents at this URL:

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

- Error Message Decoder at this URL:

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation*, which lists all new and revised Cisco Technical documentation, as an RSS feed and deliver content directly to your desktop using a read application. The RSS feeds are a free service.
