



Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 4.2.176.51M

Last Revised: July 1, 2009

These release notes describe features, enhancements, and caveats in release 4.2.176.51M.



Note

Before installing this software, refer to the [“System Requirements” section on page 3](#) for details on compatibility with Cisco Wireless LAN Controllers (controllers), Cisco Wireless Control Systems (WCS), and access points.

Contents

These release notes contain the following sections:

- [Overview, page 2](#)
- [System Requirements, page 3](#)
- [Important Notes, page 6](#)
- [Software Upgrade Procedure, page 11](#)
- [Caveats, page 13](#)
- [Troubleshooting, page 17](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation, Support, and Security Guidelines, page 18](#)



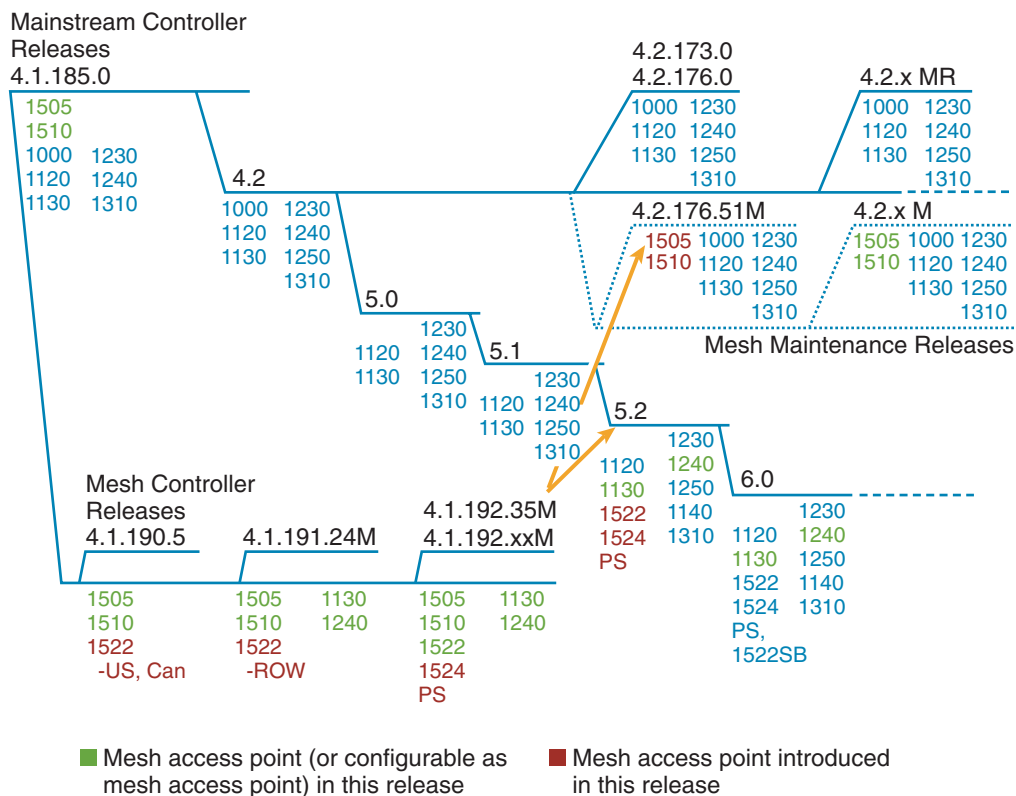
Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

Release 4.2.176.51M provides support for Cisco 1500 (1505 and 1510) series outdoor mesh access points on the controller mainline release base (see Figure 1). The 1505 and 1510 **will not** be supported on any controller release beyond 4.2.

You can upgrade to this release from mesh release 4.1.192.35M.

Figure 1 Controller Mainstream and Mesh Releases



251207

Note

Depending on the customer’s feature requirements, customers operating with both Cisco1500 series (1505, 1510) and 1520 (1522, 1524) series mesh access points in their network might need to use two separate controllers in the network (one for the 1500 series, and one for the 1520 series). For detailed interoperability guidelines between 1500 series and 1520 series mesh access point and other access points, refer to *Cisco Aironet 1500 and 1520 Series Access Points Software Release Guidelines* at http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/bulletin_c78-542046.html

Release 4.2.176.51M is supported on the following Cisco Wireless LAN controller platforms:

- 2106 series, 4400 series, and Wireless Service Module (WiSM) for the Catalyst 6500 and 7600.

Release 4.2.176.51M is compatible with Cisco WCS release 6.0, 5.2.148, and 4.2.128.0.

Release 4.2.176.51M is compatible with the following indoor and outdoor access points:

- Cisco Aironet 1500 (1505 and 1510) series outdoor mesh access points
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1250, and 1310 indoor access points.



Note Release 4.2.176.51M does not support Cisco 1520 (1522, 1524) series mesh access points. Cisco 1520 series mesh access points are supported in release 5.2 (and later) of the controller mainline release.



Note Enterprise mesh is not supported in 4.2.176.51M.



Note The 1250 series access point have a hardware limitation where beacons can only be output at intervals that are multiples of 17 milliseconds. When these APs are configured for a 100-millisecond beacon interval, they transmit beacons every 102 milliseconds. Similarly, when the beacon interval is configured for 20 milliseconds, these APs transmit beacons every 17 milliseconds.



Note Refer to the *Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide and Getting Started Guide* for details on the physical installation and initial configuration of the mesh access points at: http://www.cisco.com/en/US/products/ps6548/prod_installation_guides_list.html



Note Refer to “Monitoring Wireless Devices” (Chapter 6) in the *Cisco Wireless Control System Configuration Guide, Release 6.0* for details on monitoring the mesh network (access points, links, statistics, alarms) at http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0mon.html

System Requirements



Caution You can downgrade from 4.2.176.51M to release 4.1.192.35M. You cannot downgrade to any other mesh release (4.1.190.5, 4.1.191.24M, or 4.1.192.22M).



Caution A downgrade to any previous release resets the controller to the factory default.

Software Images

Table 1 lists the names of the images associated with this release.

Table 1 Software Images Associated with Release 4.2.176.51M

Products	4.2.176.51M and Related Software Images	
Access Point		
	1000	c1000-k9w8-mx.124-10b.JDA1
	1100	c1100-k9w8-mx.124-10b.JDA1

Table 1 **Software Images Associated with Release 4.2.176.51M**

Products	4.2.176.51M and Related Software Images	
	1130	c1130-k9w8-mx.124-10b.JDA1
	1200	c1200-k9w8-mx.124-10b.JDA1
	1240	c1240-k9w8-mx.124-10b.JDA1
	1250	c1250-k9w8-mx.124-10b.JDA1
	1310	c1310-k9w8-mx.124-10b.JDA1
	1505	VxWorks_5312
	1510	VxWorks_5312
WLC-4400	AIR-WLC4400-K9-4-2-176-51M-MESH.aes	
WLC-2100	AIR-WLC2100-K9-4-2-176-51M-MESH.aes	
WiSM	AIR-WLC4400-K9-4-2-176-51M-MESH.aes Note The Catalyst 6500 Supervisor 720 image is s72033_rp-ADVENTERPRISEK9_DBG-M	
Cisco WCS	WCS-STANDARD-K9-6.0.132.exe WCS-STANDARD-K9-5.2.148.0.exe WCS-STANDARD-K9-4.1.128.0.exe	
Cisco WCS Navigator	NAVIGATOR-K9-1.5.132.exe NAVIGATOR-K9-1.4.148.exe NAVIGATOR-K9-1.1.128.exe	

Upgrading to this Software Release

For instructions on downloading software to the controller using Cisco WCS, refer to the release 6.0 version of the *Cisco Wireless Control System Configuration Guide* at the following link:

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

For instructions on downloading mesh release 4.2.176.51M software to the controller using the controller GUI or CLI, refer to [Software Upgrade Procedure, page 11](#).

Upgrade Compatibility Matrix

[Table 2](#) outlines the upgrade compatibility of controller mesh and non-mesh releases and indicates the intermediate software releases required as part of the upgrade path.

Table 2 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases

Upgrade to	4.2.176.51M ¹	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0	3.1.59.24	
Upgrade from																											
4.1.192.35M	Y																										
4.1.192.22M	-	Y	-																								
4.1.191.24M	-	Y	-																								
4.1.190.5	-	Y ²	Y	-																							
4.1.185.0			Y	Y ³	-																						
4.1.181.0				Y ²	Y ²																						
4.1.171.0				Y ²	Y ²	-																					
4.0.219.0					Y ²	Y ²	-																				
4.0.217.204			Y ²		Y ²	Y ²	Y ²	-																			
4.0.217.0					Y ²	Y ²	Y ²	Y ⁴	-																		
4.0.216.0					Y ²	Y ²	Y ²	Y ³	Y	-																	
4.0.206.0					Y ²	Y ²	Y ²	Y ³	Y		-																
4.0.179.11									Y		Y ⁵	-															
4.0.179.8									Y		Y ⁴	Y	-														
4.0.155.5									Y		Y ⁴	Y	Y	-													
4.0.155.0									Y		Y ⁴	Y	Y	Y	-												
3.2.195.10									Y		Y ⁴	Y	Y	Y		-											
3.2.193.5									Y		Y ⁴	Y	Y	Y		Y	-										
3.2.171.6									Y		Y ⁴	Y	Y	Y		Y		-									
3.2.171.5									Y		Y ⁴	Y	Y	Y		Y		Y	-								
3.2.150.10									Y		Y ⁴	Y	Y	Y		Y		Y		-							
3.2.150.6									Y		Y ⁴	Y	Y	Y		Y		Y		Y	-						
3.2.116.21									Y		Y ⁴	Y	Y	Y		Y		Y		Y		-					
3.2.78.0									Y		Y ⁴	Y	Y	Y		Y		Y		Y		Y	-				
3.1.111.0																Y		Y		Y		Y	Y	-			
3.1.105.0																Y		Y		Y		Y	Y	Y	-		
3.1.59.24																Y		Y		Y		Y	Y	Y	Y	-	

1. You must be at release 4.1.192.35M to upgrade to release 4.2.176.51M.
2. You can upgrade directly from 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.
3. Dynamic frequency selection (DFS) is not supported.
4. Release 4.0.217.204 provides fixes for DFS on the 1510. This functionality is only needed in countries where DFS rules apply.
5. An upgrade to 4.0.206.0 is not allowed in the following Country Codes when operating with the following access points: Australia (AP1505 and 1510), Brazil (AP1505 and AP1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and AP1510), New Zealand (1505 and 1510), and Russia (1505 and 1510).

Important Notes

This section describes information about new hardware and software features, and operational notes for release 4.2.176.51M.



Note

Release 4.2.176.51M provides wireless mesh features that are not found in other mainline 4.2.x controller releases. Mesh features are also found for the 1520 series in the main controller release 5.2 and later.



Note

Release 4.2.176.51M supports the features of 4.2.176.0 (non-mesh controller release). Refer to: <http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn421760.html>

Hardware Features

Access Point Support

Release 4.2.176.51M is compatible with the following indoor and outdoor access points:

- Cisco Aironet 1500 (1505 and 1510) series outdoor mesh access points
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1250, and 1310 indoor access points



Note

Release 4.2.176.35M does **not** support Cisco 1520 (1522, 1524) series mesh access points.

RAP vs. MAP Functionality

Access points within a mesh network operate as either a root access point (RAP) or mesh access point (MAP).

Outdoor mesh access points (1505, and 1510) can function as either RAPs or MAPs. By default, all outdoor mesh access points are shipped as MAPs and must be configured to function as a RAP.

At least one access point within a mesh network must be configured to function as a RAP.

RAPs within the network have a wired connection to the controller, and MAPs communicate among themselves and back to the RAP using wireless connections over the backhaul. MAPs use the AWPP protocol to determine the best path through the other mesh access points to the controller.

All the possible paths between the MAPs and RAPs form the wireless mesh that is used to carry traffic from wireless LAN clients connected to MAPs and to carry traffic from devices connected to MAP Ethernet ports.

Software Features and Enhancements

The following software features and enhancements are supported in release 4.2.176.51M.



Note

Enterprise mesh is not supported in 4.2.176.51M.

1505 and 1510 Support

Release 4.2.176.51M supports Cisco 1500 (1505 and 1510) Series Outdoor Mesh Access Point. This release is the only 4.2 mainstream controller release that supports the 1505 and 1510.

Continued Feature Support

A summary of previously released mesh software features supported by 1505 and 1510 outdoor mesh access points is provided in [Table 3](#).

Table 3 Mesh Access Point Feature Support Matrix for 4.2.176.51M

Feature/Platform	1505	1510
Mesh Network Functionality		
Passive scanning —Access point searches for an alternative parent on its current backhaul.	X	X
Background Scanning —Access point searches for an alternative parent on any possible backhaul channel.	X	X
Optimal Parent Selection —Access point joins the best available parent.	X	X
Exclusion Listing —Access point avoids selecting as parent those access points which have a pattern of failing.	X	X
Radar-free Coordinated Sector —Access point notifies parent when radar is detected on the channel so an alternative channel can be employed by the sector.	X	X
Dynamic Frequency Selection —Alternative channel is selected when radar is detected in regulated bands.	–	X
Synchronized Channel Change —Parent advises children of intended channel change.	X	X
Reliable Link Layer, Extended Retries —Transmissions that do not succeed will extend the number of retry attempts in an effort to improve reliability.	–	X
Reliable Link Layer, Secondary Backhaul Radio —A secondary backhaul radio is used as a temporary path for traffic that cannot be sent on the primary backhaul because of intermittent interference.	–	X
Passive Beaconing —Log messages from an access point that cannot connect are relayed through other access points to the controller.	X	X

Table 3 Mesh Access Point Feature Support Matrix for 4.2.176.51M (continued)

Feature/Platform	1505	1510
Network Services Functionality		
Ethernet Bridging —Traffic is bridged from hosts connected to a wired port.	X	X
Containment of Bridged Multicast Traffic —There are two types of multicast traffic, bridged and LWAPP, and each is governed by a different mechanism. LWAPP multicast is managed by the LWAPP methods at the controller, and bridged multicast is governed by the multicast network settings. Multicast flows (such as video camera broadcasts) originating in the network from a MAP Ethernet port terminate only at the RAP Ethernet (In mode Multicast). In this mode, multicast flows are not transmitted throughout the mesh network, thereby reducing bandwidth requirements.	X	X
Universal Access —Radio used for backhaul traffic provides access for client traffic. Note This feature is only configurable on the 1510. On the 1505, this feature is always enabled because the 1505 only supports one radio (802.11b/g).	X	X
Support for Workgroup Bridges —Allows multiple wired hosts to connect to the wireless network through a workgroup bridge.	X	X
Multiple Queues for Backhaul Traffic —Extends client traffic prioritization to the backhaul traffic.	X	X
Static Call Admission Control (CAC) —Ensures sufficient bandwidth is available in a mesh sector before serving new T-SPEC client call requests. Note Static CAC is not fully supported. Static CAC functions as expected; however, there is no way to verify static CAC parameters on the controller using CLI or the GUI (CSCta46421, CSCsz82878).	–	X

Table 3 Mesh Access Point Feature Support Matrix for 4.2.176.51M (continued)

Feature/Platform	1505	1510
Mesh Security		
EAP Authentication —Restricts mesh node access to approved, authenticated access points. EAP-FAST authentication provides secure authentication and encryption key management.	X	X
Applications		
High-speed Roaming —Roam speeds of up to 70 mph are supported for Cisco Compatible Extension (CX) v4 clients.	–	X

Operational Notes

This section describes information about important operational notes and changes to existing controller CLI and GUI for release 4.2.176.51M.

Unable to Verify Static Call Admission Control (CAC) Parameters

Static CAC functions as expected; however, there is no way to verify static CAC parameters on the controller (CSCta46421, CSCsz82878) using the controller CLI or GUI.

Access Point Support Limit on WiSMs

The WiSM only supports up to 300 mesh access points reliably. Therefore, do not allow more than 300 mesh access points to associate with a WiSM.

Configuration Database Setting of 2048 Recommended for Large Mesh Deployments

In large mesh deployments, increasing the configuration database setting to 2048 is highly recommended. The configuration database total includes MAC filter entries, access point MIC and SSC entries, dynamic interfaces, management users, and local net users. You can increase the configuration database to 2048 using the **config database size 2048** command and in the controller GUI, at the Security > AAA > General window (CSCsg88704).

Bridge MAC Filter Config Status Shown in Error

The **show network summary** command mistakenly displays a status for the Bridge MAC Filter Config parameter. This parameter is not a configurable option in release 4.2.176.51M (CSCsk40572).

Limit Bridge Group Names to 11 Characters

Entering more than 11 characters into the bridge group name (BGN) field in the controller GUI mesh access point configuration window (Wireless > All APs > AP-Name > Mesh) generates an error message. This is also true when assigning bridge group names for mesh access points using Cisco WCS (Configure > Access Points > AP_name) and the **config ap bridgegroupname set groupname Cisco_MAP** command (CSCsk64812).

In Cisco WCS, port status is found on the Interfaces tab of the access point page (Monitor > Access Points > AP Name).

Battery Charge Information is not Available for 1510s with Power Supply 1.01d Firmware

A1510 with an *Alpha FlexNet MPS30-48C-SL* power supply must have firmware version 1.02d or greater to supply information about its remaining charge to the controller and Cisco WCS. Otherwise, the controller and WCS display incorrect battery information.

To upgrade your power supply to 1.02d (or greater) firmware, return the power supply to an Alpha service center (Argus).

To arrange return of power supply call or email:

Phone: US and Canada: 1 888 GO ARGUS (462-7487), International: 1 604 436 5547

Email: support@argusdcpower.com

For additional Alpha service centers, see:

<http://www.alpha.com/Contacts/Service-Centers/>

Probing of Battery Charge Levels for 1510 Requires Allowance for Cycles

After detaching and reattaching a probe to a backup battery on a 1510 mesh access point, the battery status remains at a 0% charge reading for up to 30 minutes. This is in keeping with the design of the battery. The battery estimates its charge on 30 minute cycles (CSCsi83272).

Warning Message Added for AP Bridging Disable Requests

When a request is made to disable access point bridging using either the controller GUI (All APs > AP_Name > Mesh) or CLI (**config ap bridging disable**), the following message is displayed (CSCsi88127,CSCsm16458):

Disabling ethernet bridging will affect servicing of ethernet bridged clients.

Are you sure you want to continue?

LinkTest Limitations Message Added

The following warning message appears in the controller GUI (Wireless > All APs > Access Point Name > Neighbor Info) and CLI (**config mesh linktest**) when you run a linktest that might oversubscribe the link (CSCsm11349).

Warning! Data Rate (100 Mb/s) is not enough to perform this link test on packet size (2000bytes) and (1000) packets per second. This may cause AP to disconnect or reboot. Are you sure you want to continue?

Software Upgrade Procedure

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded.



Caution

Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. The access points must remain powered, and the controller must not be reset during this time.



Caution

Controller software releases 4.2.176.51M is greater than 32 MB; therefore, you must verify that your TFTP server supports files this size. Two TFTP servers that support files of this size are *tftpd* and the TFTP server within the WCS. If you download the 4.2.176.51M mesh software and your TFTP server does not support greater than 32 MB file size, the following error message appears: "TFTP failure while storing in flash."



Caution

Refer to the "[Upgrade Compatibility Matrix](#)" section on page 4 to verify the upgrade path to this release before starting any software upgrade.



Note

When upgrading to an intermediate software release as part of the 4.2.176.51M controller software upgrade, ensure that all access points associated with the controller are at the same intermediate release before preceding to install the next intermediate or final version of software. In large networks, it can take some time to download the software on each access point. **You must be at 4.1.192.35M to directly upgrade to 4.2.176.51M.**



Caution

A backup of your controller configuration file is recommended prior to any software upgrade. Without this backup, you will need to manually reconfigure the controller should the configuration file be lost or corrupted or you need to downgrade.

Follow these steps to upgrade the mesh controller software using the controller GUI.

Step 1 Upload your controller configuration files to a backup server.

Step 2 Follow these steps to obtain the mesh controller software and the associated boot images from the Software Center on Cisco.com:

- a. Click this URL to go to the Software Center:
<http://www.cisco.com/cisco/software/navigator.html>
- b. Click **Wireless Software**.
- c. Click **Wireless LAN Controllers**.
- d. Click **Standalone Controllers, Wireless Integrated Routers, or Wireless Integrated Switches**.
- e. Click the controller product name.
- f. Click **Mesh Controller Software**.

- g. Click a controller software release.



Note Verify that the software release is 4.2.176.51M and is for Mesh Networks. Do not download any version that is not noted as a mesh release.

- h. Click the filename (*filename.aes*).



Note Refer to the “[Software Images](#)” section on page 3 for image filenames associated with this release.

- i. Click **Download**.
- j. Read Cisco’s End User Software License Agreement and then click **Agree**.
- k. Save the file to your hard drive.
- l. Repeat steps a. to k. to download the boot image file.

- Step 3** Copy the controller software file (*filename.aes*) and the boot image to the default directory on your TFTP server.
- Step 4** Click **Commands > Download File** to open the Download File to Controller page.
- Step 5** From the File Type drop-down box, choose **Code**.
- Step 6** In the IP Address field, enter the IP address of the TFTP server.
- Step 7** The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.
- Step 8** In the File Path field, enter the directory path of the controller software.
- Step 9** In the File Name field, enter the name of the software file (*filename.aes*).
- Step 10** Click **Download** to download the software to the controller. A message appears indicating the status of the download.
- Step 11** Repeat [Step 6](#) to [Step 12](#) to install the controller boot image.
- Step 12** Disable any WLANs on the controller.
- Step 13** After the download is complete, click Reboot.
- Step 14** If prompted to save your changes, click **Save and Reboot**.
- Step 15** Click **OK** to confirm your decision to reboot the controller.
- Step 16** After the controller reboots, re-enable the WLANs.
- Step 17** If desired, reload your latest configuration file to the controller.
- Step 18** To verify that the 4.2.176.51M controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.
-

Caveats

This section lists open, resolved and closed caveats in release 4.2.176.51M.

Open Caveats

The following caveats are open (unresolved) in this release:

- CSCsg88704—In large mesh deployments, the default configuration database settings of 512 and 1024 (system dependent) might not be large enough to address the needs of the network and additional entries to the database are refused. This condition is true of large non-mesh deployments as well.

Configuration database entries include MAC filter lists, access point MIC and SSC lists, dynamic interfaces, management users and local net users.

The following error messages are indicative of a configuration database that is full and not accepting additional entries:

- "Error in creating MAC filter"
- "Authorization entry does not exist in Controller's AP Authorization List."

Workaround: Increase the configuration database to 2048 using the **config database size 2048** command. In the controller GUI, you can set the configuration database setting at the following window: **Security > AAA > General**.

- CSCsj79606—In some cases, mesh neighbors for a RAP do not display in the WCS mesh link panel (**Monitor > Access Points > RAP Name > Mesh Links**) when the RAP is operating without an assigned bridge group name.

Workaround: Check the controller GUI (**All APs > Access Point Name > Neighbor Info Page**) or CLI (**show mesh neigh {summary | detail} Cisco_MAP**) for the mesh neighbor information or assign a bridge group name to the RAP.

- CSCsj98069—In some cases, after a RAP changes its bridge group name, the modified name does not display in Cisco WCS; however, the modified name does display in the controller GUI and CLI.

Workaround: Use the controller GUI or CLI commands to access the required information for the relevant RAP.

- CSCsk43788—If a large number of mesh access point neighbors have an SNR of zero (0), these might fully populate the Mesh Worst SNR Links report.

Workaround: When running the Mesh Worst SNR Link, select the Parent/Child option as the Neighbor Type to display, to minimize the number of low SNR links reported. Additionally, you can increase the number of listings that display from the default of 10.

- CSCsl20845—It might take an extended period of time (an hour or more) for a change in attenuation to cause the SNR for an existing AWPP neighbor entry to change accordingly. If an access point is rebooted, the newly created AWPP neighbor entry has the expected SNR value immediately.

Workaround: None.

- CSCsl63171—A controller might report a platinum QoS overflow condition to the message log even when platinum QoS is not configured on any of the WLANs. The overflow condition is only reported for 1510s.

Workaround: None.

- CSCsm37109—If some cases, enabling the anti-stranding feature might cause the controller console to be swamped with debug messages from a stranded access point and you are not able to access the console prompt until the messages finish displaying. Messages disappear after 30 minutes when the stranded mesh access point reloads.

Workaround: None.

- CSCsm49862—When a 802.11a network is disabled and a new mesh access point joins, the 802.11a radio displays as UP or REG instead of the expected DOWN state because the 802.11a radio is not shut off due to potential stranding issues. If a mesh access point joins before a 802.11a network is disabled, the mesh access point displays as DOWN even though the 802.11a radio is actually UP. In both cases, the mesh access points are not turned off.

Workaround: None.

- CSCsx28806—In some situations, changing channels on the backhaul of a 1510 RAP causes all downstream MAPs to crash.

Workaround: Reboot the RAP.

- CSCsy97877—After 3 days of uptime, a mesh access point might reload and display an out of buffer message. Problem is often triggered by a client with incorrect credentials trying to continuously associate with two MAPs.

Workaround: None.

- CSCsz82878—Multiple WiSMs with a large number of 1510s connected might crash noting *Task Name: reaperWatcher* as the cause.

Workaround: Disable CAC for mesh by using the following CLI command: **config mesh cac disable**.

This command should be entered even if CAC is not enabled for voice or video. The **config mesh cac {enable | disable}** command is only relevant to mesh access points.

- CSCsz92765—A 1510 RAP or 1510 MAP might randomly start reporting: "Unable to transmit mesh adjacency frame." While this error is reported, the Parent AP will not accept any Children and must be rebooted. This issue appears to be related to the Child AP's encryption keys disappearing from the Parent. Remote debug commands *keyShow* and *sibAgingShow* were used to identify this issue.

Workaround: Reboot the ap or sometimes the condition has cleared itself after some time.

- CSCta26112—Randomly, 1510 MAPs will not be able to join any controller through their original Parent or RAP (1510). All controllers on the network send the join reply to the MAPs but the MAPs all report:

```
Apr 29 13:54:37 172.31.54.3 AP:00:0b:85:86:58:a0: %LWAPP-ERRORLOG: Join Reply:
certificate is not valid
Apr 29 13:54:37 172.31.54.3 AP:00:0b:85:86:58:a0: %LWAPP-ERRORLOG: Join Reply: message
decoding failed (controller - WLC4_2)
Apr 29 13:54:37 172.31.54.3 AP:00:0b:85:86:58:a0: %LWAPP-ERRORLOG: Verify Cert
Nochain: d2i_X509_bio failed
Apr 29 13:54:37 172.31.54.3 AP:00:0b:85:86:58:a0: %LWAPP-ERRORLOG: Verify Cert
Nochain: d2i_X509_bio failed
Apr 29 13:54:37 172.31.54.3 AP:00:0b:85:86:58:a0: %LWAPP-ERRORLOG: Verify Cert
Nochain: d2i_X509_bio failed
```

Workaround: Reboot the RAP or allow the MAP to move to a new RAP or Parent.

- CSCta46421—No CLI commands or GUI windows are available on the controller to verify that Mesh CAC is working.

Workaround: None.

Resolved Caveats

The following caveats are resolved in 4.2.176.51M.

- CSCsk68719—On the controller GUI, when you changed and applied data rates on a mesh access point radio you were prompted with a window that warned you of a pending reboot. When using the CLI, no reboot was necessary and no reboot prompt appeared. Workaround was to use the CLI to change the data rates to avoid the reboot.
- CSCsl15370—Mesh access points were unable to associate with controllers whose names were of varying string lengths. The workaround was to have the same name length for the primary, secondary, and tertiary controllers.
- CSCsl40587—Channel 192 could not be set on a 1510.
- CSCsl90654—When background scanning was enabled, sometimes RAPs would get into a state in which they could not transmit, and network would not be able to communicate. This occurred only in large networks.
- CSCsl91623—The 1510 was not properly advertising its SSID. There was confusion as to which radio (802.11a or 802.11b/g) it was transmitted on.
- CSCsl91679—A reboot of mesh access points was often required to reset adjacency counters or the adjacency. Changes were added to the code
- CSCsm25938—The 1510 could not be deployed in South Africa (country code-ZA). The 802.11a radio was in a disabled state.
- CSCsm62772—A controller running 4.1.190.5 or 4.1.191.24M software might crash unexpectedly due to an SNMPTask.
- CSCsm73147— When a configured country code did not support the 5-GHz band (802.11a), an UP condition for both the 2.4Ghz and 5Ghz radio of a 1510 mistakenly displayed. As an unsupported band, no data should display for the 5-GHz band and MAPs could not join the RAP via that band.
- CSCso17430—In some cases, mesh networks with workgroup bridges (WGB) connections might experience lower throughput. This lower throughput is mostly seen when a series 1300 access point is configured as the WGB and its first connection within the mesh network is a 1510 mesh access point.
- CSCso28047—In release 04.1.191.24M, a controller might display the following message when polled by SNMP (generally Cisco WCS) instead of generating an error message for each access point every five minutes:

```
/tmp/gate/lvl7dev/src/mgmt/snmp/snmp_sr/src/snmpd/unix/k_mib_cisco_lwapp_ap.c:144
SNMP-4-MSGTAG008: Failed to get cLLwappJoinTakenTime for AP XX:XX:XX:XX:XX, API return
code: 1.
```

XX:XX:XX:XX:XX would be the mac address of each AP.

The problem was not service affecting and could be ignored.

- CSCsq15736—All 1510s were advertising an incorrect transmit power (through their dynamic transmit power control (DTPC) information element (IE) beacons) to clients. (Clients use this information to automatically adjust their transmit power to the same level as the access point). This caused the client to set their power too low. Software was modified to report the correct transmit power of the access point in the DTPC IE beacon.
- CSCsq17074—When a user was using the controller GUI to access or modify an access point that was unreachable, a crash on the emWebtask occurred. No crash file was generated.

- CSCsu04143–In some cases, the radio resource manager (RRM) would over allocate timers, not allowing new timers to be allocated. Client association and rogue detection were affected.

Controller often would report the following message:

```
Aug 14 07:05:37.297 timerlib.c:460 OSAPI-0-TIMER_CREATE_FAILED: Failed to create a timer.
```

- CSCsv04340–When a 1510 configured as a MAP, was deployed in a multi-hop mesh network operating with 4.1.192.22M, it would reset after several days of uptime.
- CSCsw73052–Ease calculation did not work correctly causing a 1510 MAP to remain with a secondary parent with a lower linkSNR and higher hop count than its original parent after connectivity to its original parent was restored. Release 4.1.192.35M was operating in the network. For DFS channels, the off channel adjacencies that are updated depend on the map receiving a beacon in the 60 ms interval, that it stays off channel when 802.11b/g scanning is enabled. If the adjacencies are not updated, the map might not roam to neighbors on a different channel.
- CSCsx31684–The 802.11a radio was shown as disabled for the -N domain (Brazil) even though the controller was configured to work in the Brazil country code. Problem was resolved by updating country code tables in the software.
- CSCsy31659–A 1510 did not send a beacon from the 5GHz band when client access was enables on the backhaul. However, the 1510 did respond to probe requests and clients that were actively scanning were able to associate. Problem was seen in release 4.1.192.35M.
- CSCsy52216–A 1510 was not able to authenticate with a local controller or external RADIUS server when using a MAC address to authenticate.
- CSCsy55568–When the access point unicast syslog feature was configured, mesh access points would disassociate from the controller.
- CSCsz32172– The LockAsset error could occur on WiSM blades that were heavily loaded with access points and clients.

Closed Caveats

The following caveats represent those bugs that are closed and not actively being investigated but might still represent active conditions in a product. Workarounds are provided.

- CSCsm80803–When a wired client is connected to a workgroup bridge using WPAv1+TKIP (PSK), it loses its association with a 1510.

Bug was closed because workaround is effective. Code changes would be substantial.

Workaround: Configure WPAv2+AES.

If You Need More Information

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.)

Troubleshooting

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

<http://www.cisco.com/tac>

Click **Troubleshooting**. Then choose your product and then select the **Troubleshoot and Alerts** heading on the product page to find information on the problem you are experiencing and other service advisories.

For additional suggestions on troubleshooting mesh networks, refer to the *Troubleshooting Mesh Networks* document at the following Cisco.com URL:

http://www.cisco.com/en/US/products/ps6548/prod_troubleshooting_guides_list.html

Related Documentation

The following documents are related to mesh networks:

- *Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide*
- *Cisco Aironet Series 1500 Access Point LED Indicator Installation Instructions*
- *Cisco Aironet 8-dBi Omnidirectional Antenna (AIR-ANT5180V-N) and Cisco Aironet 5-dBi Omnidirectional Antenna (AIR-ANT2450V-N)*
- *Cisco Wireless LAN Controller Command Reference, Release 4.2*
- *Cisco Wireless Control System Configuration Guide, Release 6.0* (See also versions for 4.2 and 5.0)
- *Troubleshooting a Mesh Network*

Click this link to browse to the Cisco Support and Documentation page:

<http://www.cisco.com/cisco/web/support/index.html>

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only.

Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

Printed in the USA on recycled paper containing 10% postconsumer waste.