Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 4.1.191.24M-Mesh

Last Revised: February 19, 2008

These release notes describe features, enhancements, and caveats in Release 4.1.191.24M.

Release 4.1.191.24M is compatible with Release 4.2 of the Cisco Wireless Control System (WCS) and is supported on the following Cisco Wireless LAN controller platforms:

- 2100 series, 4400 series and Wireless Service Module (WiSM) for the Catalyst 6500 and 7600.

Release 4.1.191.24M supports full interoperability between the following indoor and outdoor mesh access points:

- Cisco Aironet 1500 (1505 and 1510) series and 1520 (1522) series outdoor access points
- Cisco Aironet 1130AG and 1240 AG series indoor access points

Note Release 4.1.191.24M also supports the following indoor non-mesh Cisco access points:

1000 series, 1100 series, 1130 series, 1200 series, 1230 series, 1240 series and 1300 series.

  - 1250 series access points are **not** supported on this release.

- If some or all of your indoor access points **will** be operating in an indoor Enterprise Mesh deployment or an upgrade to a mesh deployment is planned, install mesh release 4.1.191.24M on your controller.
- If your indoor access points **will not** be operating in an indoor mesh deployment and no future upgrade to a mesh deployment is planned, install non-mesh release 4.2 or later on your controller.

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

Caution If your network is operating with 1520s or you plan to install 1520s in your network, you must set the boot variable on the 1520 before upgrading from release 4.1.190.5 to 4.1.191.24M (or greater mesh release). This ensures the 1520 joins correctly (CSCsl70218). Refer to the "Mandatory Boot Variable Update for Networks with 1520s" section on page 14 for specific configuration details.

Caution A downgrade to mesh releases 4.1.190.5 and 4.1.191.24M from non-mesh release 4.2 is **not** supported. Please see the "System Requirements" section on page 12 for important software upgrade and compatibility details prior to upgrading to this release.

Note Refer to the *Cisco Aironet 1500 Series Outdoor Mesh Access Point Hardware Installation Guide* for details on the physical installation and initial configuration of the mesh access points at http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html

Note Refer to "Monitoring Wireless Devices" (Chapter 6) in the *Cisco Wireless Control System Configuration Guide, Release 4.2* for details on monitoring the mesh network (access points, links, statistics, alarms) at the following link:
http://www.cisco.com/en/US/docs/wireless/wcs/4.2/configuration/guide/wcsmon.html

Note Refer to "Running Reports" (Chapter 14) in the *Cisco Wireless Control System Configuration Guide, Release 4.2* for more details on mesh reports at the following link:
http://www.cisco.com/en/US/docs/wireless/wcs/4.2/configuration/guide/wcsreps.html

Contents

These release notes contain the following sections:

Important Notes

This section describes information about new hardware and software features, and operational notes for Release 4.1.191.24M.

Note Release 4.1.191.24M provides extended wireless mesh features beyond those offered in the main Cisco Unified Wireless Network (CUWN) release base. Mesh-specific features are currently only available in the mesh release series.

Hardware Features

Release 4.1.191.24M supports the following indoor and outdoor wireless access points:

- The 1130 which is equipped with two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.
  - The 5-Ghz radio on the 1130 supports the following bands:5.15GHz, 5.25GHz, and 5.47GHz.
- The 1240 which is equipped with two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.
  - The 5-Ghz radio on the 1240 supports the following bands: 5.15GHz, 5.25GHz, and 5.47GHz.
- The 1505 which is equipped with a single 2.4-GHz radio that provides client access and data backhaul.
- The 1510 which is equipped with two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul and client access.
  - The 5Ghz radio on the 1510 supports the following bands: 4.9GHz, 5.47GHz, and 5.8GHz.
- The 1522 which is equipped with two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.
  - The 5Ghz radio on the 1522 supports the following bands: 4.9GHz, 5.25 GHz, 5.47 GHz, and 5.8 GHz.
- Non-mesh indoor access points: 1000 series, 1100 series, 1200 series (excluding 1250) and 1300 series.

T.

Table 1 Hardware Feature and Band Support by Platform

Feature/Platform	AP1505	AP1510	AP1522	AP1130	AP1240
2.4 GHz Band	X	X	X	X	X
4.9 GHz Band	–	X	X		
5.15 GHz Band				X	X
5.25 GHz Band			X	X	X
5.47 GHz Band	–	X[1]	X[2]	X	X
5.8 GHz Band	–	X[3]	X[4]		
DOCSIS 2.0 Cable Modem (Optional)	–	–	X		
Fiber Module (Optional)	–	–	X	–	–
External Battery Status	X	X	–		
Internal Battery Status	–	–	X		
LEDs	X[5]	X[5]	X	X	X

[1] The 5.47 GHz band is used by the -E and -K regulatory domains for the 1510.

2. The 5.47 GHz band is used by the -A, -E, -K and -T regulatory domains for the 1522.
3. The 5.8 GHz band is used by the -A, -C, -N and -S regulatory domains for the 1510.
4. The 5.8 GHz band is used by the -A, -C, -N, -S and -T regulatory domains for the 1522
5. A detachable, removable Cisco LED indicator is available to detect power for the 1505 and 1510.

RAP vs. MAP Functionality

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

Outdoor mesh access points (1505, 1510 and 1522) and indoor mesh access points (1130 and 1240) can function as either RAPs or MAPs. By default, all outdoor mesh access points functions as MAPs and must be configured to function as a RAP.

Note Indoor access points by default are in local (non-mesh) mode. Specific configuration on the controller is required to convert indoor access points from local to mesh (bridge) access points and to assign the specific mesh role (RAP or MAP). Refer to the "Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)" section on page 19 for details.

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 new software features and enhancements are introduced in Release 4.1.191.24M:

- Dynamic Frequency Selection (DFS) support with seamless channel change for 1520 series access points.
- Indoor Mesh functionality for Cisco Aironet 1130AG and 1240AG series access points.
  - Refer to Table 2 for detailed feature summary.
  - Refer to "Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)" section on page 19 for details on how to upgrade these access points.
- Expanded Mesh Alarms, Events, Reports and Statistics in Cisco WCS release 4.2
  - Three new general parameters are available for monitoring mesh access points from Cisco WCS: AP Uptime, LWAPP Uptime, LWAPP Join Taken Time and Hop count. (Monitor > Access Points > *AP Name* > *Mesh Statistics).*
  - The software version for a mesh access point is now appended with the letter *M:* 4.1.191.24M.
  - Mesh Statistics are summarized under a three-tabbed Mesh Statistics panel rather than on a single page. Statistics are summarized under the following sub-panel headings: Bridging, Queue and Security. (Monitor > Access Points > *AP Name* > *Mesh Statistics).*

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point. Statistic entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

Queue statistics are new to release 4.1.191.24M and summarize the average and peak number of packets waiting in management, platinum, gold, silver and bronze queues. Packets dropped and queue size are also summarized. This information was previously only available on the controller.

- Label and color coding of mesh links to reflect Signal-to-Noise Ratio (SNR) and Packet Error Rate (PER) values on maps (Monitor > Maps > *Map Name*).
- Traps for Poor Link SNR, excessive parent changes, console login and MAC authorization failure.
- Alarms for excessive hop count, excessive child count, default bridge group name (BGN), excessive association, no alternate path, and too high or too low SNR levels.

Note Refer to “Monitoring Wireless Devices” (Chapter 6) in the *Cisco Wireless Control System Configuration Guide, Release 4.2* for details on monitoring the mesh network (access points, links, statistics, alarms) at the following link:
http://www.cisco.com/en/US/docs/wireless/wcs/4.2/configuration/guide/wcsmon.html

- New reports for mesh access points: AP Uptime (Report > Access Point), Client count by RAP (Reports > Client Report); and Mesh Packet Statistics and Mesh Stranded APs (Report > Mesh).

Note Refer to “Running Reports” (Chapter 14) in the *Cisco Wireless Control System Configuration Guide, Release 4.2* for more details on the mesh reports at the following link:
http://www.cisco.com/en/US/docs/wireless/wcs/4.2/configuration/guide/wcsreps.html

- MAC Authorization by a RADIUS Server (NEW CLI Command)

  To provide an additional level of security in authorizing an access point’s MAC address, the following command is introduced.

  config mesh security radius-mac-filter [**enable** | **disable**]

  Enabling this feature, provides backup authorization for an access point on the RADIUS server in case the MAC address is not found in the controller’s MAC filter. In addition to enabling the command on the controller, the user must enter the MAC address of the access point as the username and password in the RADIUS server.

  This feature is disabled by default.

- Available Channels for a Mesh Access Point (NEW CLI command)

  A new command, **show ap channel** *AP_Name* displays the available channels for a specified mesh access point. An example of the command and its display is shown below.

```
>show ap channel AP_Name

802.11b/g Current Channel ................. 1
  Allowed Channel List......................1,2,3,4,5,6,7,8,9,10,11
  802.11a Current Channel ..................161
  Allowed Channel List..................... 36,40,44,48,52,56,60,64,100,
    .........................................104,108,112,116,132,136,140,
    .........................................149,153,157,161
```

- DFS Mesh Sector Change (NEW CLI command)
  - **config mesh full-sector-dfs {enable | disable}**

  This command instructs the mesh sector to do a coordinated channel change on the detection of a radar signal. For example, if a MAP detects radar, the MAP will notify the RAP, and the RAP will initiate a sector change.

  All MAPs and the RAP belonging to that sector go to a new channel. This lowers the probability of MAPs stranding when radar is detected on the current backhaul channel, and no other valid parent is available as backup.

  Each sector change causes the network to be silent for 60 seconds (as dictated by the DFS standard).

  It is expected that after a half hour, the RAP will go back to the previously configured channel. This means that if radar is frequently observed on a RAP's channel, it is important to configure a different channel for that RAP, and additionally to exclude the radar affected channel at the controller using the following commands:

  - **config 802.11a disable** *AP_name*

    where *AP_name* refers to the RAP name

    config 802.11a channel *AP_name channel number*

    where *channel number* refers to the new channel number

    config advanced 802.11a channel delete *channel number*

    where *channel number* refers to the radar-bearing channel number

    config 802.11a enable *AP_name*

Note The **show network** command displays status of DFS.

- Expanded DFS events and history information (NEW CLI commands)

  Two new commands are introduced to provide additional DFS event and history information for mesh access points. Command structure and example displays are shown below.

  - **show mesh dfs history**

```
ap1520#show mesh dfs history
Channel 100 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 10 
minute(s), 24 second(s)).
Channel is set to 136 (Time Elapsed: 18 day(s), 22 hour(s), 10 minute(s), 24 
second(s)).
Channel 136 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 9 
minute(s), 14 second(s)).
Channel is set to 161 (Time Elapsed: 18 day(s), 22 hour(s), 9 minute(s), 14 
second(s)).
Channel 100 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 40 minute(s), 24 
second(s)).
Channel 136 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 39 minute(s), 14 
second(s)).
Channel 64 detects radar and is unusable (Time Elapsed: 0 day(s), 1 hour(s), 20 
minute(s), 52 second(s)).
Channel 104 detects radar and is unusable (Time Elapsed: 0 day(s), 0 hour(s), 47 
minute(s), 6 second(s)).
Channel is set to 120 (Time Elapsed: 0 day(s), 0 hour(s), 47 minute(s), 6 
second(s)).
```

- **show mesh dfs channel** *channel number*

```
ap1520#show mesh dfs channel 104
Channel 104 is available
Time elapsed since radar last detected: 0 day(s), 0 hour(s), 48 minute(s), 11
second(s).
```

Note A mesh access point must be associated with a controller to display the correct time elapsed value in both commands given that MAPs are time synchronized with controllers.

A summary of previously released mesh software features supported by each mesh access point is provided in Table 2.

Table 2 Cisco AP 1500 Series Feature Support Matrix for 4.1.191.24M

Feature/Platform	AP1505	AP1510	AP1522	AP1130	AP1240
Mesh Network Functionality					
Passive scanning–Access point searches for an alternative parent on its current backhaul.	X	X	X	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	X	X	X
Exclusion Listing–Access point avoids selecting as parent those access points which have a pattern of failing.	X	X	X	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	X	X	X
Dynamic Frequency Selection–Alternative channel is selected when radar is detected in regulated bands.	–	X	X	X	X
Synchronized Channel Change–Parent advises children of intended channel change.	X	X	X	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	X	X	X	X
Reliable Link Layer, Secondary Backhaul Radio–A secondary backhaul radio is utilized as a temporary path for traffic that cannot be sent on the primary backhaul due to 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	X	X	X

Table 2 Cisco AP 1500 Series Feature Support Matrix for 4.1.191.24M (continued)

Feature/Platform	AP1505	AP1510	AP1522	AP1130	AP1240
Network Services Functionality					
Ethernet Bridging–Traffic is bridged from hosts connected to a wired port.	X	X	X	X	X
Containment of Bridged Multicast Traffic–There are two types of multicast, 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 (e.g. 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	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	X	X	X
Static Call Admission Control (CAC)–Ensures sufficient bandwidth is available in a mesh sector before serving new T-SPEC client call requests.	–	X	–	–	–
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	X	X	X
Applications					
High-speed Roaming–Roam speeds of up to 70 mph are supported for Cisco Compatible Extension v4 clients.	–	X	–	–	–

Software Images

Table 3 lists the names of the images associated with this release.

Table 3 Software Images Associated with Release 4.1.191.24M

Products	**4.1.191.24M and Related Software Images**		
Access Point		**Image**	**Boot Image**
	1130	c1130-k9w9-tar.124-3g.JMB (mesh, bridge mode) c1130-k9w8-tar.124-3g.JMB (non-mesh, local mode)	c1130-boot.m.124-3g.JMB
	1240	c1240-k9w9-tar.124-3g.JMB (mesh, bridge mode) c1240-k9w8-tar.124-3g.JMB (non-mesh, local mode)	c1240-boot.m.124-3g.JMB
	1505	VxWorks	VxWorks
	1510	VxWorks	VxWorks
	1520	c1520-k9w9-tar.124-3g.JMB	c1520-boot-m.124-3g.JMB
WLC-4400	AIR-WLC4400-K9-4-1-191-24M-MESH.aes		
WLC-2100	AIR-WLC2100-K9-4-1-191-24M-MESH.aes		
WiSM	SWISMK9-4-1-191-24-MESH.aes		
WCS	WCS-STANDARD-K9-4.2.62.0.exe **Note** For release 4.1.191.24M, Cisco WCS is only supported on Windows Server 2003.		
WCS Navigator	NAVIGATOR-K9-1.1.62.exe **Note** For release 4.1.191.24M, Cisco WCS Navigator is only supported on Windows Server 2003.		

Operational Notes

This section describes information about important operational notes and changes to existing controller CLI and GUI for Release 4.1.191.24M.

New controller GUI windows and CLI commands are summarized under the“Software Features and Enhancements” section on page 4 of this release note.

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 following **Security** > **AAA** > **General** window (CSCsg88704).

Bridge MAC Filter Config Status Shown in Error

The **show network** command mistakenly displays a status for the Bridge MAC Filter Config parameter. This parameter is not a configurable option in release 4.1.191.24M (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 in Cisco WCS (**Configure** > **Access Points** > *AP_name*) and the **config ap bridgegroupname set groupname** *Cisco_AP* command (CSCsk64812).

External AAA is not Supported

The **config mesh local-auth** {**enable** | **disable**} command should not be used. Local authorization should never be disabled. Enter the **show mesh config** command to view local authorization status.

```
(controller) >show mesh config
Mesh Range..................................... 12000
Backhaul with client access status.............. disabled
Background Scanning State....................... enabled
MAC Filter Config............................... enabled
Radius MAC Filter............................... disabled
Security Mode................................... EAP
Local-Auth...................................... enabled
```

Four Gigabit Ethernet Ports Supported on 1520s

The 1520 series access point supports four Gigabit Ethernet interfaces.

- Port 0 (g0) is a Power over Ethernet input port–PoE (in)
- Port 1 (g1) is a Power over Ethernet output port–PoE (out)
- Port 2 (g2) is a cable connection
- Port 3 (g3) is a fiber connection

You can query the status of these four interfaces in the controller CLI and Cisco WCS.

In the Controller CLI, the **show mesh env summary** command is used to display the status of the ports.

- The Up or Down (Dn) status of the four ports is reported in the following format:
  - port0(PoE-in):port1(PoE-out):port2(cable):port3(fiber)
- For example, *rap1522.a380* in the display below shows a port status of *UpDnDnDn.* This indicates that:
  - PoE-in port 0 (g0) is Up, PoE-out port 1 (g1) is Down (Dn), Cable port 2 (g2) is Down (Dn) and Fiber port 3 (g3) is Down (Dn).

```
(controller)>show mesh env summary
AP Name      Temperature(C/F) Heater Ethernet Battery
--------     --------------- -------- ------- -------
rap1242.c9ef    N/A             N/A    UP       N/A
rap1522.a380    29/84           OFF    UpDnDnDn N/A
rap1522.4da8    31/87           OFF    UpDnDnDn N/A
```

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

Probing of Battery Charge Levels Requires Allowance for Cycles

After detaching and reattaching a probe to a backup battery on a 1510 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).

Monitoring Port LED Status on an Cisco Aironet 1520 Series Access Point

When physically disconnecting a cable from an 1520 series access point, the port LED associated with that connection might remain lit for up to 3 seconds.

Data Rate Considerations in Short Link Deployments of 1520s

For DFS bands, the Hammer 5 GHz radio does not meet the receiver saturation specification of -30 dBm for some of the higher data rate modes due to a transceiver chipset optimization made to lower the DFS false detect probability. The typical receiver saturation input level is -37 dBm at 24 and 36 Mbps. Future releases of the 1522 will contain an improvement to this parameter by way of further chipset register setting optimization. The receiver saturation performance impact can be mitigated by reducing transmit power and antenna gain where possible. For typical deployments where radios are separated by reasonable distances there is no impact to high data rate support.

System Requirements

You can install this software release on the following Cisco Wireless LAN controller platforms: 2100 series, 4400 series and Wireless Service Module (WiSM) for the Catalyst 6500 and 7600.

Note

- You must install release 4.1.190.5 or 4.1.191.24M to operate Cisco Aironet 1520 series access points in your mesh network.
  - Release 4.2.x and earlier 4.1.x releases will not support 1520 series mesh access points.
  - A 1520 mesh access point operating with release 4.1.190.5 is only supported in the US and Canada.

    Release 4.1.191.24M provides international support for 1520s, 1240s, and 1130s and support for the UNI-2 band in the US.
  - If a 1520 mesh access point is operating in a network, and you downgrade the software release within your network to a non-mesh release, the 1520 will not reconnect and might become stranded.
- If 1520s are going to be installed in a mesh network that is also operating with 1510s, then note the following:
  - The network must first be upgraded to a version of 4.1.190.5 or 4.1.191.24M.
  - All 1510s must be upgraded to the new mesh release and associated with the controller (joined) before any 1520s can be added to the network.
  - A 1520 should not be added to the network until release 4.1.190.5 or 4.1.191.24M is running on the network to ensure proper communication between 1510s and 1520s.
  - Mobility groups functionality is supported when operating with 4.1.190.5 or 4.1.191.24M and all 4.1.x versions of non-mesh controller software.
  - A 1510 can be a parent to a 1520 mesh access point in release 4.1.191.24M; however, in release 4.1.190.5 the 1510 can only be a child to a 1520.

  Note Upgrading to 4.1.191.24M provides full interoperability between 1510s and 1520s. Release 4.1.190.5 does not provide full interoperability. Refer to the "Upgrade Compatibility Matrix" section on page 13 for upgrade path specifics.
- If you are operating with indoor and outdoor access points in your mesh network, then note the following:
  - Series 1130 and 1240 indoor access points can operate as mesh access points in this release.
  - All other indoor access points (excluding 1250) operate as standard, non-mesh access points.

Caution Indoor access points 1130 and1240 configured as mesh access points (bridge mode) should not be connected to a controller without mesh release 4.1.191.24M installed. The1130 and 1240 mesh access points must be converted back to LWAPP (local mode) access points before they are connected to a controller with a non-mesh release. See the "Converting Indoor Mesh Access Points to Non-Mesh Lightweight Access Points (1130AG, 1240AG)" section on page 21 for details on the conversion.

Upgrade Compatibility Matrix

Table 4 outlines the upgrade compatibility of controller mesh and non-mesh releases and indicates the intermediate software releases required as part of the upgrade path. A summary of upgrade path requirements is noted in the "Upgrading to this Software Release" section on page 14.

Table 4 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases

Upgrade to	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																								
4.1.191.24 M	–																							
4.1.190.5	Y	–																						
4.1.185.0	Y	Y[1]	–																					
4.1.181.0		Y[1]	Y[1]																					
4.1.171.0		Y[1]	Y[1]	–																				
4.0.219.0			Y[1]	Y[1]	–																			
4.0.217.204	Y[1]		Y[1]	Y[1]	Y[1]	–																		
4.0.217.0			Y[1]	Y[1]	Y[1]	Y[2]	–																	
4.0.216.0			Y[1]	Y[1]	Y[1]	Y[2]	Y	–																
4.0.206.0			Y[1]	Y[1]	Y[1]	Y[2]	Y		–															
4.0.179.11							Y		Y[3]	–														
4.0.179.8							Y		Y[3]	Y	–													
4.0.155.5							Y		Y[3]	Y	Y	–												
4.0.155.0							Y		Y[3]	Y	Y	Y	–											
3.2.195.10							Y		Y[3]	Y	Y	Y		–										
3.2.193.5							Y		Y[3]	Y	Y	Y		Y	–									
3.2.171.6							Y		Y[3]	Y	Y	Y		Y		–								
3.2.171.5							Y		Y[3]	Y	Y	Y		Y		Y	–							
3.2.150.10							Y		Y[3]	Y	Y	Y		Y		Y		–						
3.2.150.6							Y		Y[3]	Y	Y	Y		Y		Y		Y	–					
3.2.116.21							Y		Y[3]	Y	Y	Y		Y		Y		Y		–				
3.2.78.0							Y		Y[3]	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] CUSTOMERS THAT REQUIRE DYNAMIC FREQUENCY SELECTION (DFS) FUNCTIONALITY SHOULD NOT USE THIS RELEASE. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI compliant countries or Singapore.

2. Release 4.0.217.204 provides fixes for DFS on the AP1510. This functionality is only needed in countries where DFS rules apply.
3. 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 AP1510), Brazil (AP1505 and AP1510), Hong Kong (AP1505 and AP1510), India (AP1505 and AP1510), Japan (AP1510), Korea (AP1505 and AP1510), Mexico (AP1505 and AP1510), New Zealand (AP1505 and AP1510), and Russia (AP1505 and AP1510).

Upgrading to this Software Release

For instructions on downloading software to the controller using Cisco WCS, refer to the release 4.2 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 4.1.191.24M software to the controller using the controller GUI or CLI, refer to Software Upgrade Procedure, page 17.

Upgrade Path to Release 4.1.191.24M

Details for upgrading your network to Release 4.1.191.24M from earlier releases of 3.1, 3.2, 4.0 and 4.1 are described below.

- If your controller is installed with release 4.0.2xx.x software, you must upgrade with two intermediate releases (or one if a DFS network) prior to installing 4.1.191.24M in your network.
  - First upgrade to 4.1.185.0 (non-DFS network) **or** to 4.0.217.204 (DFS network)
  - Secondly, upgrade to 4.1.190.5 (not required for networks that upgraded to 4.0.217.204)
  - Thirdly, upgrade to 4.1.191.24M
- If your controller is installed with release 4.0.1xx.x or 3.2.xx, you must upgrade with three intermediate releases (or two if a DFS network) prior to installing Release 4.1.191.24M.
  - First, upgrade to 4.0.217.0
  - Secondly, upgrade to release 4.0.217.204 (DFS network) **or** 4.1.185.0 (non-DFS network)
  - Thirdly, upgrade to Release 4.1.190.5 (not required for networks that upgraded to 4.0.217.204)
  - Fourthly, upgrade to release 4.1.191.24M
- If your controller is installed with release 3.1.x, you must upgrade with four intermediate releases (or three if a DFS network) prior to installing Release 4.1.191.24M.
  - First, upgrade to 3.2.195.10
  - Secondly, upgrade to 4.0.217.0
  - Thirdly, upgrade to 4.1.185.0 (non-DFS network) **or** 4.0.217.204 (DFS network)
  - Fourthly, upgrade to Release 4.1.190.5 (not required for networks that upgraded to 4.0.217.204)
  - Fifthly, upgrade to Release 4.1.191.24M.

Mandatory Boot Variable Update for Networks with 1520s

If your network is operating with 1520s or you plan to install 1520s in your network, you must set the boot variable on the 1520 BEFORE upgrading from release 4.1.190.5 to 4.1.191.24M or installing a 1520 in a 4.1.191.24M network. Updating the boot variable ensures the 1520 joins correctly.

Note You should check the boot variable setting before updating the boot.

- If the boot system image is visible, then no boot variable update is required.
  - If upgrading from release 4.1.190.5, the system image should read: flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1
- If the boot system image is missing, then you must update the boot variable.

Checking the Boot Variable Setting

To check the setting of the boot variable, do the following:

Step 1 On the controller, enter the following commands for each mesh access point (MAP):

debug ap enable *AP_Name*

debug ap command "more flash:/env_vars" *Cisco_AP*

A display similar to the following appears:

```
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_CARRIER_SET=0020
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_ENCRYPTION_CONFIG=02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: 5G_RADIO_MAX_TX_POWER=65535
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f:
BOOT=flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DEFAULT_ROUTER=11.200.9.20
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DEVIATION_NUM=0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11G_RADIO_MODE=255
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_DEVICE_TYPE=4C
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_ENCRYPTION_CONFIG=02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: DOT11_MAX_ASSOCIATION_NUM=2007
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: ENABLE_BREAK=yes
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: FAB_PART_NUM=800-28909-02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: IP_ADDR=11.200.9.99
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: MAC_ADDR=00:1d:e5:e8:aa:00
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: MAC_ADDR_BLOCK_SIZE=256
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: MANUAL_BOOT=no
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: NETMASK=255.255.0.0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: NEW_IMAGE=yes
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_ASSY_NUM_800=03 20 00 70 ED 02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_PART_NUM_73=49 2A A6 02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_REVISION_NUM=A0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCA_REVISION_NUM_800=A0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PCB_SERIAL_NUM=FHH1101007F
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PEP_PRODUCT_ID=AIR-LAP1521AG-A-K9
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PEP_VERSION_ID=V01
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: PRODUCT_MODEL_NUM=AIR-LAP1521AG-A-K9
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: RADIO_CARRIER_SET=00FF
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: RADIO_MAX_TX_POWER=65535
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: SYSTEM_REVISION_NUM_800=A0
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: TOP_ASSY_NUM_800=03 20 00 71 22 02
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: TOP_ASSY_SERIAL_NUM=SJC1101007F
Tue Jan 15 00:00:15 2008: SLT-HCAB-MAP-01-fe.bb.6f: param-any=
```

Step 2 To turn off debug access, enter **debug ap disable** *AP_Name*.

Note You do not need to turn off the debug access at this point if a boot update is required. Continue to the “Updating the Boot Variable” section on page 16.

.

Updating the Boot Variable

To update the boot variable on a 1520 prior to a software upgrade, do the following:

Step 1 On the controller, enter the following commands for each mesh access point (MAP):

debug ap enable *AP_Name*

debug ap command "debug lwapp con cli" *AP_Name*

debug ap command "test mesh enable telnet" *AP_Name*

show ap config general *AP_Name*

Note Find the IP address for the access point in the **show ap config general** *AP_Name* command and continue to Step 2.

Step 2 Telnet to the access point using the IP address identified in Step 2 by entering the following command:

telnet *IP_address*

Step 3 From the AP console, enter the following:

enable

debug lwapp console cli

show version

Look for the system image as noted in the example below:

```
System image file is “flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1”
```

Enter the image name (enclosed within quotes) into the **boot system**... command below.

config term

boot system flash:/c1520-k9w9-mx.124-3g.JMA1/c1520-k9w9-mx.124-3g.JMA1

Note The system image entered in the **boot system** *image-name* command must match the version identified in the **show version** command.

exit

Enter the following command to verify you typed the image string correctly.

more flash:/env_vars *Cisco_AP*

Step 4 Disconnect Telnet.

Software Upgrade Procedure

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded. When an access point is loading software, each of its LED blinks in succession.

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 release 4.1.191.24M 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 4.1.191.24M 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 13 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 4.1.191.24M 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.

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/kobayashi/sw-center/sw-wireless.shtml

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 4.1.191.24M 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 9 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 4.1.191.24M controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)

Before you can install a 1130AG or 1240AG indoor access point into an indoor mesh deployment you must do the following.

1. Convert the autonomous access point (k9w7 image) to a lightweight access point.

   A detailed explanation of this process is located at:

   http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

2. Convert the lightweight access point to either a mesh access point (MAP) or root access point (RAP).

   Indoor mesh access points (1130 and 1240) can function as either a *root access point (RAP)* or a *mesh access point (MAP)*. By default, all are configured as MAPs.

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

Note The access point reboots after entry of the conversion commands (CLI, GUI, and WCS noted below), and initially reloads its existing non-mesh image (k9w8) and then rejoins the controller. After successfully rejoining, the access point receives a download of the mesh image (k9w9) from the controller. The mesh image then reloads and replaces the non-mesh image on the access point. Afterwards, the access point rejoins the controller as a mesh access point operating in the bridging mode as either a MAP or RAP as configured.

Note The indoor mesh access point image (k9w9) is a different image than the autonomous (k9w7) and lightweight access point images (k9w8).

- To convert the access point to a mesh access point using the CLI, enter the commands noted in either **Step a** or **b** below.
  a. To convert from a lightweight access point to a MAP, enter the following CLI commands:

     config ap mode bridge *AP_name*

     The mesh access point image (k9w9) is downloaded.

  b. To convert from a lightweight access point to a RAP, enter the following CLI commands:

     config ap mode bridge *AP_name*

     config ap role rootAP *AP_name*

     The mesh access point image (k9w9) is downloaded and the mesh access point is configured to operate as a RAP.

- To convert the access point to a mesh access point using the GUI, do the following.
  a. Choose **Wireless** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.

  b. At the General Properties panel, select Bridge from the AP Mode drop-down menu.

     The access point loads the new image (k9w9) and reboots.

  c. At the Mesh panel, select either RootAP or MeshAP from the AP Role drop- down menu.

d. Click **Apply** and **Save Configuration**.

- To convert the access point to a mesh access point using Cisco WCS, do the following.

  a. Choose **Configure > Access Points** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.

  b. At the General Properties panel, select Bridge as the AP Mode (left-side) and either RAP or MAP as the AP Role (right-side).

  c. Click **Save**.

Changing MAP and RAP Roles for Indoor Mesh Access Points (1130AG, 1240AG)

Indoor mesh access points can function as either root access points (RAPs) or mesh access points (RAPs). To change from one role to another, follow the appropriate step below.

1. To change the role of an indoor access point from MAP to RAP or RAP to MAP using the CLI, enter the following command choosing the appropriate option:

   config ap role {rootAP | meshAP} *AP_name*

2. To change the role of an indoor access point using the GUI, do the following.

   a. Choose **Wireless** and click on the AP Name link for the 1130 or 1240 indoor access point you want to change.

   b. At the Mesh panel, select MeshAP or RootAP from the AP Role drop-down menu.

   c. Click **Apply** and **Save Configuration**.

3. To change the role of an indoor access point using Cisco WCS, do the following

   a. Choose **Configure > Access Points** and click on the AP Name link for the 1130 or 1240 indoor access point you want to change.

   b. At the General Properties panel, select either RAP or MAP as the AP Role (right-side).

   c. Click **Save**.

Note The access point reboots after the role is changed.

Note When changing from a MAP to RAP, a Fast Ethernet connection between the MAP and controller is recommended.

Note After a RAP to MAP conversion, the MAP's connection to the controller is a wireless backhaul rather than a Fast Ethernet connection. It is the responsibility of the user to ensure that the Fast Ethernet connection of the RAP being converted is disconnected before the MAP comes up so that the MAP can join over air.

Note The recommended power source for MAPs is either a power supply or power injector. PoE is not a recommended power source for MAPs.

Converting Indoor Mesh Access Points to Non-Mesh Lightweight Access Points (1130AG, 1240AG)

The access point reboots after entry of the conversion commands (noted below), and initially reloads its existing mesh image (k9w9) and then rejoins the controller. After successfully rejoining, the access point receives a download of the non-mesh image (k9w8) from the controller. The non-mesh image reloads and replaces the mesh image on the access point. Afterwards, the access point rejoins the controller as a non-mesh lightweight access point operating in the local mode.

Note A Fast Ethernet connection to the controller for the conversion from a mesh (bridge) to non-mesh (local) access point is recommended. If the backhaul is a radio, after the conversion you must enable Ethernet and then reload the access image. After the reload and reboot the backhaul is Fast Ethernet.

Note When a root access point is converted back to a lightweight access point, all of its subordinate mesh access points lose connectivity to the controller. Consequently, a mesh access point is unable to service its clients until the mesh access point is able to establish connectivity to a different root access point in the vicinity. Likewise, clients might connect to a different mesh access point in the vicinity to maintain connectivity to the network.

1. To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using the CLI, enter the following command.

    config ap mode local *AP_name*

   The access point loads the non-mesh image (k9w8).

2. To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using the GUI, do the following.

   a. Choose **Wireless** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.

   b. At the General Properties panel, select Local from the AP Mode drop-down menu.

   c. Click **Apply** and **Save Configuration**.

3. To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using Cisco WCS, do the following.

   a. Choose **Configure > Access Points** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.

   b. At the General Properties panel, select Local as the AP Mode (left-side).

   c. Click **Save**.

Caveats

This section lists open, resolved and closed caveats in Release 4.1.191.24M.

Open Caveats

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

- CSCsg10476–MAPs do not join when the configured mesh security mode is EAP and an external RADIUS server is used for authentication. Only controller-based local authentication is supported in 4.1.191.24M.

  Workaround: None.

- CSCsg44445–The **show ap config {802.11a| 802.11b}** *Cisco_AP* command displays incorrect power level values for the 1510; however, the power levels in use by the 1510 are correct.

  Workaround: None.

- 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**.

- CSCsj18620–From the Mesh Parent-Child Hierarchal View panel, selecting a colored dot next to a MAP or RAP to view SNR details might result in an overlap of the two panels.

  Workaround: None.

- CSCsj47801–In some cases, an outdoor mesh access point might attempt authorization on a RADIUS server when its MAC address is not found in the in the controller's MAC filter.

  Workaround: A new command **config mesh security radius-mac-filter** [**enable** | **disable**] is available to provide backup MAC address authorization for the MAP. Refer to the "Software Features and Enhancements" section on page 4 of this release note for details.

- CSCsj48049–The Custom options for the TX Power Level Assignment parameter (Configure > Access Point > *Radio)* in Cisco WCS do no reflect the correct dBm values; however, the correct values are resident in the software.

  Workaround: Select the Tx Power Level Assignment based on the values 1 (high) to 5 (low) and ignore the dBm values associated with those numbers.

- 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_AP*) for the mesh neighbor information or assign a bridge group name to the RAP.

- CSCsj79625–In Cisco WCS, the link test results panel generated from the Mesh Links tab (Monitor > Access Points > *AP Name)* might not be easily viewed.

  Workaround: Ensure the browser window is fully open. Slide the browser scroll bar down to modify the location of the link test results panel for better viewing.

- CSCsj87294–In a mesh network operating with 1510s and any or all of the following mesh access points:1520, 1240 or 1130, the 802.11h channel change management frame sent by either the 1520, 1240 or 1130 might not be handled properly by the 1510. As a result, the channel change on the RAP might not propagate to the 1510 children mesh node. However, the channel change management frame is correctly handled between and among the 1520, 1240 and 1130 mesh access points. Additionally, channel change management between and among 1510s is handled correctly.

  Workaround: None.

- 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.

- CSCsk01686–In Cisco WCS, when a child MAP is removed from a parent RAP the resulting Mesh List Event message (Monitor > Access Points > *AP Name* > *Mesh Links* > *Mesh List Event*) might note the neighbor type as ‘unknown’ rather than ‘child’ as seen in the following example event.

  Parent AP 'AP 1242-rap1/00:1b:2b:35:52:40' lost connection to AP '00:1b:2b:35:51:bf'. AP neighbor type is 'unknown.’

  Workaround: None.

- CSCsk08657–In the controller GUI, entry of an antenna gain greater than the highest allowed antenna gain threshold value is allowed with no resulting error message.

  Workaround: Verify that the entered antenna gain is within the regulatory domain limit.

- CSCsk21715–In some circumstances, some of the configurable fields of the Cisco WCS AP Template might not be selectable.

  Workaround: Refresh the browser window.

- CSCsk36281–When you disable battery status using the **config mesh battery-state disable** command, you must reset the access point to enable battery status again.

  Workaround: None.

- CSCsk37948–In Cisco WCS, the Mesh Links Stats Report (Reports-> Mesh reports > Mesh Link Stats) displays time without AM or PM.

  Workaround: None.

- 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.

- CSCsk49160–In Cisco WCS, the word “association” is misspelled in the excessive association trap event when viewed on the alarms (Monitor > Alarms) window.

  Workaround: None.

- CSCsk53479–In some cases, a channel update coming from a parent 1522 mesh access point, is reported by the child as an IDS signature. An example channel change message is shown below:

  *Sep 13 13:25:09.143: %WIDS-4-SIG_ALARM: Attack is detected on Sig:Standard Id:10 Channel:112 Source MAC:001a.a2ff.8e00

  Workaround: None.

- CSCsk64802–In Cisco WCS, when the *Mesh Stranded APs* report is run (Reports > Mesh Reports) no values are reported in the first time seen and last time seen columns for those access points identified as “detected but previously associated stranded aps” (State column).

  Workaround: None.

- CSCsk64812–In Cisco WCS, entering more than 11 characters into the bridge group name (BGN) field in the Access Point configuration window (Configure > Access Point > *AP Name*) generates an error message. This is true for the relevant controller GUI fields and CLI commands as well.

  Workaround: Create a bridge group name with less than 11 characters.

- CSCsk68719–On the controller GUI, when you change and apply data rates on a mesh access point radio you are prompted wit h a window warning you of a pending reboot. When using the CLI, no reboot is necessary and no reboot prompt appears.

  Workaround: To avoid a reboot when changing data rates on a mesh access point, use the CLI to change data rates.

- CSCsk93910–Cisco compatible clients do not adjust their power level to mesh access points power levels as designed. The initial setting of the client remains.

  Workaround: None.

- CSCsl01648–If a 1520 is configured with channels or antenna gain combinations that are outside the permitted values for a particular domain, the RAP might join the controller, however, the channel or antenna gain values cannot be changed. MAPs configured with incorrect channels or antenna gain combinations are not able to join the controller.

  Workaround: Verify antenna and channel settings permitted in a regulatory domain before configuring the mesh access point. Do not configure channel and antenna gains outside the permitted values.

- CSCsl10590–In periods of heavy multicast traffic, error messages such as those noted below might display for the controller but expected system throughput is maintained. No system impact.

  Example error messages:

  Msg 'LRAD Entry set' of LRAD Table failed, Id = 0x00622075 error value = 0xfffffffc

  Msg 'Set Multicast Params' of System Table failed, Id = 0x006c2075 error value = 0xfffffffc

  Workaround: None. No system impact.

- CSCsl15941–On the 1520, when operating in the -K regulatory domain, channels on which radar is detected might allow a MAP to join the disallowed channels if the antenna gain on a RAP is:

  - changed from a starting value between 0 and 16 to a value greater than 16.
  - changed from a starting value that is greater than 16 to a value less than 16.

  Workaround: None.

- CSCsl15976–On the 1520 when operating in the -C regulatory domain, a change in the antenna gain to a value greater than 16 is not accepted by the RAP; however, the change is reflected in the controller GUI.

  Workaround: None.

- 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.

- CSCsl22083–When Admin is in a disabled state on the 1510, the 1510 will crash after 30 minutes.

  Workaround: Do not set the 1510 to an Admin Disabled state.

- CSCsl21116–The **show ap summary** command does not display the correct Ethernet MAC address for the 1520s.

  Workaround: None.

- CSCsl24620–In some circumstances a 1520 might attempt simultaneous authorization with the controller via two different parents, if a better parent is located during its authorization process. The parent access points might be initially blacklisted by the child after a failed authorization but the child will re initiate a search for a parent and join.

  Workaround: None. Child mesh access point will join a parent successfully although convergence time might be increased.

- CSCsl30771–In some cases a 1520 configured with DFS on channel 64 might not be able to access the channel when the non-occupancy period (activated when radar is detected) of 30 minutes expires for that channel. It might report the following log: "Radar non-occupancy required on this channel. Pick another channel or try again later."

  Workaround: None.

- CSCsl39876–In rare circumstances, a RAP that has lost its wired connection to the controller and has reconnected to the controller, over the air through a nearby parent mesh AP, might require multiple scans or exceed the lonely timer and reboot before it reconnects to a wired connection. As designed, a RAP will scan for wired connections every 15 minutes until the lonely timer expires at 40 minutes and initiates a reboot of the access point.

  Workaround: None.

- CSCsl40515–In some cases, the MAP linktest fails and the MAP loses its LWAPP connection. A high packet per second (PPS) default setting of 1,000 is related to the failure.

  Workaround: Run the link test from the controller GUI which has a default PPS setting of 100 PPS.

- CSCsl70218–The BOOT bootloader environment variable is not set on some early shipments of 1520 mesh access points. Any image download that fails during upgrade might cause a partial image to be written on the1520. Without the BOOT variable, the bootloader might attempt to boot the partial image rather than the original complete image, causing the 1520 to get stuck and not join the controller. (*Continued on next page*)

  This is seen when a controller is upgraded from mesh release 4.1.190.5 to 4.1.191.24M and the 1520 has a wireless connection to the controller. It might also happen when a controller is upgraded from 4.1.190.5 to other future mesh releases.

  Workaround: To recover from an incomplete 1520 boot up due to a 4.1.190.5 to 4.1.191.24M upgrade, enter the following bootloader commands in the AP console:

  ```
  delete flash:/update/c1520-k9w9-mx.124-3g.JMB/c1520-k9w9-mx.124-3g.JMB
  set BOOT flash:/c1520-k9w9-mx.124-3g.JMA/c1520-k9w9-mx.124-3g.JMA
  boot
  ```

To verify the configuration, enter

```
set
```

Note For details on connecting to the AP console, refer to the "Connecting to the Access Point Locally" section of the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* found at: http://www.cisco.com/en/US/docs/wireless/access_point/1520/installation/guide/1520_ch3.html#wp1099247

Note To prevent the 1520 boot up problem, a change in the boot variable must be made prior to any upgrade to 4.1.191.24M (or greater mesh release). Refer to the "Mandatory Boot Variable Update for Networks with 1520s" section on page 14 for configuration details.

Resolved Caveats

The following caveats represent those bugs resolved since 4.1.190.5.

- CSCek79361–When a 1520 that supported fiber ports was operating without a fiber connection, the G3 Ethernet fiber port would periodically go up and down by itself.
- CSCsg10476–MAPs would not join when the configured mesh security mode was EAP and an external RADIUS server was used for authentication. Only controller-based local authentication is supported in 4.1.191.24M.
- CSCsg48056–In some cases, when the DHCP proxy was disabled it would cause an access point to be seen as a client (STA) instead of an access point (AP) and no DHCP address was assigned to the access point. The workaround involved enabling DHCP proxy for mesh access points (**config dhcp proxy enable**).
- CSCsg88380–Mesh Linktest between two mesh access points failed when the two MAPs were associated with different controllers. The workaround was to establish the same controller as the primary controller for the two mesh access points.
- CSCsh68471–Public safety channels did not display the correct channels in Cisco WCS.
- CSCsi70440–The error message that displayed when the **config mesh multicast** [**regular** | **in** | **in-out**] command was entered without the mode type (regular, in, in-out) was missing a character.
- CSCsi83988– An AP1520 did not rate-shift down soon enough in noisy environments which affected overall throughout.
- CSCsi88163–The **config ap disable** *Cisco_AP* message returned an incomplete error message. The message was expanded to read: "Can't disable ADMIN state of the Cisco AP, since disabling will make Mesh AP stranded!."
- CSCsi89805–The MAC address of child mesh access points (1510s) did not display correctly in the message log.
- CSCsj26541–Some wireless LAN configuration changes such as changing network data rates did not take effect for 1500 series access points when operating in RAP mode without a reboot.The workaround was to use the controller GUI to disable the access point's backhaul radio, change the data rate, and then re-enable the backhaul radio.
- CSCsj48044–In some cases, public safety information did not display accurately in Cisco WCS. The workaround was to query the information using the controller GUI or CLI, where applicable.

- CSCsj59145–When a VLAN was configured on a mesh backhaul radio that did not support client access, an error similar to the following could display: “Jul 10 00:09:44.587: LWAPP_CLIENT_ERROR_DEBUG: spamDecodeMwarMsg: Could not match Vapid 3.” this condition was not service affecting.
- CSCsj67716–When1522 and 1510 were operating in the same network, public safety channels for the 1510 might display (**show mesh neigh summary** *Cisco_AP*) the public safety channel values of 190 or 196 rather than 20 and 26, if the AP1510 was operating with a release earlier than 4.1.181.0. Channels 20 and 26 were adopted for public safety transmissions in release 4.1.181.0. Previous releases used channels 190 and 196 for public safety transmission. This was a display issue only. It was not service affecting.
- CSCsj78944–Inaccurate SNR values were reported to Cisco WCS from the controller, rendering inaccurate data in Cisco WCS Worst SNR Report.
- CSCsj87294–Channel changes for the 1520 might not be immediate when operating in the US regulatory domain. In some cases, the 1520 might take up to 30 minutes to rejoin.
- CSCsk47555–In some cases, AP Mode (Monitor > Access Point > *AP_Name* > *General Parameters*) would display as Local when the access points were in Bridge mode.
- CSCsk07157–When operating as a MAP, the AP1522 generally prefers to select a parent that shares the same bridge group name (BGN), rather than a wired interface (uplink) to the controller. This approach is different from the AP1510 which always places a higher priority on selecting a parent with a wired connection.

  Additionally, when a 1522 mesh access point connects to a parent with a default (null) BGN, the 1522 disables the Ethernet Bridging feature to prevent a potential bridge loop. This behavior also differs from that of the AP1510.

  The workaround involved configuring a bridge group name for the AP1520 and verifying that its parent was on the same bridge group to allow Ethernet Bridging.
- CSCsk07319–The txpkts rate for the neighboring mesh node always displayed a value of 5000 in the text of the **show mesh adjacency all** command for the AP1522. There was no workaround.
- CSCsk19379–Link test to AP1520 neighbors was not supported.
- CSCsk21520–The AP Join Taken Time displayed by the **show ap config general** *Cisco_AP* command was inaccurate for 1520s. This error generally occurred in multi-hop configurations.
- CSCsk47555—In Cisco WCS, the access point would display as local rather than bridging mode on the monitor list page.
- CSCsk48251–An Admin disabled mesh access point would disconnect from the controller and only momentarily join the controller before disconnecting. The mesh access point would then reboot in 30 minutes because it had not reassociated with a controller. The controller would often repeat this rejoin, disconnect and reboot cycle several times.
- CSCsk63833, CSCsk63809–The fallback from secondary to primary controller could take up to 20 minutes.
- CSCsk75003–An AP1520 with a cable modem link was assigned an extra IP address. The extra IP address was allocated by the DHCP server because of a DHCP Discover Requests sent to determine link status of the cable.
- CSCsl00807– When a controller was configured for the -K regulatory domain, the 802.11a radio transmission level configuration window in the controller GUI displayed only four levels rather than the supported five levels (Wireless > Radio > 802.11a A-radio > *AP Name* > *Antenna* > *Configure* > *Tx Power Level Assignment* > *Assignment Method* > *Custom*). Additionally, transmission power levels 1 to 5 were not seen for the -S and -C regulatory domains.

- CSCsl01069–In some circumstances, the mesh network would not form in optimal topologies and MAPs would make unnecessary parent changes which would result in small outages in network service (on the order of several seconds).
- CSCsl15370–A 1510 child MAP would fail to connect to the network during its security stage if it was connecting to controllers whose names had different string lengths. The workaround was to use the same string length for all controller names; and update each MAP with the relevant controller name. Ensure that the modified name is reflected for the primary, secondary and tertiary controller names.
- CSCsl24573–In some cases, the MAC addresses of some mesh access points appeared in the Excluded Client list of controllers. You could not remove (delete) the MAP entry from the Excluded Client List. However, these MAPs were able to join the network by associating through a different controller. The workaround was to reboot the controller to clear the client entries.

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.

- CSCsg60778–When background scanning is enabled, it may cause temporary backhaul congestion, which might result in voice packet loss and jittery voice traffic.

  Workaround: Turning off background scanning can alleviate this problem to some extent. However, if the packet loss and the jittery voice traffic are due to RF issues, then changing the RAP to a different channel might help.
- CSCsi07934—Efficient multicast to 802.11 clients is not supported on mesh access points.Therefore, you should not turn on multicast mode on the controller when it needs to service mesh access points. If you do, the mesh access points may start disconnecting due to issues with queue overflow at the MAPs. This issue applies to all controller commands starting with: **config network multicast**

  Workaround: If you need to turn on the controller multicast mode for non-mesh access points, service mesh access points on a different controller than the one used for non-mesh access points.
- CSCsi67588, CSCsi74994–Bridge group names applied by Cisco WCS Access Point templates are not updated in WCS windows because the controller initiates a reboot of the relevant mesh access point before the information can be updated in Cisco WCS.

  Workaround: At the **Configure > Access Point** window, select **Audit** from the Select a command drop-down menu and click **GO.** at the Configure > Access Points to update the access point information.
- CSCsi74994–See description under CSCsi67588 above.
- CSCsi83262–The back up battery for an AP1510 provides no warning when the AC source fails.

  Workaround: Battery status warnings available in WCS and controller GUI and CLI.
- CSCsi83272–After detaching and reattaching a probe to a backup battery on an AP 1510 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.

  Workaround: Keep probe attached to the battery for 30 minutes for accurate reading.
- CSCsi84448–When a backup battery on an AP1510 has a charge of 1% or less, it does not display that information when the **show mesh env detail** *AP-name* command is entered.

  Workaround: None.

- CSCsk40572—The CLI command **show network** mistakenly displays a status for the Bridge MAC Filter Config parameter. This parameter is not a configurable option in release 4.1.191.xM.

  Workaround: None.
- CSCsk86926–Voice calls originating from Cisco 7921 phones and transmitted over 1240 mesh access points will not authenticate if using EAP-FAST.

  Workaround: Set EAP request timeout to 20.
- CSCsk86942–Voice calls originating from Cisco 7921 phones and transmitted over 1240 mesh access points might experience quality issues when configured for more than one hop. Similar behavior might occur for IP phones by other vendors.

  Workaround: Set EAP timeout values larger than the default for clients.

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://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

(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 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*
- *Cisco Aironet 1520 Series Outdoor Mesh Access Points*
- *Cisco Aironet Series Power Injector Installation Instructions*
- *Cisco Aironet Series 1500 Access Point LED Indicator Installation Instructions*
- *Cisco Aironet 8-dBi Omnidirectional Antenna (AIR-ANT5180V-N)*
- *Cisco Aironet 5-dBi Omnidirectional Antenna (AIR-ANT2450V-N)*

- *Cisco Wireless LAN Controller Configuration Guide, Release 4.2*
- *Cisco Wireless LAN Controller Command Reference, Release 4.2*
- *Cisco Wireless Control System Configuration Guide, Release 4.2*
- *Troubleshooting a Mesh Network*

Note You can view the latest online versions of these documents at the following link: http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.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