



# Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 4.1.192.35M

---

**Last Revised: September 01, 2009**

These release notes describe features, enhancements, and caveats in release 4.1.192.35M.

Release 4.1.192.35M is compatible with releases 5.0 and 5.1 of the Cisco Wireless Control System (WCS) and is supported on the following Cisco Wireless LAN controller platforms:

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

Release 4.1.192.35M supports full interoperability between the following indoor and outdoor mesh access points:

- Cisco Aironet 1520 (1522, 1524) series and 1500 (1505 and 1510) series outdoor access points
- Cisco Aironet 1130AG and 1240 AG series indoor access points.



## Note

Release 4.1.192.35M 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 in 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 4.1.192.35M 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.



## Caution

A downgrade to mesh releases 4.1.190.5, 4.1.191.24M, and 4.1.192.35M from non-mesh release 4.2 is **not** supported. Please see the [“System Requirements” section on page 18](#) for important software upgrade and compatibility details prior to upgrading to this release.



**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.



**Caution**

If your network is operating with 1522s or you plan to install 1522s in your network, you must set the boot variable on the 1522 before upgrading from release 4.1.190.5 to 4.1.191.24M or from 4.1.191.24M to 4.1.192.35M. This ensures that the 1522 joins correctly (CSCsl70218).



**Caution**

A GUI and CLI message warning users not to select *global* as the backhaul setting is missing in release 4.1.192.35M. This message was present in 4.1.191.24M. The same warning applies even though it is not shown in the current release. Configuring the ‘global’ setting on a backhaul setting often causes unpredictable behavior and might cause network problems with the mesh access points. Therefore, do not configure the *global* setting on mesh access point backhauls using the CLI and GUI (CSCso21425).



**Note**

Refer to the *Cisco Aironet 1520 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](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 5.0* for details on monitoring the mesh network (access points, links, statistics, alarms) at: <http://www.cisco.com/en/US/docs/wireless/wcs/5.0/configuration/guide/wcsmon.html>



**Note**

Refer to “Running Reports” (Chapter 14) in the *Cisco Wireless Control System Configuration Guide, Release 5.0* for more details on mesh reports at: <http://www.cisco.com/en/US/docs/wireless/wcs/5.0/configuration/guide/wcsreps.html>

## Contents

These release notes contain the following sections:

- [Important Notes, page 2](#)
- [System Requirements, page 18](#)
- [Converting Indoor Access Points to Mesh Access Points \(1130AG, 1240AG\), page 24](#)
- [Documentation Updates, page 27](#)
- [Caveats, page 30](#)
- [Troubleshooting, page 38](#)
- [Related Documentation, page 38](#)
- [Obtaining Documentation, Support, and Security Guidelines, page 39](#)

## Important Notes

This section describes information about new hardware and software features, and operational notes for release 4.1.192.35M.

**Note**

Release 4.1.192.35M 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

### NEW Series 1520 Access Point, 1524

The latest 1520 series access point, 1524, includes three radios: a 2.4-GHz, a 5.8-GHz, and a 4.9-GHz radio. The 2.4-GHz radio is for client access (non-public safety traffic) and the 4.9-GHz radio is for public safety client access traffic only. The 5.8-GHz radio is used as the backhaul for both public safety and non-public safety traffic.

The 4.9-GHz and 5.8-GHz radios are 802.11a sub-band radios which support a subset of specific 802.11a channels and include a sub-band specific filter designed to lessen interference from other 11a sub-band radios within the same access point. The 4.9-GHz sub-band radio on the 1524 access point supports public safety channels within the 5-MHz (channels 1 to 10), 10-MHz (channels 11-19), and 20-MHz (channels 20-26) bandwidths.

- The following data rates are supported within the 5 MHz bandwidth: 1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5 Mb/s. *Default rate is 6 Mb/s.*
- The following data rates are supported within the 10 MHz bandwidth: 3, 4.5, 6, 9, 12, 18, 24, and 27 Mb/s. *Default rate is 12 Mb/s.*

**Note**

- Those 1522 mesh access points with serial numbers *prior* to FTX1150XXXX do **not** support 5 and 10 MHz channels on the 4.9-GHz radio; however, a 20-MHz channel is supported.
- Those 1522 mesh access points with serial numbers *after* FTX1150XXXX support 5, 10 and 20 MHz channels.

**Note**

For public safety only deployments, 1522s and 1524s must each be connected to its own separate RAP-based tree. For such deployments, 1522s must use the 4.9-GHz backhaul and 1524s must be in their own RAP tree(s) and use the 5.8-GHz backhaul.

**Note**

Universal access, which allows client access over the 5.8-GHz backhaul radio, is not supported on the 1524; however, it is supported on the 1522 and indoor mesh access points (1130, 1240). For more details on Universal Access see the [“Backhaul Client Access \(Universal Access\) for Indoor and Outdoor Mesh Access Points”](#) section on page 6.

### Additional Access Point Support

Release 4.1.192.35M also 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: 5.15-GHz, 5.25-GHz, and 5.47-GHz.
- 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: 5.15-GHz, 5.25-GHz, and 5.47-GHz.




---

**Note** Mesh 1242 access points are exclusive Indoor Mesh access points. These access points do not provide Outdoor Mesh support.

---

- 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 5-GHz radio on the 1510 supports the following bands: 4.9-GHz, 5.47-GHz, and 5.8-GHz.
- 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 5-GHz radio on the 1522 supports the following bands: 4.9-GHz, 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.
  - Models 1130 (1100 series) and 1240 (1200 series) operating as non-mesh nodes are also supported.

[Table 1](#) provides a summary of hardware options and band support by platform.

**Table 1**      **Hardware Feature and Band Support by Platform**

Feature/Platform	1505	1510	1522	1524 <sup>1</sup>	1130	1240
2.4-GHz band	X	X	X	X	X	X
4.9-GHz band	–	X	X	X	–	–
5.15-GHz band	–	–	–	–	X	X
5.25-GHz band	–	–	X	–	X	X
5.47-GHz band	–	X <sup>2</sup>	X <sup>3</sup>	–	X	X
5.8-GHz band	–	X <sup>4</sup>	X <sup>5</sup>	X	–	–
DOCSIS 2.0 cable modem (optional)	–	–	X	–	–	–
Fiber module (optional)	–	–	X	–	–	–
External battery status	X	X	–	X	–	–
Internal battery status	–	–	X	X		
LEDs	X <sup>6</sup>	X <sup>5</sup>	X	X <sup>7</sup>	X	X

1. Mesh access point 1524 is only supported in the -A regulatory domain in release 4.1.192.35M. This includes the following countries: Argentina, Brazil, Canada, Chile, Paraguay, Puerto Rico, United States, and Venezuela.
2. The 5.47-GHz band is used by the -E and -K regulatory domains for the 1510.
3. The 5.47-GHz band is used by the -A, -E, -K, and -T regulatory domains for the 1522.
4. The 5.8-GHz band is used by the -A, -C, -N, and -S regulatory domains for the 1510.
5. The 5.8-GHz band is used by the -A, -C, -N, -S and -T regulatory domains for the 1522.
6. An optional removable Cisco LED indicator is available to detect power for the 1505 and 1510.
7. The 1524 and 1522 mesh access points support the same LEDs. The four access point LEDs monitor system and uplink status; 802.11a radio and 802.11b/g radio status.

## 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, 1522, and 1524) and indoor mesh access points (1130 and 1240) 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.



### 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 24](#) 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 4.1.192.35M.

### Series 1520 Mesh Access Point Interoperability with Cisco 3200 Mobile Access Routers

Cisco series 1520 (1522, 1524) access points can interoperate with the Cisco series 3200 Wireless Mobile Access Router (MAR) on the public safety channel (4.9-GHz) as well as the 2.4-GHz access and 5.8-GHz backhaul.

The Cisco 3200 creates an *in-vehicle network* in which devices such as PCs, surveillance cameras, digital video recorders, printers, PDAs, and scanners can share wireless networks such as cellular or WLAN based services back to the main infrastructure. This allows data collected from in-vehicle deployments such as a police cars to be integrated into the overall wireless infrastructure. For specific interoperability details between series 1130, 1240, and 1520 mesh access points and series 3200 mobile access routers, refer to [Table 2](#).

**Table 2**      **Mesh Access Points and MAR 3200 Interoperability**

Mesh Access Point Model	MAR Model
1522 <sup>1</sup>	c3201 <sup>2</sup> , c3202 <sup>3</sup> , c3205 <sup>4</sup>
1524	c3201, c3202
1130, 1240 configured as indoor mesh access points with universal access	c3201, c3205

1. Universal access must be enabled on the 1522 if connecting to a MAR on the 802.11a radio or 4.9-GHz band.
2. Model c3201 is a MAR with a 802.11b/g radio (2.4-GHz).
3. Model c3202 is a MAR with a 4-9-GHz sub-band radio.
4. Model c3205 is a MAR with a 802.11a radio (5.8-GHz sub-band).

For configuration details refer to the [“Configuring Interoperability with the Series 3200 Mobile Access Router”](#) section on page 27.

### Backhaul Client Access (Universal Access) for Indoor and Outdoor Mesh Access Points

You can configure the backhaul for mesh access points (1522, 1510, 1240 and 1130) to accept client traffic. When this feature is enabled, mesh access points allow wireless client association over the 802.11a radio. This universal access allows an access point to carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, backhaul traffic is only transmitted over the 802.11a radio and client association is only allowed over the 802.11b/g radio.

After this feature is enabled, all mesh access points reboot.

**Default:** Disabled.



**Note** This parameter is applicable to mesh access points with two radios (1522, 1510, 1240 and 1130) *excluding* the 1524. However, backhaul client access is always automatically enabled for the single 802.11b/g radio on the 1505.

**Note**

To enable this feature on the controller, check the Backhaul Client Access check box on the **Wireless > Mesh** window.

## External AAA (RADIUS) Server for Mesh Access Points

External authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later) is supported in this release.

Before you employ external authentication within the mesh network, you must make these changes:

- Configure the RADIUS server to be used as an AAA server on the controller.
- Configure the controller on the RADIUS server.
- Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server. For additional details, refer to [“Adding a Username to a RADIUS Server” section on page 8](#).
- Configure EAP-FAST on the RADIUS server and install certificates. EAP-FAST authentication is required if mesh access points are connected to the controller using an 802.11a interface; the external RADIUS servers need to trust Cisco Root CA 2048.

**Note**

Controllers and access points have a Certificate Authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific CA certificate, it must be downloaded to the controller.

- For information on installing and trusting the CA certificates, see the "Transferring Files to and from a Controller" section in Chapter 9 of the *Cisco Wireless LAN Configuration Guide*:
- <http://www.cisco.com/en/US/docs/wireless/controller/5.2/configuration/guide/c52mfw.html#wp1051903>
- For information on configuring local EAP:  
<http://www.cisco.com/en/US/docs/wireless/controller/5.2/configuration/guide/c52sol.html#wp1172157>

**Note**

Local EAP and PSK authentication within the controller is also supported.

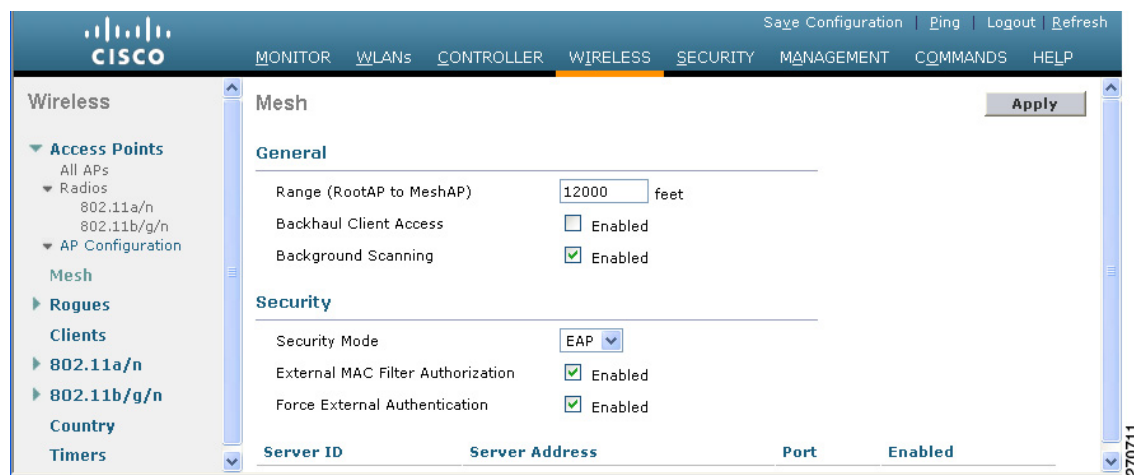
For additional configuration details on Cisco ACS servers, refer to the following link:

[http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products\\_installation\\_and\\_configuration\\_guides\\_list](http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list)  
(Windows)

To enable external authentication for a mesh access point using the GUI, do the following.

- Step 1** In the controller GUI, click **Wireless > Mesh**. The mesh general and security window appears (Figure 1).

**Figure 1** *Wireless > Mesh*



- Step 2** In the security section, select the **EAP** option from the Security Mode drop-down menu.
- Step 3** Check the **Enabled** check boxes for the External MAC Filter Authorization and Force External Authentication options.
- Step 4** Click **Apply**.
- Step 5** Click **Save Configuration**.

To enable external authentication for mesh access points using the CLI, enter the following commands:

```
config mesh security eap
config macfilter mac-delimiter colon
config mesh security rad-mac-filter enable
config mesh radius-server index enable
config mesh security force-ext-auth enable (Optional)
```

### Adding a Username to a RADIUS Server

MAC addresses of mesh access point that are authorized and authenticated by external RADIUS servers must be added to the user list of that server.

For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.

- For VxWorks-based mesh access points (1505 and 1510), the Ethernet address is incorporated into the certificate-based identity; therefore, their username for external RADIUS servers is their Ethernet MAC address hex string without colons such as *001122334455*.



- For IOS-based mesh access points (1240, 1522, 1524), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, their username for external RADIUS servers is *platform\_name\_string-Ethernet MAC address* such as *c1240-001122334455*.

## Workgroup Bridge Support

A workgroup bridge (WGB) connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the mesh access point using Internet Access Point Protocol (IAPP) messaging. The mesh access point treats the WGB as a wireless client.

When configured as a WGB, the 1130, 1240, and 1310 autonomous access points as well as the series 3200 mobile access router (MAR) can associate with mesh access points. The mesh access points can be configured as RAPs or MAPs. WGB association is supported on both the 2.4-GHz (802.11b) and 5-GHz (802.11a) radio on the 1522, and the 2.4-GHz (802.11b) and 4.9-GHz (public safety radio) on the 1524.

### Supported Workgroup Modes and Capacities

- The 1130, 1240, 1310 autonomous access point must be running Cisco IOS release 12.4(3g)JA or later (on 32-MB access points) or Cisco IOS release 12.3(8)JEB or later (on 16-MB access points). Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.



**Note** If your access point has two radios, you can only configure workgroup bridge mode on one of the radios. Cisco recommends that you disable the second radio.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported.
- Mesh access points can support up to 200 clients including wireless clients, WGBs, and wired clients behind the associated WGBs.
- WGBs operating with Cisco IOS release 12.4(3g)JA cannot associate with mesh access points if the WLAN is configured with WPA1 (TKIP) +WPA2 (AES), and the corresponding WGB interface is configured with only one of these encryptions (either WPA1 or WPA2).

## Client Roaming Supported on 1522 and 1524 Access Points

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 mph in outdoor mesh deployments on series 1520 (1522, 1524) mesh access points. An example application might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network.

Three Cisco CX v4 Layer 2 client roaming enhancements are supported:

- **Access point assisted roaming**—This feature helps clients save scanning time. When a Cisco CX v4 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.

- **Enhanced neighbor list**—This feature focuses on improving a Cisco CX v4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.
- **Roam reason report**—This feature enables Cisco CX v4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

## Mesh Multicast Containment for Video

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

Mesh multicast modes determine how bridging-enabled access points [mesh access points (MAPs) and root access points (RAPs)] send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-LWAPP multicast traffic only. LWAPP multicast traffic is governed by a different mechanism.

The three mesh multicast modes are:

- **Regular mode**—Data is multicast across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs.
- **In mode**—Multicast packets received from the Ethernet by a MAP are forwarded to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-LWAPP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP-to-MAP multicasts do not occur because they are filtered out.
- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP Ethernet networks, and the MAP-to-MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.
  - In-out mode is the default mode.



### Note

If 802.11b clients need to receive LWAPP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the **config network multicast global enable** CLI command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled (using the **config network multicast global disable** CLI command).

To enable multicast mode on a mesh network, enter this command:

```
config mesh multicast { regular | in | in-out }
```

## Support for 16 SSIDs on Series 1520 (1522, 1524) Access Points

Series 1520 (1522, 1524) mesh access points now support up to 16 SSIDs on each access radio. Previously, only 8 were supported.

The 1510 continue to support 16 SSIDs.

Indoor mesh access points (1130, 1240) continue to support a maximum of 8 SSIDs on each radio.

## Brown-Out Notification

A brown-out trap is generated and sent to the controller to aid in troubleshooting when a mesh access point experiences a reset, power outage, or drop in voltage below an acceptable threshold.



### Note

The following types of power outages at the mesh access point generate and send brown-out traps to the controller: External power loss, generic Power-over-Ethernet (PoE) loss, change of PoE source, power injector loss, AC power lost, cable power lost, and too high or too low power source.

## New and Modified CLI Commands on the Controller

- **config 802.11-a49:** Configures the 4.9-GHz sub-band radio.

*where*

**antenna extAntGain** *antenna gain Cisco\_MAP*: Configures the 802.11a 4.9-GHz antenna.

**channel** {**ap** *Cisco\_MAP channel number* | **global**}: Configures either a single 802.11a 4.9-GHz channel (ap) or enables auto-RF (global).

**disable** *Cisco\_MAP*: Disables the 802.11a 4.9-GHz sub-band radio.

**enable** *Cisco\_MAP*: Enables the 802.11a 4.9-GHz sub-band radio.

**txPower** *Cisco\_MAP power level*: Configures the Tx power level for the 802.11a 4.9-GHz sub-band radio.

- **config 802.11-a58:** Configures the 5.8-GHz sub-band radio.

*where*

**antenna extAntGain** *antenna-gain Cisco\_MAP*: Configures the 802.11a 5.8-GHz antenna.

**channel** {**ap** *Cisco\_MAP channel number* | **global**}: Configures either a single 802.11a 5.8-GHz channel (ap) or enables auto-RF (global).

**disable** *Cisco\_MAP*: Disables the 802.11a 5.8-GHz sub-band radio.

**enable** *Cisco\_MAP*: Enables the 802.11a 5.8-GHz sub-band radio.

**txPower** *Cisco\_MAP power level*: Configures the Tx power level for the 802.11a 5.8-GHz sub-band radio.

- **config advanced 802.11-a49 profile:** Configures the 4.9-GHz radio profile.

*where*

**coverage** *Cisco\_MAP threshold value*: Configures the 802.11a coverage threshold. Values are 3 and 50 dB.

**customize** *Cisco\_MAP* {**on** | **off**}: Turns the performance profile either on or off.

**exception {global | Cisco\_MAP} percent:** Configures the 802.11a coverage exception level as either global or for an individual access point. Values are 0 to 100.

**foreign {global | Cisco\_MAP} percent:** Configures the 802.11a interference threshold as either global or for an individual access point. Values are 0 to 100.

**level Cisco\_MAP clients:** Configures the 802.11a client minimum exception level. Values are 1 to 75 clients.

**clients Cisco\_MAP clients:** Configures the 802.11a client threshold. Values are 1 to 75 clients.

**noise {global | Cisco\_MAP} threshold:** Configures the 802.11a foreign noise threshold as either global or for an individual access point. Values are -127 to 0 dBm.

**throughput {global | Cisco\_MAP} threshold:** Configures the 802.11a throughput threshold as either global or for an individual access point. Values are 1000 and 10000000 bytes per second.

**utilization {global | Cisco\_MAP} percent:** Configures the 802.11a RF utilization threshold as either global or for an individual access point. Values are 0 to 100.

- **config slot slot-ID**

where

**enable Cisco\_MAP:** Enables a slot for a particular mesh access point.

**disable Cisco\_MAP:** Disables a slot for a particular mesh access point.

**channel ap Cisco\_MAP {channel number | global}:** Configures a single 802.11a 5.8-GHz channel for the slot or enables auto-RF (global).

**chan\_width Cisco\_MAP channel-width:** Configures the channel width for a slot.

**txPower ap Cisco\_MAP {power level | global}:** Configures the Tx power level for the slot.

- **show ap config {802.11-a49 | 802.11-a58} {Cisco\_MAP | summary}:** Displays detailed or summary information for either a 4.9-GHz or 5.8-GHz sub-band 802.11a radio.
- **show client ap 802.11-a49:** Displays client information for a 4.9-GHz sub-band radio.
- **show ap slots:** Displays slot information for mesh access points.

```
(Cisco Controller) > show ap slots
Number of APs..... 3
AP Name Slots AP Model      Slot0      Slot1      Slot2      Slot3
-----
R1      2      LAP1510      802.11A    802.11BG
H1      3      AIR-LAP1521AG-A-K9 802.11BG 802.11A    802.11A
H2      4      AIR-LAP1521AG-A-K9 802.11BG 802.11A    802.11A 802.11BG
```

- **show mesh ap tree:** Displays mesh access points within a tree structure (hierarchy).

```
(Cisco Controller) > show mesh ap tree
R1(0,y1)
|-R2(1,y1)
|-R6(2,y1)
|-H2(1,default)
Number of Mesh APs..... 4
Number of RAPs..... 1
Number of MAPs..... 3
```

- **show mesh ap summary:** Revised to show the CERT MAC field which shows a MAC address within an AP certificate that can be used to assign a username for external authentication.

```
(Cisco Controller) >show mesh ap summary
```

AP Name	AP Model	BVI MAC	CERT MAC	Hop	Bridge Group Name
R1	LAP1510	00:0b:85:63:8a:10	00:0b:85:63:8a:10	0	y1
R2	LAP1510	00:0b:85:7b:c1:e0	00:0b:85:7b:c1:e0	1	y1
H2	AIR-LAP1522AG-A-K9	00:1a:a2:ff:f9:00	00:1b:d4:a6:f4:60	1	
Number of Mesh APs.....				3	
Number of RAPS.....				2	
Number of MAPs.....				1	

## Continued Feature Support

A summary of previously released mesh software features supported by each mesh access point is provided in [Table 3](#).

**Table 3** Mesh Access Point Feature Support Matrix for 4.1.192.35M

Feature/Platform	1505	1510	1522	1524	1130	1240
<b>Mesh Network Functionality</b>						
<b>Passive scanning</b> —Access point searches for an alternative parent on its current backhaul.	X	X	X	X	X	X
<b>Background Scanning</b> —Access point searches for an alternative parent on any possible backhaul channel.	X	X	—	—	—	—
<b>Optimal Parent Selection</b> —Access point joins the best available parent.	X	X	X	X	X	X
<b>Exclusion Listing</b> —Access point avoids selecting as parent those access points which have a pattern of failing.	X	X	X	X	X	X
<b>Radar-free Coordinated Sector</b> —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	X
<b>Dynamic Frequency Selection</b> —Alternative channel is selected when radar is detected in regulated bands.	—	X	X	—	X	X
<b>Synchronized Channel Change</b> —Parent advises children of intended channel change.	X	X	X	X	X	X
<b>Reliable Link Layer, Extended Retries</b> —Transmissions that do not succeed will extend the number of retry attempts in an effort to improve reliability.	—	X	—	—	—	—
<b>Reliable Link Layer, Secondary Backhaul Radio</b> —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	—	—	—	—

**Table 3**      **Mesh Access Point Feature Support Matrix for 4.1.192.35M (continued)**

<b>Feature/Platform</b>	<b>1505</b>	<b>1510</b>	<b>1522</b>	<b>1524</b>	<b>1130</b>	<b>1240</b>
<b>Passive Beaconing</b> —Log messages from an access point that cannot connect are relayed through other access points to the controller.	X	X	X	X	X	X
<b>Network Services Functionality</b>						
<b>Ethernet Bridging</b> —Traffic is bridged from hosts connected to a wired port.	X	X	X	X	X	X
<b>Containment of Bridged Multicast Traffic</b> —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	X	X	X	X
<b>Universal Access</b> —Radio used for backhaul traffic provides access for client traffic	X	X	X	—	X	X
<b>Support for Workgroup Bridges</b> —Allows multiple wired hosts to connect to the wireless network through a workgroup bridge.	X	X	X	X	X	X
<b>Multiple Queues for Backhaul Traffic</b> —Extends client traffic prioritization to the backhaul traffic.	X	X	X	X	X	X
<b>Static Call Admission Control (CAC)</b> —Ensures sufficient bandwidth is available in a mesh sector before serving new T-SPEC client call requests.	—	X	—	—	—	—
<b>Mesh Security</b>						
<b>EAP Authentication</b> —Restricts mesh node access to approved, authenticated access points. EAP-FAST authentication provides secure authentication and encryption key management.	X	X	X	X	X	X
<b>Applications</b>						
<b>High-speed Roaming</b> —Roam speeds of up to 70 mph are supported for Cisco Compatible Extension v4 clients.	—	X	X	X	—	—

## Software Images

Table 4 lists the names of the images associated with this release.

**Table 4** *Software Images Associated with Release 4.1.192.35M*

Products	4.1.192.35M and Related Software Images		
Access Point		Image	Boot Image
	1130	c1130-k9w9-tar.124-3g.JMC (mesh, bridge mode)  c1130-k9w8-tar.124-3g.JMC (non-mesh, local mode)	c1130-boot.m.124-3g.JMC
	1240	c1240-k9w9-tar.124-3g.JMC (mesh, bridge mode)  c1240-k9w8-tar.124-3g.JMC (non-mesh, local mode)	c1240-boot.m.124-3g.JMC
	1505	VxWorks	VxWorks
	1510	VxWorks	VxWorks
	1522, 1524	c1520-k9w9-tar.124-3g.JMC	c1520-boot-m.124-3g.JMC
MAR 3201	c3201-k9w7-tar.124-3.JK1.tar		MAR boot images are installed during MAR manufacture. Images cannot be downloaded from Cisco.com.
MAR 3202	c3202-k9w7-tar.124-3.JK1.tar		
MAR 3205	c3205-k9w7-tar.124-3.JK1.tar		
WLC-4400	AIR-WLC4400-K9-4-1-192-35M-MESH.aes		
WLC-2100	AIR-WLC2100-K9-4-1-192-35M-MESH.aes		
WiSM	AIR-WLC4400-K9-4-1-192-35M-MESH.aes		
	<b>Note</b>	The Catalyst 6500 Supervisor 720 image is s72033_rp-ADVENTERPRISEK9_DBG-M	
WCS	WCS-STANDARD-K9-5.0.56.0.exe		
	<b>Note</b>	For release 4.1.192.35M, Cisco WCS is only supported on Windows Server 2003.	
WCS Navigator	NAVIGATOR-K9-1.2.56.exe		
	<b>Note</b>	For release 4.1.192.35M, 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 4.1.192.35M.

New controller GUI windows and CLI commands are summarized under the [“Software Features and Enhancements”](#) section on page 6 of this release note.

## 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 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 4.1.192.35M (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\_MAP** command (CSCsk64812).

## 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.a3800* 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.a300    29/84          OFF    UpDnDnDn N/A
rap1524.4d00     31/87            OFF     UpDnDnDn  N/A
```

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 AP1510s with Power Supply 1.01d Firmware

An AP1510 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](mailto: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).

## 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 Mb/s. 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.

## 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?*

## Warning Message Added When Changing Antenna Gain

The following warning message appears when a change to the antenna gain is made on either the 1522 or 1524 radio. This message appears for both the controller CLI (**config 802.11a antenna extAntGain**) and GUI (Wireless > Access Points > Radios). (CSCsl75327)

*Changing antenna gain can make current channel unusable. The AP will be rebooted. A new channel must be chosen once the AP rejoins. If no channel is available with the new antenna gain, it will return back to the original value. 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?*

# 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 the 1522 mesh access point in your mesh network. Release 4.1.192.35M is required for the 1524 mesh access point.
  - Release 4.2.x and earlier 4.1.x releases will not support 1520 series mesh access points.
  - A 1522 mesh access point operating with release 4.1.190.5 is only supported in the US and Canada.

Release 4.1.191.24M (and later) provides international support for 1522s, 1240s, and 1130s and support for the UNI-2 band in the US.

- If a 1522 mesh access point is operating in a network, and you downgrade the software release within your network to a non-mesh release, the 1522 will not reconnect and might become stranded.
- If 1522s 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 1522 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 1522s.
  - 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 1522 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 1522.



### Note

Upgrading to 4.1.192.35M or later provides full interoperability between 1510s and 1522s. Release 4.1.190.5 does not provide full interoperability. Refer to the [“Upgrade Compatibility Matrix” section on page 19](#) for upgrade path specifics.

- If 1524s are going to be installed in a mesh network, then note the following:
  - Release 4.1.192.35M is required for the 1524 mesh access point.

- A 1524 is only supported in the -A regulatory domain in release 4.1.192.35M. This includes the following countries: Argentina, Brazil, Canada, Chile, Paraguay, Puerto Rico, United States and Venezuela.
- 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.
  - All other indoor access points (excluding 1250) operate as standard, non-mesh access points.

**Caution**

Indoor access points 1130 and 1240 configured as mesh access points (bridge mode) should not be connected to a controller without mesh release 4.1.191.24M or later installed. The 1130 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 26 for details on the conversion.

## Upgrade Compatibility Matrix

[Table 5](#) 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 21.

**Table 5 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases**

Upgrade to	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																									
4.1.192.22M	Y	–									Y	–													
4.1.191.24M	Y	–																							
4.1.190.5	Y <sup>1</sup>	Y	–																						
4.1.185.0		Y	Y <sup>2</sup>	–																					
4.1.181.0			Y <sup>2</sup>	Y <sup>2</sup>																					
4.1.171.0			Y <sup>2</sup>	Y <sup>2</sup>	–																				
4.0.219.0				Y <sup>2</sup>	Y <sup>2</sup>	–																			
4.0.217.204		Y <sup>2</sup>		Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>2</sup>	–																		
4.0.217.0				Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>3</sup>	–																	
4.0.216.0				Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>3</sup>	Y	–																
4.0.206.0				Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>2</sup>	Y <sup>3</sup>	Y		–															
4.0.179.11								Y		Y <sup>4</sup>	–														
4.0.179.8								Y		Y <sup>4</sup>	Y	–													
4.0.155.5								Y		Y <sup>4</sup>	Y	Y	–												
4.0.155.0								Y		Y <sup>4</sup>	Y	Y	Y	–											
3.2.195.10								Y		Y <sup>4</sup>	Y	Y	Y		–										
3.2.193.5								Y		Y <sup>4</sup>	Y	Y	Y		Y	–									
3.2.171.6								Y		Y <sup>4</sup>	Y	Y	Y		Y		–								
3.2.171.5								Y		Y <sup>4</sup>	Y	Y	Y		Y		Y	–							
3.2.150.10								Y		Y <sup>4</sup>	Y	Y	Y		Y		Y		–						
3.2.150.6								Y		Y <sup>4</sup>	Y	Y	Y		Y		Y		Y	–					
3.2.116.21								Y		Y <sup>4</sup>	Y	Y	Y		Y		Y		Y		–				
3.2.78.0								Y		Y <sup>4</sup>	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 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.
2. 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.
3. Release 4.0.217.204 provides fixes for DFS on the 1510. This functionality is only needed in countries where DFS rules apply.
4. 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).

## Upgrading to this Software Release

For instructions on downloading software to the controller using Cisco WCS, refer to the release 5.0 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](http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html)

For instructions on downloading mesh release 4.1.192.35M software to the controller using the controller GUI or CLI, refer to [Software Upgrade Procedure, page 22](#).

### Upgrade Path to Release 4.1.192.35M

Details for upgrading your network to release 4.1.192.35M 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 three intermediate releases (or two if a DFS network) prior to installing 4.1.192.35M in your network.

Detailed steps are noted below.

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Upgrade to 4.1.185.0 (non-DFS network) or to 4.0.217.204 (DFS network).        |
| <b>Step 2</b> | Upgrade to 4.1.190.5 (not required for networks that upgraded to 4.0.217.204). |
| <b>Step 3</b> | Upgrade to 4.1.191.24M.  |
| <b>Step 4</b> | Upgrade to 4.1.192.35M.  |
- 

**If your controller is installed with release 4.0.1xx.x or 3.2.xx**, you must upgrade with four intermediate releases (or three if a DFS network) prior to installing release 4.1.192.35M.

Detailed steps are noted below.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Upgrade to 4.0.217.0.   |
| <b>Step 2</b> | Upgrade to release 4.0.217.204 (DFS network) <b>or</b> 4.1.185.0 (non-DFS network).   |
| <b>Step 3</b> | Upgrade to release 4.1.190.5 (not required for networks that upgraded to 4.0.217.204) |
| <b>Step 4</b> | Upgrade to release 4.1.191.24M.   |
| <b>Step 5</b> | Upgrade to 4.1.192.35M.   |
-

**If your controller is installed with release 3.1.x**, you must upgrade with five intermediate releases (or four if a DFS network) prior to installing release 4.1.192.35M.

- 
- Step 1** Upgrade to 3.2.195.10.
  - Step 2** Upgrade to 4.0.217.0
  - Step 3** Upgrade to 4.1.185.0 (non-DFS network) **or** 4.0.217.204 (DFS network).
  - Step 4** Upgrade to release 4.1.190.5 (not required for networks that upgraded to 4.0.217.204).
  - Step 5** Upgrade to release 4.1.191.24M.
  - Step 6** Upgrade to release 4.1.192.35M.
- 

## 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 releases 4.1.192.35M and 4.1.191.24M are 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 4.1.192.35M 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 19](#) 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 4.1.192.35M 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 4.1.192.35M 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 15 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 4.1.192.35M 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](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**.
- 

## Documentation Updates

This section provides configuration details for the software features introduced in release 4.1.192.35M.

## Configuring Interoperability with the Series 3200 Mobile Access Router

### Configuration Guidelines

For the 1522 or 1524 mesh access point and Cisco MAR 3200 to interoperate on the public safety network, the following configuration guidelines must be met:

- Client access must be enabled on the backhaul (Mesh global parameter).
- Public Safety must be enabled globally on all mesh access points (MAPs) in the mesh network.
- Channel number assignment on the 1522 or 1524 must match those on the Cisco 3200 radio interfaces.
  - Channels 20 (4950 GHz) through 26 (4980 GHz) and sub-band channels 1-19 (5 and 10 MHz) are used for MAR interoperability. This configuration change is made on the controller. No changes are made to the access point configuration.
  - Channel assignments are only made to the RAP. Updates to the MAP are propagated by the RAP.
  - To ensure interoperability between mesh access points 1510 and 1522, channels 190 and 196 are used for the backhaul.

The default channel width for MAR 3200s is 5 MHz. You must *either* change the channel width to 10 or 20-MHz to enable WGBs to associate with series 1520 mesh access points *or* change the channel on the 1522 or 1524 to a channel in the 5-MHz (channels 1 to 10) or 10-MHz band (channels 11 to 19).

- Radio (802.11a) must be disabled when configuring channels and then reenabled when using the CLI.
  - When using the GUI, enabling and disabling of the 802.11a radio for channel configuration is not required.
- Cisco MAR 3200s can scan channels *within* but not across the 5, 10 or 20-MHz bands.

## Using the GUI to Enable 1522 and 1524 to Associate with Cisco 3200

Follow these steps to enable 1522 and 1524 to associate with Cisco 3200.

- Step 1** To enable the backhaul for client access, click **Wireless > Mesh** to access the Mesh page.
- Step 2** Check the Backhaul Client Access **Enabled** check box to allow wireless client association over the 802.11a radio. Click **Apply**.



**Note** You are prompted with a message to allow reboot of all the mesh access points to enable Backhaul Client Access on a network. Click **OK**.

- Step 3** To assign the channel to use for the backhaul (channels 20 through 26), click **Wireless > Access Points > Radio** and select **802.11a/n** from the Radio sub-heading. A summary page for all 802.11a radios displays.
- Step 4** At the Antenna drop-down menu for the appropriate RAP, select **Configure**. The page seen in [Figure 2](#) displays.

**Figure 2** *Wireless > Access Points > Radio > 802.11 a/n > Configure Window*

The screenshot shows the Cisco Wireless GUI configuration window for the radio **balar1520Cable 802.11 a/n (4.9GHz)**. The window is divided into several sections:

- General:** AP Name: balar1520Cable, Admin Status: **Disable**, Operational Status: DOWN.
- RF Channel Assignment:** Current Channel: 1, Channel Selection: **20**.
- 11n Parameters:** 11n Supported: No.
- Antenna:** Antenna Type: External, Antenna Gain: 0 x 0.5 dBi.
- Management Frame Protection:** Version Supported: 1, Protection Capability: All Frames, Validation Capability: All Frames.
- WLAN Override:** (Empty section)
- Tx Power Level Assignment:** Current Tx Power Level: 1, Tx Power Level Selection: **1**.
- Performance Profile:** View and edit Performance Profile for this AP. **Performance Profile** button.

A note at the bottom right states: **\*\* Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity some clients.**

- Step 5** At the RF Backhaul Channel Assignment section, select the **Custom** option for the Assignment Method option and select any channel between 1 and 26.
- Step 6** Click **Apply** to commit your changes.
- Step 7** Click **Save Configuration** to save your changes.

## Using the CLI to Enable 1522 and 1524 Association with Cisco 3200

Follow these steps to enable 1522 or 1524 to associate with Cisco 3200.

**Step 1** To enable client access mode on the 1522 and 1524, enter this command:

```
config mesh client-access enable
```

**Step 2** To enable the public safety on a global basis, enter this command:

```
config mesh public-safety enable all
```

**Step 3** To enable the public safety channels, enter these commands:

a. On the 1522, enter these commands:

```
config 802.11a disable Cisco_MAP
```

```
config 802.11a channel ap Cisco_MAP channel number
```

```
config 802.11a enable Cisco_MAP
```

b. On the 1524, enter these commands:

```
config 802.11-a49 disable Cisco_MAP
```

```
config 802.11-a49 channel ap Cisco_MAP channel number
```

```
config 802.11-a49 enable Cisco_MAP
```



**Note** Enter **config 802.11-a58 enable Cisco\_MAP** to enable a 5.8-GHz radio.



**Note** For both the 1522 and 1524, *channel number* is equal to any value 1 to 26.

**Step 4** To save your changes, enter this command:

```
save config
```

**Step 5** To verify your configuration, enter these commands:

```
show mesh public-safety
```

```
show mesh client-access
```

```
show ap config 802.11a summary (1522 only)
```

```
show ap config 802.11-a49 summary (1524 only)
```



**Note** Enter **show config 802.11-a58 summary** to display configuration details for a 5.8-GHz radio.

# Caveats

This section lists open, resolved and closed caveats in release 4.1.192.35M.

## 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**.

- 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.

- CSCsj48049—The Custom options for the TX Power Level Assignment parameter (Configure > Access Point > *Radio*) in Cisco WCS do not 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\_MAP**) 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.

- 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.

- CSCsk35348—The packet error rate (PER) displayed for backhaul links in Cisco WCS is not correct.

**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.

- 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 was run (Reports > Mesh Reports) no values were reported in the first time seen and last time seen columns for those access points identified as "none 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 with 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.

- 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 = 0xffffffffc

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

**Workaround:** None. No system impact.

- 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.

- CSCsm44951—The **show country channel** command does not display the 4.9-GHz channel for the 1524 mesh access point although it is supported. It only lists the 5-8-GHz channels.

**Workaround:** None. It is not service affecting. The 4.9-GHz channel is operating and the mesh access point is able to join the controller.

- 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.

- CSCsm62772—A controller running 4.1.190.5 or 4.1.191.24M software might crash unexpectedly due to an SNMPTask.

**Workaround:** None.

- CSCsm73147—When a configured country code does not support the 5-GHz band (802.11a), an UP condition for both the 2.4Ghz and 5Ghz radio of a 1510 mistakenly displays. As an unsupported band, no data should display for the 5-GHz band and MAPs cannot join the RAP via that band.

**Workaround:** None.

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

**Workaround:** Configure WPAv2+AES.

- CSCsm84194—A mesh access point might restart discovery while downloading an image. When this occurs the mesh access point might require a number of retries before it successfully joins the controller.

**Workaround:** None. Recovery is automatic, mesh access point joins after retries without user intervention.

- CSCsm90114—In some cases, when RRM is enabled and a mesh access point radio goes off channel frequently (every 30 to 60 seconds), clients are not being notified and the clients transmission queue is not being reserved, so the client disconnects from the mesh access point.

**Workaround:** Increase the load and neighbor timers to 3600 seconds.

- CSCsm90785—The WiSM only supports up to 300 mesh access points reliably.

**Workaround:** Do not allow more than 300 mesh access points to associate with a WiSM.



- CSCsm92850—In some cases, running a link test between a MAP and a RAP might fail if run on a heavily utilized link. Additionally, mesh access points on that link might disconnect as a result.

**Workaround:** Decrease the packets per seconds parameter for the link test to reduce the number of packets being transmitted on the link.

- CSCso07544—When mesh access points are on the same layer 2 VLAN with autonomous access points, clients associated with mesh access points cannot ping or access network resources. Additionally, pings from the controller to the client often fail or intermittently return a third of the ping requests; and pings from the controller to mesh access points often fail as well. If you enter the **show mesh table** command from the mesh access point, the display indicates that the MAC addresses of clients associated with autonomous access points flip-flop.

**Workaround:** Configure mesh access points on different layer 2 VLANs than autonomous access points.

- 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.

**Workaround:** None.

- CSCso21425—A GUI and CLI message warning users not to select 'global' as the backhaul setting is missing in release 4.1.192.35M. This message was present in 4.1.191.24M. The same warning applies even though it is not shown in the current release. Configuring the 'global' setting on a backhaul setting often causes unpredictable behavior and might cause network issues with the mesh access points.

**Workaround:** Do not configure the 'global' setting on mesh access point backhauls using the CLI and GUI.

- CSCso21445—Manually rebooting radios on mesh access point as well as some configuration changes initiated from the controller might mistakenly generate power loss traps.

**Workaround:** None.

- CSCso93562—When an antenna on a 1240 mesh access point is enabled as *Right Primary* and then antennas are installed, a subsequent change in the antenna configuration from *Right Primary* to *Diversity* is not accepted by the 802.11a radio.

**Workaround:** Change the value of the antenna gain value to a different value (from X to Y) and apply the configuration. The antenna configuration will change from *Right Primary* to *Diversity*.

- CSCsu93322—When an WMIC, configured as a workgroup bridge (WGB) in a Cisco 3200 series MAR, encounters a session-timeout, it might not be able to reassociate to a mesh access point. This condition occurs when MFP is configured using WPA2 key management with TKIP encryption. A symptom of the issue is a steady stream of Deauth frames being sent from the mesh access point to the WGB.

**Workaround:** Disable MFP on the mesh access point and/or the WGB and/or use AES rather than TKIP.

- CSCsu96326—All mesh 152x access points that join a controller might suddenly disconnect when the WCS map (release 5.1.64.0) is saved.

**Workaround:** Configure the antenna gain in WCS after initial placement of the mesh access point on the WCS map. Additionally, verify that the antenna gain entered in WCS and the controller are set to the same value to prevent reboot of the mesh access points.

## Resolved Caveats

The following caveats are resolved in 4.1.192.35M.

- CSCsj48872—In some cases, the wireless LAN controllers on a WiSM blade crashed and rebooted after a software upgrade from version 4.0.206.0 to version 4.1.171.0.
- CSCsk41360—In some cases, a workgroup bridge looped when it attempted to authenticate using the controller and EAP-TLS (802.1x). The workaround required adjusting the EAP timers on the controller using the **config advanced eap...** command.
- CSCsm16872, CSCsu52762—Viewing the access point detail window from the controller GUI caused the GUI to freeze and the controller to reboot. No crash file was created.
- CSCsm30850—In some circumstances, when an Atheros client tried to connect to a mesh access point, the controller crashed.
- CSCso00294—In some cases, a mesh access point would not go back to its configured static IP address after a fallback to DHCP mode. The static link was not restored until the mesh access point rebooted after multiple attempts to connect. The workaround was to always have a DHCP server installed in the network to support mesh access points.
- CSCsq25270— When querying a Catalyst 3750 switch with an integral controller module, the **show cdp neighbor** command does not display any information for 1522 and 1524 mesh access points.
- CSCsq50779—In rare circumstances, the 802.11b/g radio firmware on an 1522 mesh access point would lockup.
- CSCsq51903—A spanning tree loop occurred when a RAP had both a wireless (failover mode, over-the-air connection) and wired Ethernet connection to a layer 2 network.

The incorrect configuration occurred when the Ethernet port connecting the RAP to the network was disabled by the customer causing the RAP to connect over-the-air to the controller through a neighbor sector. When the RAP Ethernet connection was reestablished by enabling the Ethernet port on the switch, a layer 2 loop was created. This scenario only occurred on RAPs because only RAPs have an Ethernet connection to a backend switch which can result in the loop.

Moving the backend network to layer 3 was recommended for all customers with large networks.

- CSCsq64862— Wired clients behind a non-root MAP could not communicate with a GLBP or HSRP router via a mesh bridge link. Changes were made in the software to make the default multicast mode *in-out* to eliminate this communication problem. The workaround in the previous release involved changing the multicast mode setting to *in-out* using the **config mesh multicast in-out** command.
- CSCsq82061—A subordinate SNMP task failure caused SNMP to crash on the controller.
- CSCsq99212— ACKs for the 1252 were sent with the wrong preamble length for 802.11b rates (2, 5.5 and 11 Mb/s) 2, 5.5 and 11Mb/s. For some clients, throughput was slowed down.
- CSCsr01267—In some cases, mesh access points falsely detected radar on all 802.11 radio channels despite the absence of radar on those channels.
- CSCsr15074— A root access point (RAP) did not forward multicast packets into the mesh network when ethernet bridging was disabled (off). The resolution was to enable Ethernet bridging on RAPs using the **config ap bridging enable Cisco\_AP** command. Ethernet bridging must be enabled to support multicast traffic within a mesh network.
- CSCsr25044— In some cases, a mesh access points stopped communicating on Ethernet although beacons were still generated on the radio. The console port was rendered dead and access lost. Rebooting the mesh access point restored Ethernet communication and console access.

- CSCsr89403–The RX antenna diversity was not enabled on the 2.4GHz access radio. Adjustments to the initialization software were done to ensure all receive antennas would enable.
- CSCsr92067–A controller running 4.1.185.0 (non-mesh code) rebooted unexpectedly when operating in the same RF group as a controller running mesh code 4.1.192.22M. The mesh controller was elected as the RF group leader and caused the non-mesh controller to crash. Crashes only occurred after the controller with mesh code was deployed in the network.
- CSCsr96003– When you had a remote Telnet session to a 1522 mesh access point, the following debug commands did not send any output to the console or syslog destinations: **debug mesh forwarding**, **debug dot11 d1 trace print txfail**, **debug dot11 d0 trace print txfail**, and **debug dot11 d0 trace print clients**.
- CSCsu22727– In some cases, a controller crash occurred while pushing an AP template from WCS.
- CSCsu86874–A refresh of the controller GUI when running a link test for mesh access points often caused a crash of the controller task.

The following caveats were resolved in 4.1.192.22M.

- CSCsg44445–The **show ap config {802.11a| 802.11b} Cisco\_AP** command displayed incorrect power level values for the 1510; however, the power levels in use by the 1510 were correct.
- 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.
- CSCsh94313–When special characters were used in a bridge group name (BGN) for a RAP, MAPs were not able to associate with RAP using the default BGN. All bridge group names are now checked against an allowed character set.
- CSCsi74181–Ethernet clients that were connected to Ethernet ports of different 1500 series MAPs, that did not share the same mesh path to the controller and that did not have a RAP as a parent, did not have connectivity to each other. The workaround was to move MAPs so that each was directly connected to a RAPs or had the same mesh path.
- 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 have been handled properly by the 1510. As a result, the channel change on the RAP might not have propagated to the 1510 children mesh node. However, the channel change management frame was correctly handled between and among the 1520, 1240 and 1130 mesh access points. Additionally, channel change management between and among 1510s was handled correctly.
- CSCsk37948–In Cisco WCS, the Mesh Links Stats Report (Reports-> Mesh reports > Mesh Link Stats) did not display time without AM or PM.
- CSCsk41197–A message (MAXAAA\_FAILURE\_ON\_MOBILE) mistakenly reported failed external authentication when no AAA servers were configured on the controller and local authentication was in use by the 1510.
- CSCsk49160–In Cisco WCS, the word “association” is misspelled in the excessive association trap event when viewed on the alarms (Monitor > Alarms) window.
- CSCsk93571–The Global Tx Power Level setting is not a supported function on 802.11a backhauls for mesh access points by design. However, changing from the custom to global TX setting was allowed by the controller GUI and caused the controller to crash upon reboot. The problem was resolved by removing the global configuration option for mesh access points.

- CSCsl01648—If a 1520 was configured with channels or antenna gain combinations that were outside the permitted values for a particular domain, the RAP might have joined the controller, however, the channel or antenna gain values could not be changed. MAPs configured with incorrect channels or antenna gain combinations were not able to join the controller.

The workaround was to verify antenna and channel settings permitted in a regulatory domain before configuring the mesh access point. Users were cautioned not to configure channel and antenna gains outside the permitted values.

- CSCsl21116—The **show ap summary** command did not display the correct Ethernet MAC address for the 1520s.
- CSCsl22083—When Admin is in a disabled state on the 1510, the 1510 will crash after 30 minutes. The workaround was not to set the 1510 to an Admin Disabled state.
- CSCsl24620, CSCsl73295—In some circumstances a 1520 would attempt simultaneous authorization with the controller via two different parents, if a better parent was located during its authorization process. The parent access points would initially be blacklisted by the child after a failed authorization but the child would re initiate a search for a parent and join.
- CSCsl39876—In rare circumstances, a RAP that lost its wired connection to the controller and had reconnected to the controller, over the air through a nearby parent mesh AP, might have required multiple scans or exceeded the lonely timer and reboot before it reconnected to a wired connection. As designed, a RAP scans for wired connections every 15 minutes until the lonely timer expires at 40 minutes and initiates a reboot of the access point.
- 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.

The workaround was to run the link test from the controller GUI which had a default PPS setting of 100 PPS.

- CSCsl70218—The BOOT bootloader environment variable was not set on some early shipments of 1520 mesh access points. Any image download that failed during upgrade could cause a partial image to be written on the 1520. Without the BOOT variable, the bootloader could attempt to boot the partial image rather than the original complete image, causing the 1520 to get stuck and not join the controller.

This was seen when a controller was upgraded from mesh release 4.1.190.5 to 4.1.191.24M and the 1522 had a wireless connection to the controller. The workaround to recover from an incomplete 1520 boot up due to a 4.1.190.5 to 4.1.191.24M upgrade, involved entering 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
```

- CSCsl90654—In rare circumstances, when background scanning was enabled, a transmit queue for a RAP would lock up causing its MAPs to attempt to connect to other access points. This resulted in a sub-optimal topological formation.

- CSCsl91623—When 802.11b only radio policy was configured on a WLAN and only 1510 mesh access points were on the network, the following message would often appear in the message log:  

```
apf_spam.c:930 APF-1-NOT_ADV_SSID_ON_AP: Not advertising SSID <ssid> on AP
00:0b:85:xx:xx:xx due to radio policy
```

This message was generated because the radio policy of the WLAN was not applied to the 802.11a radio. However, it was not service affecting because 1510s by design do not advertise the WLAN on its 802.11a radio as it is for backhaul use only and does not support clients.
- CSCsl91679—RAPs retained information on connections (adjacencies) to MAPs even when the connection was no longer valid. A reboot of the RAP was necessary to clear the adjacency information. A new debug command was added to remove MAP adjacencies without a reboot of the RAP (**debug adj\_deladj adjacency**).
- CSCsm25938—When using the South Africa code (ZA), the RAP was not able to see any MAPs. The access point 802.11 radio was seen as enabled by the controller but querying the access point directly showed that the interface was disabled but in fact the radio was disabled. The workaround was not to use the ZA code.
- CSCsm76803—A 1522 mesh access point mistakenly sent the Ethernet address (GigEthernet2) rather than the bridged virtual interface (BVI). The Ethernet address was used as the source Ethernet address for all ARP packets and non-broadcast IP packets which was not correct. This caused users to use multiple MAC addresses. Additionally, CDP was enabled on the GigEthernet2 cable modem Ethernet interface which was not required.
- CSCso44015—In some cases, a 1522 or 1524 mesh access point radio receiver would sporadically get into a *hung* state and would stop receiving frames. The 1522 was unable to communicate over the radio interface. The workaround was to reset (soft or hard) the mesh access point.
- CSCso45207—In some cases, a 1522 or 1524 mesh access point would get in a *lockup* state at startup after a soft reset. All interfaces were down and the console interface was non-functional. An *AVR 2 interface error* was often seen at startup; however, no further symptoms were seen once the MAP was up and running. This *lockup* state only occurred at startup, following a soft reset. The workaround was to power-cycle the access point.

## 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.

- 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.

## 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](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 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*
- *Getting Started Guide: Cisco Aironet 1520 Series Outdoor Mesh Access Points*
- *Cisco Aironet 1520 Series Outdoor Mesh Access Point Mounting Instructions*
- *Cisco Aironet 1520 Series Outdoor Mesh Access Point Power Injector Installation Instructions*
- *AC Power Cords for Cisco Aironet 1520 Series Outdoor Mesh Access Points*
- *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 5.0*
- *Cisco Wireless Control System Configuration Guide, Release 5.0*
- *Cisco 3200 Series Mobile Access Router Software Configuration Guide*
- *Troubleshooting a Mesh Network*



### Note

You can view the latest online versions of these mesh documents at:

[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)

**Note**

You can find the MAR configuration guide and related documentation at:

[http://www.cisco.com/en/US/products/hw/routers/ps272/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/routers/ps272/products_installation_and_configuration_guides_list.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.