Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.181.0

July 23, 2007

These release notes describe open and resolved caveats for software release 4.1.181.0 for Cisco 2000, 2100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 (1505 and 1510) Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

Note Unless otherwise noted, all of the Cisco wireless LAN controllers are hereafter referred to as *controllers*, and all of the Cisco lightweight access points are hereafter referred to as *access points*.

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

- Software release 4.1.181.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 2.01
- Cisco Wireless Control System (WCS) software release 4.1.91.0
- Cisco Wireless Control System (WCS) Navigator 1.0.91.0
- Location appliance software release 3.0.42.0
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 (1505 and 1510) Series Lightweight Access Points

Special Notice for Mesh Networks

Note Controller software release 4.1.181.0 does not support the new Cisco Aironet 1520 Series Mesh Access Point. If you intend to use this new access point, you must run controller software release 4.1.19x.y, which supports only mesh access points. If your network contains 1520 mesh access points and Cisco non-mesh access points (such as 1240 series access points), you need to manage your 1520 mesh access points with one controller and your non-mesh access points with a second controller. If you have 1505 and/or 1510 mesh access points, you should connect them to the same controller as the 1520 mesh access points.

Note Cisco WCS software release 4.1.91.0 manages controllers running software release 4.1.181.0 or 4.1.19x.y. You do not need a separate instance of WCS to manage each controller.

Controller Requirements

The controller graphical user interface (GUI) requires the following operating system and web browser:

- Windows XP SP1 or higher or Windows 2000 SP4 or higher
- Internet Explorer 6.0 SP1 or higher

Note Internet Explorer 6.0 SP1 or higher is the only browser supported for accessing the controller GUI and for using web authentication.

Software Release Information

Software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point joins a controller. As new releases become available for the controllers and their access points, consider upgrading.

Note The Cisco WiSM requires software release SWISMK9-32 or later. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software release 3.2.78.4 or later, and the Supervisor 720 12.2(18)SXF5 (Cisco IOS Software Modularity) supports the Cisco WiSM software release 4.0.155.5 (with Cisco IOS Software Modularity).

Note The Cisco WiSM is only supported on Cisco 7609 and 7613 Series Routers running Cisco IOS Release 12.2(18)SXF9 or later.

Note The Cisco Wireless LAN Controller Network Module-Enhanced (WLCM-E) is supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2 or later.

Note To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2.25.FZ or 12.2(25)SEE.

Finding the Software Release

To find the software release running on your controller, look on the Monitor > Summary page of the controller GUI or enter **show sysinfo** on the controller command line interface (CLI).

Upgrading to a New Software Release

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 LEDs 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. However, with the increased number of concurrent access point upgrades supported in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Special Rules for Upgrading to Controller Software Release 4.1.181.0

Caution Before upgrading your controller to software release 4.1.181.0, you must comply with the following rules.

- Controller software release 4.1.181.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the WCS. If you attempt to download the 4.1.181.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
- If your controller is running software release 3.2.195.10 (or a later 3.2 release) or 4.0.206.0 (or a later 4.0 release), you can upgrade your controller directly to software release 4.1.181.0. If your controller is running an earlier 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 4.1.181.0. Table 1 shows the upgrade path that you must follow before downloading software release 4.1.181.0.

Table 1 Upgrade Path to Controller Software Release 4.1.181.0

Current Software Release	Upgrade Path to 4.1.181.0 Software
3.2.78.0	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.1.181.0.
3.2.116.21	
3.2.150.10	
3.2.171.6	
3.2.193.5	If your controller is configured with the new J3 country code, upgrade to 3.2.195.10 (or a later 3.2 release). If your controller is not configured for the new J3 country code, you can upgrade to 3.2.195.10 (or a later 3.2 release) or to 4.0.206.0 (or a later 4.0 release).
3.2.195.10 or later 3.2 release	You can upgrade directly to 4.1.181.0.
4.0.155.5	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.1.181.0.
4.0.179.11	
4.0.206.0 or later 4.0 release	You can upgrade directly to 4.1.181.0.
4.1.171.0	You can upgrade directly to 4.1.181.0.

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 4.1.181.0 software. In large networks, it can take some time to download the software on each access point.

- Cisco recommends that you also install the Cisco Unified Wireless Network Controller Boot Software 4.1.181.0 ER.aes file on the 2106 controller. This file resolves bootloader defects and is necessary to ensure proper operation of the controller. The ER.aes file is required for only the 2106 controller.

Note The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (4.1.181.0 ER.aes) ensures that the bootloader modifications in all of the previous and current boot software ER.aes files are installed.

Caution If you require a downgrade from one release to another, you may lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

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

Step 1 Upload your controller configuration files to a server to back them up.

Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Disable the controller 802.11a and 802.11b/g networks.

Step 3 Disable any WLANs on the controller.

Step 4 Follow these steps to obtain the 4.1.181.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 4.1.181.0 ER.aes file from the Software Center on Cisco.com:

a. Click this URL to go to the Software Center:

   http://www.cisco.com/cisco/software/navigator.html

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers**, **Wireless Integrated Routers**, or **Wireless Integrated Switches**.

e. Click the name of a controller.

f. Click **Wireless LAN Controller Software**.

g. Click a controller software release.

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

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 remaining file (either the 4.1.181.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.1.181.0 ER.aes file).

Step 5 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 4.1.181.0 ER.aes file to the default directory on your TFTP server.

Step 6 Click **Commands** > **Download File** to open the Download File to Controller page.

Step 7 From the File Type drop-down box, choose **Code**.

Step 8 In the IP Address field, enter the IP address of the TFTP server.

Step 9 The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. 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 10 In the File Path field, enter the directory path of the software.

Step 11 In the File Name field, enter the name of the software file (*filename*.aes).

Step 12 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 13 Repeat Step 6 to Step 12 to install the remaining file (either the 4.1.181.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.1.181.0 ER.aes file).

Step 14 After the download is complete, click **Reboot**.

Step 15 If prompted to save your changes, click **Save and Reboot**.

Step 16 Click **OK** to confirm your decision to reboot the controller.

Step 17 After the controller reboots, re-enable the WLANs.

Step 18 Re-enable your 802.11a and 802.11b/g networks.

Step 19 If desired, reload your latest configuration file to the controller.

Step 20 To verify that the 4.1.181.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Note You cannot verify the boot software version on the 2106 controller. The Bootloader Version field remains at 4.0.190.0 for the 2106 controller, so you cannot tell which ER.aes file is installed.

New and Changed Information

The following new features and changed information are included in controller software release 4.1.181.0.

RRM Features and Changed Information

These radio resource management (RRM) features have been added to controller software release 4.1.181.0.

New DCA CLI Commands

These new CLI commands have been added to configure the dynamic channel allocation (DCA) algorithm:

- To control the DCA sensitivity with respect to changes in the environment, enter this command:

  config advanced {**802.11a** | **802.11b**} **channel dca sensitivity** {**low** | **medium** | **high**}

  The DCA algorithm determines whether to make a channel change based on how much better a new channel would be for the radio with the worst DCA metric in the radio band. The DCA metric is comprised of noise, interference, channel load, and overlapping neighbors (other radios on the same channel). Previously, a channel change would occur if another channel was 5 dBm better than the current channel of the radio with the worst DCA metric. This new command allows you to control how sensitive the DCA algorithm is to environmental changes, such as signal, load, noise, and interference, when determining whether to change channels. Table 2 shows the three available DCA sensitivity levels.

Table 2 DCA Sensitivity Levels

DCA Sensitivity Level	Description	2.4-GHz DCA Sensitivity Threshold (dB)	5-GHz DCA Sensitivity Threshold (dB)
High	High sensitivity to environmental changes	5	5
Medium (default)	Moderate sensitivity to environmental changes	15	20
Low	Low sensitivity to environmental changes	30	35

  For example, if the radio with the worst DCA metric in the 2.4-GHz band has a metric of –60 dBm on its current channel and the DCA algorithm finds that the metric would be –80 dBm on another channel (which is an improvement of 20 dBm), the DCA algorithm would change the channel if the DCA sensitivity is set to high or medium. It would not change the channel if the sensitivity is set to low.

- To define the time when DCA starts, enter this command:

  config advanced {**802.11a** | **802.11b**} **channel dca anchor-time** *hour*

  where *hour* is an hour in the day from 0 to 23 (12:00 a.m. to 11:00 p.m.).

- Previously, the DCA algorithm ran every 10 minutes. To now define how often DCA runs, enter this command:

  config advanced {**802.11a** | **802.11b**} **channel dca interval** *value*

  where *value* is 0, 1, 2, 3, 4, 6, 8, 12, or 24. 0 equals 10 minutes and is the default value. The rest of the values represent hours. So if you specify a value of 8, DCA would run every 8 hours.

  For example, if you specify an anchor time of 0 and a DCA interval of 12, the DCA algorithm would run at 12:00 a.m. and 12:00 p.m. every day.

Note You can view the configured DCA sensitivity, anchor-time, and interval on the 802.11a (or 802.11b/g) Global Parameters > Auto RF page on the controller GUI. However, you can configure these values only from the controller CLI.

Note When the controller reboots, the DCA algorithm runs every 10 minutes for the first 100 minutes, regardless of how the anchor-time and interval parameters are configured. This initial startup phase enables the DCA algorithm to converge to a reliable channel before the scheduled operation occurs. After the first 100 minutes, the DCA algorithm runs at only the scheduled times.

- To enable debugging for the DCA algorithm's channel change, enter this command:

  debug airewave-director channel

  This command provides the previous channel, the 802.11 interference energy (both the previous and current values in dBm), the noise energy (both the previous and current values in dBm), and the reason why the channel was changed. Possible reasons include:

  - 0 = Other (could occur as a result of a manual channel change or for other reasons)
  - 1 = Signal (could occur if another access point moved on and off the radio's current channel)
  - 2 = Noise
  - 4 = 802.11 interference
  - 6 = Noise and 802.11 interference

Note You can see the reason why the DCA algorithm changed channels by clicking **Monitor** and then **View All** under Most Recent Traps on the controller GUI. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

RRM Changes

These changes in RRM functionality have been added to controller software release 4.1.181.0.

- The default value for the transmit power control threshold has been changed from –65 dBm to –70 dBm.
- The default setting for aggressive load-balancing has been changed to disabled, and the default value for the *clients* parameter in the **config load-balancing window** *clients* CLI command has been changed to 5.

Mesh Features and Changed Information

These mesh features have been added to controller software release 4.1.181.0.

Mesh Multicast for Video

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts. 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. This is the default mode.
- **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 Ethernets, 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.

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**}

AP1510 Interoperability with Cisco 3200 MAR in Public-Safety Networks

You can configure the Cisco AP1510 to interoperate with the Cisco 3200 Series Wireless Mobile Access Router (MAR) on the public-safety channel (4.9 GHz) to integrate data collected from in-vehicle deployments such as police cars into the overall wireless infrastructure. Follow these guidelines for the AP1510 and Cisco 3200 MAR to interoperate on the public-safety network:

- The Cisco 3200 MAR must run Cisco IOS Software Release 12.3(2)JK3, and the AP1510 must run controller software release 4.1.181.0.
- Client access must be enabled on the backhaul to use the 4.9-GHz band for client traffic.
- Public safety must be enabled globally on all MAPs in the mesh network.
- When using the CLI, the 802.11a radio must be disabled before configuring channels and then re-enabled.
- The channel number assignment on the AP1510 and Cisco 3200 MAR radio interfaces must match.
  - Channels 20 (4950 MHz) and 26 (4980 MHz) are used for client access. This configuration change is made on the controller. No changes are made to the access point configuration.
  - Channel assignments are made only to the RAP. Updates to the MAP are propagated by the RAP.
  - To ensure backward compatibility with controller software releases 4.0 and 4.1.171.0, channels 190 and 196 are still used for the backhaul and client access.

Using the GUI to Enable AP1510 Association with the Cisco 3200 MAR

Follow these steps to enable the AP1510 to associate with the Cisco 3200 MAR using the GUI.

Step 1 Click **Wireless > Mesh** to access the Mesh page.

Step 2 Check the **Backhaul Client Access** check box to allow wireless client association over the 802.11a radio and click **Apply**.

Step 3 When you are prompted to allow a reboot of all mesh access points in order to enable backhaul client access, click **OK**.

Step 4 On the controller CLI, enter this command to enable public-safety:

config mesh public-safety enable all

Step 5 On the controller GUI, click **Wireless > Access Points > Radios > 802.11a/n**. The 802.11a/n Radios page appears.

Step 6 Hover your cursor over the blue drop-down arrow for the desired RAP and choose **Configure**. The 802.11a/n Cisco APs > Configure page appears.

Step 7 Under RF Backhaul Channel Assignment, choose **Custom** for the Assignment Method and either channel **20** or **26** from the Custom drop-down menu.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Using the CLI to Enable AP1510 Association with the Cisco 3200 MAR

Follow these steps to enable the AP1510 to associate with the Cisco 3200 MAR using the CLI.

Step 1 To enable client access mode on the AP1510, enter this command:

config mesh client-access enable

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

config mesh public-safety enable all

Step 3 To choose the public-safety channels, enter these commands:

config 802.11a disable *Cisco_RAP*

config 802.11a channel ap *Cisco_RAP* {**20** | **26**}

config 802.11a enable *Cisco_RAP*

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

Transmit Power Levels for 1500 Series Access Points

In controller software release 4.1.181.0, power levels for the AP1505 and AP1510 are reported as either Tx Power Level 1 or Tx Power Level 2. Previously, only a maximum transmission power (Max Tx Power) was reported.

- Tx Power Level 1 = The maximum power level that exists across all of the data rates
- Tx Power Level 2 = Tx Power Level 1 minus 3 dBm

Note The CLI command summary displays the dBm value for power levels 1 and 2, but this reading is not available on the controller GUI.

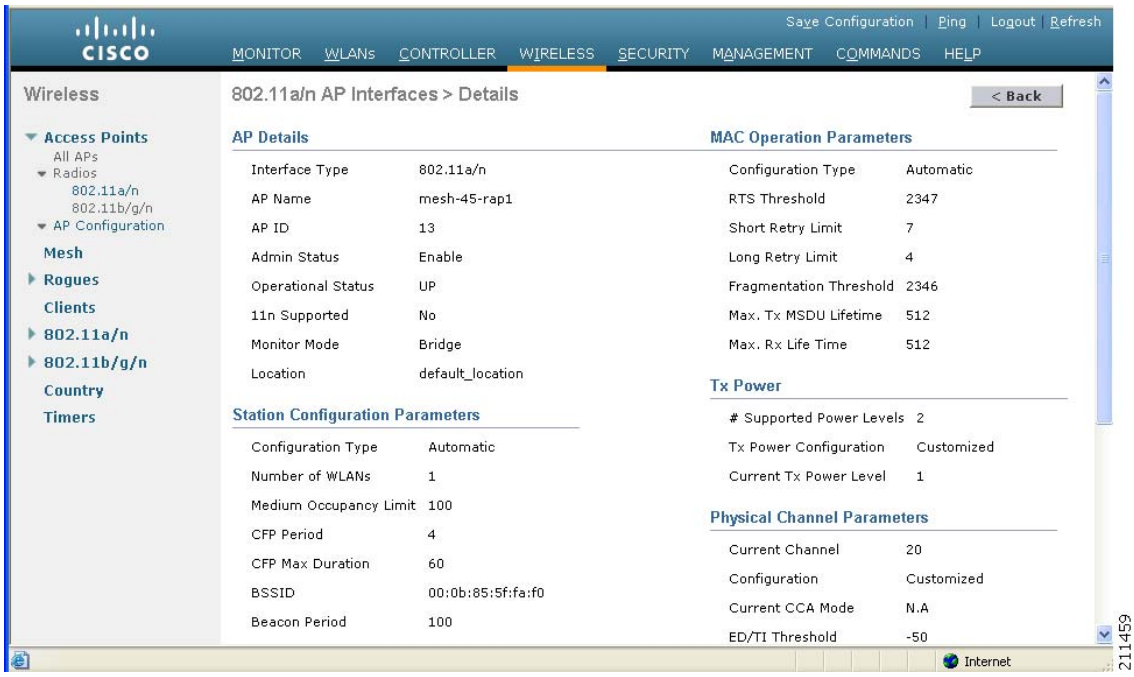
Using the GUI to View Transmit Power Levels for 1500 Series Access Points

Follow these steps to view transmit power levels for an AP1505 or AP1510 using the GUI.

Step 1 Click **Wireless > Access Points > Radios > 802.11a/n** or **802.11b/g/n** to access the 802.11a/n (or 802.11b/g/n) Radios page.

Step 2 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Detail**. The 802.11a/n (or 802.11b/g/n) AP Interfaces > Details page appears (see Figure 1).

Figure 1 802.11a/n AP Interfaces > Details Page



This page shows the current transmit power level under the "Tx Power" section.

Using the CLI to View Transmit Power Levels for 1500 Series Access Points

To view transmit power levels for an AP1505 or AP1510 using the CLI, enter these commands:

show ap config 802.11a *Cisco_AP*

show ap config 802.11b *Cisco_AP*

Note The **show ap config 802.11a** *Cisco_AP* command is not applicable to the AP1505 because it has only one radio, the 802.11b/g/n.

Information similar to the following appears:

```
show ap config 802.11a mesh-RAP-45
Tx Power
      Num Of Supported Power Levels ............. 2
      Tx Power Level 1 ........................... 26 dBm
      Tx Power Level 2 ........................... 23 dBm
      Tx Power Configuration ..................... CUSTOMIZED
      Current Tx Power Level ..................... 2
show ap config 802.11b mesh-RAP-45
Tx Power
      Num Of Supported Power Levels ............. 2
      Tx Power Level 1 ........................... 24 dBm
      Tx Power Level 2 ........................... 21 dBm
      Tx Power Configuration ..................... AUTOMATIC
      Current Tx Power Level ..................... 1
```

LED Verification on 1500 Series Access Points

You can attach an LED indicator to the Power over Ethernet (PoE) connector of AC-powered Cisco Aironet 1505 and 1510 Access Points to verify that power is on. A steady green color indicates that the access point is receiving power and that LWAPP is connected and ready to serve clients. You might notice a blinking green light between the initial and final steady green light as the LED confirms LWAPP connectivity.

Note 1500 series access points with a serial number of WCN10160121 or greater support the use of the LED indicator.

Note Do not install the LED indicator if the access point has an Ethernet connection to the network.

For details about installing the LED indicator, see the *Cisco Aironet Series 1500 Access Point LED Indicator Installation Instructions* at this URL:

http://www.ciscosystems.uz/en/US/docs/wireless/access_point/1500/installation/guide/LED1500.html

Mesh Changes

These changes in mesh functionality have been added to controller software release 4.1.181.0.

- The ability to enable or disable the MAC filter list has been removed from both the controller GUI and CLI.
- Because controller software release 4.1 does not support an external AAA server for mesh access points, local authentication and RADIUS server support should always be enabled. Therefore, the following CLI commands are no longer supported:

  config mesh local-auth disable

  config mesh radius-server

- The **show mesh env** {**summary** | *Cisco_AP*} CLI command now provides battery details, including charge, power, serial number, temperature, version, and voltage. Here is a sample output:

```
AP Name     : ap:60:6b:30
AP Model    : OAP1500
AP Role     : MeshAP

Temperature: 33 C, 91 F
Heater      : OFF
Ethernet    : UP

Battery S/W version    : 01.02a

Battery Serial Number : 0638F9500006
WARNING: Replace battery
Battery Input Voltage : 120.0 V
Battery Output Voltage:  55.1 V
Battery Output Power  : 12.2 W
Battery Voltage       :  52.5 V
Battery Temperature   : 23 C 73 F
Battery Charge        : 100.000 %
```

Installation Notes

This section contains important information to keep in mind when installing controllers and access points.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Warning **Do not locate any antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing antennas, take extreme care not to come in contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, refer to national and local codes (e.g. U.S.: NFPA70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A U.S. (240vac, 10A International)**

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Warning **Do not operate your wireless network near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.**

Warning **This unit is intended for installation in restricted areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the controllers and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution but did not take adequate steps to avoid the hazard.

For your safety, and to help you achieve a good installation, read and follow these safety precautions. **They may save your life!**

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing an antenna, remember:
   a. **Do not** use a metal ladder.
   b. **Do not** work on a wet or windy day.
   c. **Do** dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**

7. If any part of an antenna system should come in contact with a power line, **do not touch it or try to remove it yourself. Call your local power company**. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

Refer to the appropriate quick start guide or hardware installation guide for instructions on installing controllers and access points.

Note To meet regulatory restrictions, all external antenna configurations must be professionally installed.

Personnel installing the controllers and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

The controller must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the controller should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Important Notes

This section describes important information about the controllers and access points.

802.11n

802.11n radios are not supported for use with controller software release 4.1.181.0. In this release, disregard any 802.11n-related parameters that appear on the controller GUI pages and any 802.11n-related controller CLI commands.

Disabling Radio Bands

The controller disables the radio bands that are not permitted by the configured country of operation (CSCsi48220).

MAC Filtering for WGB Wired Clients

Controller software release 4.1.178.0 enables you to configure a MAC-filtering IP address for a workgroup bridge (WGB) wired client to allow passive WGB wired clients, such as terminal servers or printers with static IP addresses, to be added and remain in the controller's client table while the WGB is associated to a controller in the mobility group. This feature, activated by the **config macfilter ipaddress** *MAC_address IP_address* CLI command, can be used with any passive device that does not initiate any traffic but waits for another device to start communication.

This feature allows the controller to learn the IP address of a passive WGB wired client when the WGB sends an IAPP message to the controller that contains only the WGB wired client's MAC address. Upon receiving this message from the WGB, the controller checks the local MAC filter list (or the anchor controller's MAC filter list if the WGB has roamed) for the client's MAC address. If an entry is found and it contains an IP address for the client, the controller adds the client to the controller's client table.

Note Unlike the existing MAC filtering feature for wireless clients, you are not required to enable MAC filtering on the WLAN for WGB wired clients.

Note WGB wired clients using MAC filtering do not need to obtain an IP address through DHCP to be added to the controller's client table.

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.181.0, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. Cisco recommends that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

UNII-2 Channels Disabled on New 1000 Series Access Points for United States, Canada, and Philippines

New Cisco 1000 series lightweight access points for the United States, Canada, and the Philippines do not support the UNII-2 band (5.25 to 5.35 GHz). These models are labeled AP10x0-B, where "B" represents a new regulatory domain that replaces the previous "A" domain.

FCC DFS Support on AP1130s

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on AP1130s in the United States, Canada, and the Philippines that have a new FCC ID. Access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them. AP1130s with FCC DFS support have an FCC ID *LDK102054E* sticker. AP1130s without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. AP1130s that are operating in the United States, Canada, or the Philippines; have an FCC ID *E* sticker; and are running the 4.1.171.0 software release or greater can use channels 100 through 140 in the UNII-2 band.

Access Point Radios Are Not Enabled After Upgrading to 4.1.181.0

After you upgrade the controller in the Catalyst 3750G Wireless LAN Controller Switch to software release 4.1.181.0, the access point radios are not enabled. This issue occurs because the switch is not correctly recognizing the access points through CDP and not enabling sufficient inline power for the radios. To work around this issue, uncheck the **CDP State** check box on the AP Configuration > CDP Template page on the controller GUI or enter **config ap cdp disable all** on the controller CLI.

Setting the Retransmit Timeout Value for TACACS+ Servers

Cisco recommends that the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers be increased if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and can be increased to a maximum of 30 seconds.

Configuring an Access Point's PreStandard Power Setting

An access point can be powered by a Cisco prestandard 15-watt switch with Power over Ethernet (PoE) by entering this command:

config ap power pre-standard {**enable** | **disable**} {**all** | *Cisco_AP*}

A Cisco prestandard 15-watt switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-watt switches are available:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-watt switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-watt switches listed above.

You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable to
verify sufficient in-line power. Radio slot 0 disabled.
```

Using CCKM with CB21AG Client Adapters

Cisco Aironet CB21AG client adapters support only this CCKM configuration setting: WPA + TKIP + authentication key management CCKM.

DHCP Option 60 and 1500 Series Access Points

The VCI string for DHCP option 60 on 1500 series access point changes to *Cisco AP c1500* after the access points are upgraded to controller software release 4.1.181.0.

AP1000 and Radar Detection

The AP1000 performs radar detection on channels that do not require it (such as channel 36). If the access point detects radar on these channels, the controller captures it in log messages.

Controller Functions that Require a Reboot

After you perform these functions on the controller, you must reboot the controller in order for them to take effect:

- Switch between Layer 2 and Layer 3 LWAPP mode
- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Enable or disable the mobility protocol port using this CLI command:

  config mobility secure-mode {**enable** | **disable**}

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2006 controllers: "Rx Multicast Queue is full on Controller." This message does not appear on 4400 series controllers because the 4400 NPU filters ARP packets, and all forwarding (multicast or otherwise) and multicast replication are done in the software on the 2006.

This message appears when too many multicast messages are sent to the CPU. In controller software releases prior to 5.1, multicast, CDP, and ARP packets share the same queue. However, in software releases 5.1 and later, these packets are separated into different queues. There are currently no controller commands that can be entered to determine if the multicast receive queue is full. When the queue is full, some packets are randomly discarded.

2106 Controller LEDs

The 2106 controller's Status LED and AP LED do not flash amber when software is being uploaded to the controller or downloaded to an access point, respectively.

Note Some versions of the *Cisco 2106 Wireless LAN Controller Quick Start Guide* might incorrectly state that these LEDs flash amber during a software upload or download.

Resetting the Configuration on 2006 Controllers

If you wish to reset the configuration to factory defaults on a 2006 controller, perform one of the following:

- From the controller GUI, click **Commands > Reset to Factory Default > Reset**.
- From the controller CLI (after system bootup and login), enter **clear config**. Then after the configuration has been cleared, enter **reset system** without saving the current configuration.
- From the controller console (after system bootup), enter **Recover-Config** from the User Name prompt.

Caution Do not attempt to reset the controller's configuration by choosing Option 5, Clear Config, from the boot menu.

Rate-Limiting on the Controller

Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). Cisco recommends that you always run the controller with the default **config advanced rate enable** command in effect in order to rate-limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, Cisco recommends that you reapply the **config advanced rate enable** command after testing is complete.

Pings Supported on the Controller

Controller software release 4.1.181.0 is designed to support ICMP pings to the management interface either from a wireless client or a wired host. ICMP pings to other interfaces configured on the controller are not supported.

Pinging from a Network Device to a Controller Dynamic Interface

Pinging from a network device to a controller dynamic interface may not work in some configurations. When pinging does operate successfully, the controller places Internet Control Message Protocol (ICMP) traffic in a low-priority queue, and the reply to ping is on best effort. Pinging does not pose a security threat to the network. The controller rate limits any traffic to the CPU, and flooding the controller is prevented. Clients on the WLAN associated with the interface pass traffic normally.

IPSec Not Supported

Software release 4.1.181.0 does not allow you to choose IPSec as a Layer 3 Security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 Security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 3.2.

4400 Series Controllers Do Not Forward Subnet Broadcasts through Guest Tunnel

As designed, 4400 series controllers do not forward IP subnet broadcasts from the wired network to wireless clients across the EoIP guest tunnel.

Re-enable Broadcast after Upgrading to Release 4.0.206.0

In software releases 4.0.179.0 and earlier, broadcast and multicast forwarding were both controlled with a single global flag that enabled multicast. Beginning with software release 4.0.206.0, these functions were broken into separate configuration flags: one that controls broadcast and one that controls non-broadcast multicast. If you have multicast enabled in software releases 4.0.179.0 and earlier, the broadcast flag is left disabled after upgrading to software release 4.0.206.0. As a result, some applications that rely on broadcast do not work after the upgrade.

After you upgrade to software release 4.0.206.0, use this CLI command to re-enable broadcast:

config network broadcast enable

When re-enabled, broadcast uses the multicast mode configured on the controller.

Service Modules Supported in the Catalyst 6500 Series Switch

The Catalyst 6500 Series Switch chassis can support up to five Cisco WiSMs without any other service module installed. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included).

Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.179.8 or later on the controller before connecting 1100 and 1300 series access points to the controller.

Controllers Must Run Release 3.2.116.21 or Later to Support -P Regulatory Domain

To support access points configured for use in Japan, you must upgrade the controller software to release 3.2.116.21 or later. Earlier releases do not support access points configured for use in Japan (regulatory domain -P).

Preventing Clients from Accessing the Management Network on a Controller

To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator should ensure that there is no route through which to reach the controller from the dynamic interface or use a firewall between the client dynamic interface and the management network.

Voice Wireless LAN Configuration

Cisco recommends that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, and the handset is refused at its first reassociation attempt.

Conducting a Radio Site Survey for Mesh Deployments

A radio site survey (temporary setup of mesh links) should be conducted prior to any physical installation of 1500 series mesh access points to verify that there is no interference to the radio signal path due to physical structures such as trees and buildings or equipment that may be transmitting on the same channel (co-channel interference).

For detailed information on conducting site surveys and other factors to consider when planning your network (data rate, distance between access points, interference, and so on), refer to the *Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide* at http://www.cisco.com/c/en/us/support/wireless/aironet-1500-series/tsd-products-support-series-home.html

Operating Mesh Networks through Switches and Routers

In mesh networks that operate through switches and routers, network round-trip delays between access points and the controller must be less than 100 milliseconds (ms); otherwise, timing problems may occur during wireless client authentication. Also, network path outages of 60 seconds between access points and the controller may cause the access points to lose connectivity.

Cisco 7920 Wireless IP Phone Support

When using Cisco 7920 Wireless IP Phones with controllers, make sure that the phones and controllers are configured as follows:

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The QoS Basis Service Set (QBSS) information element (IE) must be enabled. The QBSS IE enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7920 phone uses the QBSS value to determine if they should associate with another access point. Use the following commands to enable the QBSS IE:
  - **sh wlan summary**

    Note Use this command to determine the WLAN ID number of the WLAN to which you want to add QBSS support.

  - **config wlan disable** *wlan_id_number*
  - **config wlan 7920-support ap-cac-limit enable** *wlan_id_number*
  - **config wlan enable** *wlan_id_number*

- **sh wlan** *wlan_id_number*

  Note Use this command to verify that the WLAN is enabled and the Dot11-Phone Mode (7920) field is configured for compat mode.

- **save config**

- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The Cisco 7920 Wireless IP Phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

Changing the IOS LWAPP Access Point Password

Cisco IOS Lightweight Access Point Protocol (LWAPP) access points have a default password of *Cisco*, and the pre-stage configuration for LWAPP access points is disabled by default. To enable it, you must configure the access point with a new username and password when it joins the controller. Enter this command using the controller CLI to push a new username and password to the access point:

config ap username *user_id* **password** *password* {*Cisco_AP* | **all**}

- The *Cisco_AP* parameter configures the username and password on the specified access point.
- The **all** parameter configures the username and password on all the access points registered to the controller.

The password pushed from the controller is configured as “enable password” on the access point.

There are some cases where the pre-stage configuration for LWAPP access points is disabled and the access point displays the following error message when the CLI commands are applied:

“ERROR!!! Command is disabled.”

For more information, refer to *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.*

Exclusion List (Blacklist) Client Feature

If a client is not able to connect to an access point, and the security policy for the WLAN and client are correct, the client has probably been disabled. In the controller GUI, you can view the client’s status on the Monitor > Summary page under Client Summary. If the client is disabled, click **Remove** to clear the disabled state for that client. The client automatically comes back and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients disabled due to failed authorization do not appear on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

RADIUS Servers and the Management VLAN

If a RADIUS server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet.

Cisco 1000 Series Access Points and WMM

- In order to use Layer 2 LWAPP mode and WMM with a 1000 series access point, you must make sure that WMM is disabled.
- Clients cannot associate to an AP1030 in REAP mode if WMM is enabled on the WLAN. Disable WMM to allow the clients to associate.

Cisco Aironet 1030 Remote Edge Lightweight Access Points and WPA2-PSK

Cisco Aironet 1030 Remote Edge Lightweight Access Points do not support WPA2-PSK in REAP standalone mode.

Lightweight Access Point Connection Limitations

Cisco Aironet lightweight access points do not connect to the 4400 series controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.

RADIUS Servers

This product has been tested with CiscoSecure ACS 3.2 and later and works with any RFC-compliant RADIUS server.

Management Usernames and Local Netuser Names

Management usernames and local netuser names must be unique because they are stored in the same database. That is, you cannot assign the same name to a management user and a local netuser.

802.1x and Microsoft Wireless Configuration Manager

Clients using the Microsoft Wireless Configuration Manager and 802.1x must use WLANs configured for 40- or 104-bit key length. Configuring for 128-bit key length results in clients that can associate but not authenticate.

Using the Backup Image

The controller bootloader (ppcboot) stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

With the backup image stored before rebooting, be sure to choose **Option 4: Change Active Boot Image** from the boot menu to set the backup image as the active boot image. Otherwise, when the controller resets, it again boots off the corrupted primary image.

After the controller boots, the active boot image can be changed to the backup image using the **config boot backup** command.

Home Page Retains Web Authentication Login with IE 5.x

Because of a caching problem in the Internet Explorer 5.x browser, the home page retains the web authentication login. To correct this problem, clear the history or upgrade your workstation to Internet Explorer 6.x.

Rogue Location Discovery Protocol (RLDP)

Enabling RLDP may cause access points connected to the controller to lose connectivity with their clients for up to 30 seconds.

Ad-Hoc Rogue Containment

Client card implementations may mitigate the effectiveness of ad-hoc containment.

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1* for configuration instructions.

Note SNMP v3 is time sensitive. Make sure that you have configured the correct time and time zone on your controller.

Features Not Supported on 2000 and 2100 Series Controllers

These hardware features are not supported on 2000 and 2100 series controllers:

- Power over Ethernet (PoE) for 2000 series controllers only

Note Ports 7 and 8 on 2100 series controllers are PoE ports.

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)

These software features are not supported on 2000 and 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)

Some Clients See Only 64 Access Point MAC Addresses (BSSIDs) at a Time

In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco UWN rogue access point detection and containment can help you to enforce RF policies in your buildings and campuses.

2006 Image Not Supported for 3504 Controllers

The 2006 controller image is supported for use with only 2000 series controllers. Do not install the 2006 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Running a 3504 Image on a 2000 Series Controller

It is possible to run a 3504 controller image on a 2000 series controller, but Cisco Aironet 1130, 1200, and 1240 series access points will not be able to connect to the controller.

Upgrading External Web Authentication

When upgrading a controller from operating system release 2.0 or 2.2.127.4 to release 3.2.116.21 or later, update the external web authentication configuration as follows:

1. Instead of using a preauthentication ACL, the network manager must configure the external web server IP address using this command:

   config custom-web ext-webserver add *index IP-address*

   Note *IP-address* is the address of any web server that performs external web authentication.

2. The network manager must use the new login_template shown here:

   Note Make sure to format the script to avoid any extra characters or spaces before using the web authentication template.

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache"> <meta HTTP-EQUIV=”Content-Type”
CONTENT="text/html; charset=iso-8859-1"> <title>Web Authentication</title> <script>

function submitAction(){
     var link = document.location.href;
     var searchString = "redirect=";
     var equalIndex = link.indexOf(searchString);
     var redirectUrl = "";
     var urlStr = "";
     if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
   redirectUrl += urlStr;
         if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
       document.forms[0].redirect_url.value = redirectUrl;
  }
     }

     document.forms[0].buttonClicked.value = 4;
     document.forms[0].submit();
}

function loadAction(){
     var url = window.location.href;
     var args = new Object();
     var query = location.search.substring(1);
     var pairs = query.split("&");
     for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
     }
     //alert( "AP MAC Address is " + args.ap_mac);
     //alert( "The Switch URL is " + args.switch_url);
     document.forms[0].action = args.switch_url;
```

```
     // This is the status code returned from webauth login action
     // Any value of status code from 1 to 5 is error condition and user
     // should be shown error as below or modify the message as it suits
     // the customer
     if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
     }
     else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
     }
     else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the user is
already logged into the system?");
     }
     else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
     }
     else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid.
Please try again.");
     }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();"> <form method="post">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0"> <input
TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE=""> <input
TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0"> <tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password      <input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();"> </td> </tr> </table> </div>

</form>
</body>
</html>
```

Caveats

This section lists open, resolved, and closed caveats for Cisco controllers and lightweight access points.

Open Caveats

These caveats are open in controller software release 4.1.181.0.

- CSCsb77595—When logging out from Telnet/SSH sessions, the session always prompts the user to save changes, even when no changes have been made.

  Workaround: Ignore the prompt and exit as usual.

- CSCsb85113—When users download the software image to the controller using the CLI, access points are sometimes disconnected.

  Workaround: Download new code images to the WiSM at times when there are no clients to be affected.

- CSCsb88588—Access points report incorrect power levels when the controller is set to the SG country code.

  Workaround: None.

- CSCsc03214—If a WLAN is configured to use web policy for Layer 3 security authentication and is also configured to use the controller's default authentication page, the client cannot access the authentication page using HTTPS.

  Workaround: Use HTTP (not HTTPS) to access the authentication page.

- CSCsd52483—When you make changes in the bootloader of a 2006 controller or a Controller Network Module, the bootup process may halt, and the controller may stop responding. The controller also displays the "grub>" prompt on the console port.

  Workaround: Replace the controller.

- CSCsd60169—Enabling IPSec on a RADIUS authentication server makes SNMP and the controller GUI momentarily unreachable.

  Workaround: None.

- CSCsd64081—Ethernet multicast mode is not passing multicast traffic on the 2006 controller.

  Workaround: None.

- CSCsd84706—Containment information for ad-hoc rogue access points is not shown on the controller GUI.

  Workaround: Use the controller CLI.

- CSCse11464—The Management Frame Protection Settings page on the controller GUI displays a maximum of 100 access points.

  Workaround: If there are more than 100 access points under MFP, use the controller CLI to view the complete list.

- CSCse95826—When a new mesh access point joins the controller, the controller GUI may not populate the parent MAC address field when displaying the bridging information for mesh neighbors. This problem disappears after some time with more neighbor updates.

  Workaround: Use the controller CLI to view the mesh neighbors.

- CSCsf02280—If you change the position of the antenna on an autonomous AP1200 converted to lightweight mode, the power setting does not change.

  Workaround: None.

- CSCsf99924—In controller software releases 3.2.183.0 and later, you cannot configure the controller to automatically adjust its local time for daylight saving time (DST). This feature was available in earlier software releases, but it did not correctly adjust the time in the Southern Hemisphere and did not respond to the daylight saving time changes for the United States in 2007.

  Workaround: Follow these steps to work around this issue:

  a. Configure the controller for Greenwich mean time (GMT), with no time-zone offset.
  b. During standard time, run with the standard offset.
  c. When DST goes into effect, manually configure the controller for the correct local time.

     For example, if your controller is in the U.S. Eastern time-zone, then before March 11, 2007, your offset is –5. When DST takes effect, enter this CLI command: **config time timezone -4**.

- CSCsg22915—Multicast packets from mobile clients with the access point group multicast address are not dropped at the controller when multicast mode is set to mcast.

  Workaround: Make sure the multicast stream address and the access point group multicast address are different.

- CSCsg32646—If link aggregation (LAG) is enabled on the controller and the port channel is configured on the infrastructure switch, the controller displays only a single entry for its neighbor when you enter the **sh cdp neighbor** CLI command. When you enter the same command on the switch, it displays two entries for the controller for two different ports that are part of LAG. The controller should display two entries when the command is entered on the controller because the switch sends the CDP message from two different ports that are part of the port channel.

  Workaround: None.

- CSCsg35690—The SNMP client troubleshooting buffer wraparound does not work in cases where the number of messages exceed 2,000.

  Workaround: Delete the client from the watchlist and then re-add it to the watchlist for the messages.

- CSCsg48056—In certain cases, disabling the DHCP proxy causes a mesh access point to be perceived as a client instead of an access point. Because the access point does not satisfy the “Associated” state for a client, the DHCP server refuses to hand out an IP address to the access point.

  Workaround: Do not disable the DHCP proxy for mesh access points. Use this command to enable DHCP proxy: **config dhcp proxy enable**.

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

  Workaround: Turning off background scanning can alleviate this problem to some extent. However, if the packet loss and the jittery voice traffic are due to RF issues, then changing the RAP to a different channel may help.

- CSCsg74578—If you change a controller's management IP address, it is not sent to the access point unless the access point is reset. As a result, multicasting does not work until the change is made on the access point.

  Workaround: None.

- CSCsg76946—Cisco 3201 WMIC data throughput may be affected when using TKIP encryption.

  Workaround: Use AES encryption or 802.1x dynamic keys.

- CSCsg77609—A mesh access point may disconnect from the controller during a TCP or UDP stream from a wireless or Ethernet client in a hidden node situation. This disconnect can occur when a mesh access point is a hidden node to another node. Even though the LWAPP control packets that maintain the LWAPP connection between the controller and access point are attempted with a higher 802.11 priority, the hidden node may interfere with a node's traffic and subsequent LWAPP control packets.

  Workaround: Use the new routing around interference feature to create a secondary backhaul to reduce the hidden node problem. The appropriate CLI command is **config mesh secondary-backhaul enable force-same-secondary-channel**.

- CSCsg88380—When the source access point is connected to one controller and the destination access point is connected to a second controller and both controllers have the same MAC filter list, the mesh link test fails to run between the two access points.

  Workaround: Move both access points to one controller by setting the same primary controller on both access points.

- CSCsh13494—If you set the session timeout for an 802.1x WLAN to some value and then check the session timeout through the controller CLI, the timeout always shows as infinity. However, the controller GUI displays the correct value.

  Workaround: None. The functionality is not affected as the session times out after the specified value.

- CSCsh13928—In busy RF environments in large deployments, access points may disconnect from the controller intermittently.

  Workaround: Disable radio resource management (RRM) and statically set the channels and power levels.

- CSCsh15411—When an access point drops the IAPP packet from a CCX client just after association, the CCX Layer 2 roam history may not be available for CCX clients on the controller.

  Workaround: None.

- CSCsh29597—Reauthentication occurs if you click any link on the controller GUI after using a one-time password to authenticate management users.

  Workaround: Do not use a one-time password to authenticate management users.

- CSCsh31104—The word *channel* is misspelled in the message log.

  Workaround: None.

- CSCsh54247—You cannot perform the following logging functions on the controller:
  - Setting the system logging severity to filter out-going syslog messages
  - Setting the syslog facility
  - Configuring multiple syslog servers on the controller

  Workaround: None.

- CSCsh61934—A client connecting to the LWAPP architecture using reverse-ARP may fail to obtain an IP address.

  Workaround: None.

- CSCsh66559—Radio resource management (RRM) operates on ports 12134 (manager) and 12124 (client) between controllers. When you apply the following CPU access control list (ACL) to allow these packets to the controller's CPU, RRM does not function correctly and does not maintain an RF group leader.

```
1  In    0.0.0.0/0.0.0.0    0.0.0.0/0.0.0.0    17 12134-12134 12134-12134   Any Permit
2  In    0.0.0.0/0.0.0.0    0.0.0.0/0.0.0.0    17 12134-12134 12124-12124   Any Permit
3  In   0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0   17 12124-12124 12134-12134 Any Permit
```

  Workaround: None. CPU ACLs on the controller should never be used to deny or allow RRM packets between the controllers. Applying a CPU ACL for RRM can break the RF domain relationship between the controllers.

- CSCsh73171—When you enable CCKM on the controller for use with CB21AG client adapters, some CCKM configuration settings cause the client to send an association request in the middle of CCKM, thereby resulting in full authentication rather than CCKM. See the "Using CCKM with CB21AG Client Adapters" section on page 18 for details on which CCKM configuration settings do and do not operate properly.

  Workaround: Configure WPA + TKIP + authentication key management CCKM. This setting allows the client to roam successfully without performing full RADIUS authentication.

- CSCsh98559—CPU ACLs do not work for EoIP packets and DHCP received on the distribution system port.

  Workaround: None.

- CSCsi05147—Path loss reports are not appearing on the controller.

  Workaround: None.

- CSCsi06037—You can configure peer-to-peer blocking mode only globally. You cannot configure it on a per-WLAN basis. In addition, this feature does not block ARP packets between wireless clients on the same WLAN, only IP packets.

  Workaround: None.

- CSCsi06381—The mesh link test produces no results or returns 0 or infinity as values. This problem happens when the test is being performed on a heavily congested link or in a noisy environment.

  Workaround: Rerun the link test. If this does not help, rerun the test at a lower packet or data rate.

- CSCsi06849—When the available bandwidth becomes a negative number and the corresponding voice bandwidth in use is above 100%, roam calls [with 7921 traffic specifications (TSPECs) sent as part of the re-association packets] are accepted even when the roam bandwidth is exhausted.

  Workaround: None.

- CSCsi07934—Efficient multicast to 802.11 clients is not supported on mesh access points. Therefore, you should not turn on multicast mode on the controller when it needs to service mesh access points. If you do, the mesh access points may start disconnecting due to issues with queue overflow at the MAPs. This issue applies to all controller commands starting with:

  config network multicast

  Workaround: If you need to turn on the controller multicast mode for non-mesh access points, service mesh access points on a different controller than the one used for non-mesh access points.

- CSCsi11229—Clients may disassociate from a mesh access point even though the access point seems to be up and running. This problem happens when client entries on the access point are not being aged out in a timely manner, resulting in a high client count (greater than 100) and client association problems.

  Use the following commands on the controller to display the number of users on each radio on an access point:

  show ap stats 802.11b *Cisco_AP*

  show ap stats 802.11a *Cisco_AP*

  Workaround: None.

- CSCsi15588—Wireless-to-wireless calls made using a 7921 phone may become disconnected after a few minutes. This issue occurs when bidirectional traffic specifications (TSPECs) are present and the inactivity timer becomes activated due to inactivity in any one direction.

  Workaround: Change the default state of the inactivity timer to Off.

- CSCsi18966—When the multiple-country feature is used, dynamic frequency selection (DFS) does not operate properly if a DFS channel that is not common among the configured countries is assigned manually. As a result, the access point does not scan for 60 seconds when changed to a DFS channel. If radar is detected, then the 802.11a radio is shut down until manually reset.

  Workaround: Either deploy auto RF and let the controller assign the channel or if the channel has to be assigned manually, make sure you choose a non-DFS channel or a DFS channel that is common among the configured countries.

- CSCsi25491—If you choose **Wireless** from the CPU ACL Mode drop-down box on the CPU Access Control Lists page after selecting an ACL from the ACL Name drop-down box, the controller automatically defaults to the Both option instead of the Wireless option.

  Workaround: Use the controller CLI to set the CPU ACL mode.

- CSCsi26931—Throughput is asymmetrical and has additional downlink latency after a mobile wireless client roams. This condition occurs when mobility tunnels are created between controllers on different subnets to accommodate mobility groups.

  Workaround: Minimize latency between controllers. Also, ensure the highest speed and latency on the transport between controllers separating inter-subnet controllers.

- CSCsi28214—The Cisco WISM's slot number is shown incorrectly on WCS.

  Workaround: None.

- CSCsi35792—Controllers fail to establish a connection with open LDAP on a port other than 389.

  Workaround: Always use port number 389 with an LDAP server.

- CSCsi40354—Traffic stream metrics (TSM) information is not sorted chronologically on the controller GUI.

  Workaround: None.

- CSCsi53789—Autonomous access points that have been converted to lightweight mode sometimes do not forward controller-generated IGMP queries over the air. This issue occurs when no active clients are associated to the access point and the client roams to an access point on another controller.

  Workaround: Have at least one active client associated to the WLAN on that access point.

- CSCsi64689—If you disable DTPC support when RRM is enabled, the transmit power level for LWAPP-enabled access points automatically changes to transmit power level 1.

  Workaround: None.

- CSCsi78368—The client packet dot1p check, which performs the client's tos-to-DSCP translation, is not supported in controller software release 4.1 for packets from wireless clients to the network. The priority is always mapped to 0 (null). This issue occurs when you configure the "qos profile" for platinum, gold, silver, or bronze and the "wired qos protocol" for type = 802.1p and tag = N. This issue affects the priority field in the dot1p vlan header tag for the 4.1 release, so clients on VLANs are affected.

  Workaround: Do not configure the qos profile "wired qos protocol" type to 802.1p.

- CSCsi81630—The controller might reboot repeatedly around 5 minutes after startup. This condition usually occurs when the controller, acting as a client station, attempts to associate with a rogue access point.

  Workaround: Disable the Rogue Location Discovery Protocol.

- CSCsi86794—When auto channel selection is enabled on a controller running 4.1.171.0 or later and access points are set to channels 100, 104, 108, 112, 116, 132, 136, or 140, clients cannot associate.

  Workaround: Follow these steps to disable channels 100 to 140. Make sure to disable the radio network and then enable it after the channel change.

  a. On the controller GUI, click **Wireless > 802.11a/n**.
  b. Click **DCA** under RRM.
  c. Uncheck all of the channels between 100 to 140.
  d. Click **Apply** to commit your changes.

- CSCsi88526—If WMM Allowed or Required is configured for a WLAN and a WMM client is associated to a REAP access point, no IP connectivity is available to this client.

  Workaround: If your network contains only REAP access points, disable the WMM policy. If your network contains a mix of REAP access points and other access points, enable the WLAN override feature so that WMM-configured WLANs are not applied to REAP access points.

- CSCsi90344—When you use local EAP authentication to authenticate clients, the following message appears in the message log: "OSAPI-4-TIMERTCB_REALLOCATED: Timer 3607/1800205 (EAP Local Auth) found to be destroyed/reallocated."

  Workaround: None. This issue does not affect the clients' ability to authenticate. The message just unnecessarily fills the log.

- CSCsi90962—When an access point tries to join a controller but fails AAA authorization, an SNMP trap is not generated to show the failure.

  Workaround: You can view the error from the message log or by running the **debug lwapp error enable** CLI command on the console port of the controller.

- CSCsi93408—After upgrading to controller software release 4.1.171.0, mesh access points can associate to the controller but randomly lose connectivity to the root access point and controller due to errors resulting from interference, invalid key IDs, and an unstable transmit power level.

  Workaround: None.

- CSCsj03075—The client count on the controller appears to be cumulative rather than at a point in time. When clients disconnect, it shows them as still connected. This issue occurs on a WLAN that is not using 802.1x authentication.

  Workaround: Make sure that the Session Timeout value for the WLAN is not set to 0 seconds. If it is, change it to a nonzero value, such as 300 seconds.

  Note that access points joined to the controller might need to be rebooted to clear their client count list. Access points might still show clients associated to them when in fact there are none. Alternatively, the controller itself can be rebooted.

- CSCsj04127—The Cisco WISM might lock up when the **debug lwapp events enable** CLI command is executed.

  Workaround: None.

- CSCsj06245—Portions of the output of the **show tech-support** CLI command might be formatted incorrectly, making the information difficult to read.

  Workaround: None.

- CSCsj18577—After you upgrade to controller software release 4.1.171.0 and configure WPA1 or WPA2 with PSK, the syslog server might display the following message: "AAA-5-RADSERVER_NOT_FOUND: Couldn't find appropriate Radius server for VAP 6. Reason: Radius accounting is disabled."

  Workaround: None.

- CSCsj19875—When the controller reports the following error, it fails to include the MAC address of the client. Instead, it reports the MAC address of one of its own access points.

  Thu Jun 7 12:25:19 2007 Client Association Failure: MAC Address:00:15:70:17:8f:69 Base Radio MAC:00:14:f2:7d:be:00 Slot: 0 Reason:Unspecified ReasonCode: 1

  Workaround: None.

- CSCsj20565—A 4400 series controller might reboot when you click **Monitor > CDP > Interface Neighbors** on the controller GUI in software release 4.1.171.0.

  Workaround: None.

- CSCsj21964—An incorrect warning message appears when you configure WLANs 9 to 16. The message reads, "Not all types of AP support WLAN ID greater than 8, do you wish to continue?" It should read, "Not all types of APs support WLAN IDs greater than 8, do you wish to continue?"

  Workaround: None.

- CSCsj25953—When 200 or more wireless clients try to associate to a controller at the same time, the clients become stuck in the DHCP_REQD state. The controller receives the DHCP offer from an external DHCP server but does not send the offer to the access point in LWAPP.

  Workaround: None.

- CSCsj26541—WLAN configuration changes (such as changing the network supported data rates) do not take affect for 1500 series access points in RAP mode without rebooting the access points.

  Workaround: Use the controller GUI to disable the access point's backhaul radio, change the data rate, and then re-enable the backhaul radio.

- CSCsj33229—You might be unable to ping access points that are directly connected to the switch ports on a 2106 controller. The IP address of each access point does not appear in the ARP cache of the controller, but clients connected to the access points can browse the network.

  Workaround: Connect the access points to a different device such as a switch.

- CSCsj33995—In controller software release 4.1.171.0, you cannot control whether web authentication uses an external RADIUS server database or the local database. The controller also attempts to use the local database if the user does not exist in the external RADIUS server.

  Workaround: None.

- CSCsj35540—There is no method to convert the Cisco 3201 Wireless Mobile Interface Cards (WMICs) from LWAPP to Cisco IOS.

  Workaround: None.

- CSCsj35724—When the controller is running software release 4.1.171.0, the syslog servers might stop adding an IP address to the front of syslog messages.

  Workaround: Change the syslog server to one that accepts the Cisco standard syslog format.

- CSCsj35964—A hybrid-REAP access point might reboot under the following conditions:
  - The WLAN has WMM allowed.
  - The radio policies are set to something other than *All*, such as *802.11b/g Only*.
  - The 802.11a network is disabled.
  - Changes are made to the WLAN configuration (for example, enabling or disabling the SSID.

  The hybrid-REAP configuration (VLAN mappings) might also become lost, requiring a manual reconfiguration to enable them.

  Workaround: Disable WMM before making any other changes to the WLAN or 802.11 network configuration. You might be able to prevent this issue by not disabling the 802.11 network.

- CSCsj38106—A 2106 controller running software release 4.1.171.0 might reboot without a log record.

  Workaround: None.

- CSCsj39670—When a client uses WPA2 and AES-CCMP with AironetIE disabled, it loses association when the session timeout expires on the RADIUS server.

  Workaround: Either disable **Allow AAA Override** or enable **AironetIE**.

- CSCsj40291—Controller software release 4.1.171.0 does not encapsulate broadcast traffic in the LWAPP tunnel. As a result, broadcast traffic is not sent from a server application to the wireless clients.

  Workaround: None.

- CSCsj53221—If you click **Wireless > Mesh** on the controller GUI and then click the **Apply** button on the Mesh page, all of the mesh access points are rebooted even if you have not made any changes on the Mesh page.

  Workaround: None.

- CSCsj71552—In controller software release 4.1, the location-based RSSI timer for access points may expire the rogue access point entries.

  Workaround: Make sure that the location-based RSSI timers and the rogue access point expiry timers have the same expiry value.

- CSCsj76795—The controller may send duplicate rogue access point trap messages.

  Workaround: None.

- CSCsj77612—The 7921 phone may drop calls if the controller is running software release 4.1 and is configured to use WPA2 with both AES and TKIP.

  Workaround: Configure the controller for WPA2 with AES only or WPA1 with TKIP only.

Resolved Caveats

These caveats are resolved in controller software release 4.1.181.0.

- CSCsc04907—Resetting the access point to factory defaults does not clear the static IP address.

- CSCse66714—When you use the controller GUI to set a static IP address on a different subnet than the one the access point is on, the access point reboots, but the GUI page does not refresh. When the access point reboots, it sometimes uses a fallback address, and the display shows the static IP address configuration as well as the IP address it is using.
- CSCse76616 and CSCsg29848—After a reload of the Catalyst 6500 switch and the Supervisor 720, the Supervisor 720 reports a duplicate service port IP address for the WiSM, even though no duplicate IP address for the service port is configured.
- CSCsg00073—When using web authentication, clients might not receive the username and password prompt if the session timeout is configured for a value of 60 minutes or more.
- CSCsg03174—The controller network module in the Cisco 28/37/38xx Series Integrated Services Router does not reject incompatible software.
- CSCsg26982—The 4402 controller might not respond properly to the SNMP server interface discovery.
- CSCsg32267—The controller transmits data at the 1-Mbps rate even though data transmission at this rate is disabled.
- CSCsg72036—A controller running software release 4.0.179.8 occasionally experiences an issue with certain client cards sending bad information to a 1240 series access point, which results in the access point going into discovery mode with the error message *L2 Queue Full*.
- CSCsg81953—Controllers sometimes report IDS disassociation flood attacks against valid clients in which the attacker's MAC address is that of an access point joined to that controller.
- CSCsh42173—RFID tags time out quickly when their auto-timeout feature is enabled.
- CSCsh63939—Some TACACS+ accounting commands are not logged or are logged incorrectly.

  Examples of unlogged commands:

  - The **config advanced 802.11a receiver pico-cell-V2 send_iapp_req** command is not logged.
  - The **config wlan mfp infrastructure protection** {**enable** | **disable**} command is not logged.

  Examples of incorrectly logged commands:

  - The **config 802.11b txPower global 1** command is logged as **802.11b txPower global off**.

  On the 2006, 2106, and controller network modules, the IP addresses for some of the commands appear in reverse order. The IP address appears as D.C.B.A instead of A.B.C.D. For example, **acl rule destination address test 2 192.168.0.11 255.255.255.0** is logged as **acl rule destination address test 2 11.0.168.192 0.255.255.255**.
- CSCsh73667—Controllers running software release 4.1.171.0 might not detect a rogue access point on the wire through the Rogue Location Detection Protocol (RLDP).
- CSCsh77143—When a multicast ARP request is tunnelled using EoIP from an anchor controller to a foreign controller with the proxy ARP disabled, the foreign controller drops the ARP request and does not forward it to the associated client.
- CSCsh88005—When you create a WLAN using the controller GUI, you cannot define a session timeout of 0 for WLANs with PSK encryption.
- CSCsh88426—You might experience intermittent access to the controller, whereby two gigabit ports are responsive and the other two are not. In this case, you might see console error messages similar to the following: "Msg 'Set system global config' of System Table failed, Id = 0x006e303a error value = 0xfffffffc."
- CSCsh90008—When the configuration between the controller and WCS is not synchronized, the link between the parent and child access points is not drawn. A directional arrow is seen from the child to the parent access point, but the link is not drawn.

- CSCsh92460—A TACACS+ user with the Management privilege can add or delete local management users with read-write or lobby-ambassador permission.
- CSCsh95128—Rogue Location Detection Protocol (RLDP) does not operate properly for hybrid-REAP access points.
- CSCsh95306—802.1x reauthentication might disrupt voice calls, and there is no way to stop the reauthentication from either the controller GUI or CLI.
- CSCsh98959—In controller software release 4.0.206.0 and later, the WLAN override feature does not work properly if the profile name does not match the SSID.
- CSCsi03423—When using web authentication, the server chooses a weak cipher even when the Secure Sockets Layer (SSL) client presents a strong cipher.
- CSCsi05989—Client reauthentication does not occur for a WLAN configured for WPA+WPA2+CCKM after the configured session timeout expires. This issue occurs only if the client roams.
- CSCsi16810—If an access point using infrastructure management frame protection (MFP) goes into the hybrid-REAP standalone mode, the access point ceases to attach MFP message integrity check (MIC) Aironet information elements (IEs) to transmitted frames because infrastructure MFP is not supported in this mode. Access points connected to other controllers within the same mobility group might generate *Missing MIC* alerts under some circumstances.

  If the access point changes to standalone mode because the controller has lost Ethernet connectivity, other access points within the mobility group are not informed that the access point in the standalone mode is no longer sending protected frames and might report "Missing MIC" MFP errors until the controller recovers connectivity or the access point joins another controller.
- CSCsi30017—The **session 1 processor 1** command is not working on the Catalyst 3750G Wireless LAN Controller Switch.
- CSCsi43822—If you use the controller GUI or CLI to disable and save an existing LDAP server configuration, the LDAP server configuration is re-enabled after a controller reboot.
- CSCsi47353—The Appletalk protocol is not supported in controller software release 4.1.171.0.
- CSCsi49767—If a WLAN is configured with an interface ACL and an access point group has been applied to the access point, the controller might reboot when a client joins the access point.
- CSCsi52006—The access point radio operational status is *Down* after setting the access point to factory defaults when using Power over Ethernet (PoE) from certain prestandard 15-Watt switches.
- CSCsi52637—Access point failover might not function correctly for Cisco WiSM controllers. After access points fail over to the secondary controller, only a few access points initially fall back successfully to the primary. Some might wait for 30 to 40 minutes to fall back, and some never fall back. This issue occurs only when Cisco Aironet 1000 series lightweight access points are present in the network.
- CSCsi54265—You cannot change the serial port baud rate using the controller GUI.
- CSCsi57702—The following controller CLI command to enable global public safety on mesh access points is not supported in software release 4.1.171.0: **config mesh public-safety enable all**.
- CSCsi59501 and CSCsi34566—7921 calls do not go through when the hybrid-REAP access point is in standalone mode.
- CSCsi60185—The default value for EAP-Request retransmissions (**config advanced eap request-retries**) was changed from 2 to 0. As a result, when default values are used, the controller does not retry EAP-Requests that were lost between the controller and the client. This issue applies only to new installations and customers who are using the default controller configuration on release 4.1.171.0.

- CSCsi60536—When you disable management frame protection (MFP) for a specific access point, this feature becomes re-enabled after you reboot the access point. The access point saves the setting only when MFP is enabled globally.
- CSCsi69351—You can disable the public-safety functionality (using the CLI command **config mesh public-safety disable all)** on a mesh network when public-safety channels (20 or 26) are active, and an error or warning message does not appear. The following message now appears when you attempt to disable public safety: "Public Safety cannot be disabled since Mesh AP is on public safety channel = 26." The value of 20 appears in the warning message in place of 26 when applicable.
- CSCsi75568—A mesh access point's forward state might become stuck in 802.1x-only because the controller sends the 802.1x identity message to another device. This issue occurs if the RCB of the parent MAP is changed for any reason.
- CSCsi77945—When a controller is running software release 4.1.171.0 with local EAP-FAST enabled, Cisco 7920 IP phones might not join the network when using EAP-FAST WPA/TKIP and local EAP authentication. Make sure that you are also using the latest software for your 7920 phones to ensure proper operation.
- CSCsi78460—The available admission capacity (AAC) of the QBSS Load IE is not set in beacons or probe responses. The AAC is set to zero. Clients with call admission control (CAC) enabled might not associate to an access point that sends an AAC value of zero because the clients might check the AAC before sending ADDTS requests and associate/re-associate request. The clients might judge that there are no more calls being admitted to the access point, even when the access point has the capacity to admit new traffic. This issue occurs for wireless clients that check the AAC before sending an ADDTS request.
- CSCsi80421—On some controllers, the **debug lwapp packet enable** CLI command does not show any output.
- CSCsi84986—Some mesh access points fail to join the root access point after upgrading to software release 4.1.171.0.
- CSCsi95068—The controller GUI might report a value of zero for the signal-to-noise ratio (SNR) while the **show mesh neigh summary** *Cisco_AP* CLI command reports the correct SNR value.
- CSCsi97452—When a Cisco 7921 phone associates to a WLAN or SSID that is configured on a 2006 controller, the controller might become unresponsive and eventually reboot.
- CSCsi99388—The **config msglog level security** CLI command has been removed in controller software release 4.1.181.0. Only these **config msglog level** *?* commands are now supported:
  - **critical**—Critical hardware or software failure.
  - **error**—Noncritical software error.
  - **warning**—Unexpected software events.
  - **verbose**—Significant system events.
- CSCsi99569—The Number of Clients field on the Rogue APs page of the controller GUI might not accurately reflect the number of associated rogue clients.
- CSCsj02639—Remote authentication does not work over wireless mesh network connections in some situations. Authentication for mesh networks should always be done locally on the controller. Enter the following CLI command to enable local authentication on the controller: **config mesh local-auth enable** and verify that the MAC addresses for all mesh access points are entered into the MAC filter list.
- CSCsj02690—When you use 1000 series access points, beacons might occur at irregular intervals on the 2.4-GHz band.

- CSCsj09449—The public-safety CLI command for individual access points might cause stranding issues for mesh access points. In controller software release 4.1.181.0 and later, public safety on mesh access points can only be configured globally, using the following command: **config mesh public-safety** {**enable** | **disable**} **all**.
- CSCsj11323—The 7920 phone fails EAP-FAST authentication when using local EAP authentication on the controller.
- CSCsj12053—MAC filtering is not supported for workgroup bridge (WGB) wired clients. However, a wired client might be a terminal server that does not send any traffic but receives traffic instead (through Telnet requests). As a result, the controller never learns its IP address and deletes the wired client record.
- CSCsj12637—If you choose **Authentication or Security Errors** from the Message Log Level drop-down box on the Syslog Configuration page of the controller GUI and click **Apply**, the configuration is saved as Software Error.
- CSCsj18643—Neighbor packets might not be sent at the correct rates for 802.11a and 802.11b/g radios.
- CSCsj20381—When you run controller software release 4.1.171.0, the attributes sent to the RADIUS server in **debug** commands are truncated. The output stops between 48 and 64 bytes. When **debug client** is enabled, none of the attributes appear.
- CSCsj26597—Regardless of whether an access point is in PSK or EAP mode, it can enter a state in which it excludes potential parents, even if the parents are viable. A reboot of the child immediately fixes the exclusion issue.
- CSCsj31387—The Cisco WiSM might reboot and display the following error: "Software Failed on instruction located at: 0x102eb4d4 (ewsCliDepth+100)."
- CSCsj33058—The user configuration file for lobby ambassadors has not been checked in.
- CSCsj44081—Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures. This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  Details: The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp: May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error. The error message is then followed by a traceback.
- CSCsj50374—When you enter the **config network arpunicast enable** command on the controller CLI, a broadcast ARP frame may be forwarded back and forth at a very high rate between two or more controllers in a mobility group, resulting in a broadcast storm.

Closed Caveats

These caveats are listed in the "Open Caveats" section of the controller release notes for software release 4.1.171.0 and have been closed in controller software release 4.1.181.0.

- CSCsb01980—When the operator enters incorrect data for the management interface in the controller web configuration wizard, error messages are shown only at the end of the wizard, and the user must return to the Management Interface page for correction. The data entered on the Management Interface page, such as the port number, are not validated immediately but at the end of the wizard. As a result, any error messages are shown only at the end.

  Workaround: Use the CLI configuration wizard.

- CSCsd54171—After you upgrade or modify your controller configuration, the changes might not take effect or might not function properly.

  Workaround: Follow these steps:

  a. Refresh the configuration from the switch to WCS (deleting any differences).

  b. Clear the configuration on the controller.

  c. Complete the setup wizard, making sure to set the same IP address, community string, and country code setting.

  d. Use WCS to restore the configuration to the controller.

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:

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

(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/c/en/us/support/index.html

Click **Product Support > Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Documentation Updates

This section lists updates to user documentation that has not yet been added to either printed or online documents.

Omissions

The Package Contents section in the *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers* should be updated to include this item, which is included with the 4400 series controller:

- DB-9-to-DB-9 null modem cable

Related Documentation

For additional information on the Cisco controllers and lightweight access points, refer to these documents:

- The quick start guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller Online Help*
- *Cisco Wireless Control System Configuration Guide*
- *Cisco Wireless Control System Online Help*

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

http://www.cisco.com/c/en/us/support/index.html

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html