Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 6.0.199.0

July 2010

These release notes describe open and resolved caveats for maintenance software release 6.0.199.0 for Cisco 2100, 4400, and 5500 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSMs); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points; Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh 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 referred to as *controllers*, and all of the Cisco lightweight access points are 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 6.0.199.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 6.0.196.0
- Cisco WCS Navigator 1.5.196.0
- Location appliance software release 6.0.102.0
- Cisco 2700 Series Location Appliances
- Mobility services engine software release 6.0.105.0 and Context Aware Software

  Note Client and tag licenses are required in order to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 6.0* for more information.

- Cisco 3350 Mobility Services Engines
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

Note The 6.0.199.0 release does not support the NM-AIR-WLC6 platform.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points

  Note This release does not support Cisco Aironet 1505 and 1510 access points.

- Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points

Note Controller software release 5.0.148.0 or later releases is not compatible with Cisco Aironet 1000 series access points.

Note The AP801 is an integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs).

Note The 801 access point (the access point embedded in the 88xW ISR), the 1250 series access point, and the 1140 series access point have a hardware limitation where beacons can only be output at intervals that are multiples of 17 milliseconds. When these APs are configured for a 100-millisecond beacon interval, they transmit beacons every 102 milliseconds. Similarly, when the beacon interval is configured for 20 milliseconds, these APs transmit beacons every 17 milliseconds.

Note Only Cisco Aironet 1200 Series Access Points that contain 802.11g (AIR-MP21G) or second-generation 802.11a radios (AIR-RM21A or AIR-RM22A) are supported for use with controller software releases. The AIR-RM20A radio, which was included in early 1200 series access point models, is not supported. To see the type of radio module installed in your access point, enter this command on the access point: **show controller dot11radio** *n*, where *n* is the number of the radio (0 or 1).

Note For 5500 Series controller, the Dot1p value in the capwap packet between controller and the AP is always 0 irrespective of the profile configured on the WLAN and the DSCP value.

Controller Requirements

The controller GUI requires the following operating system and web browser:

- Windows XP SP1 (or later) or Windows 2000 SP4 (or later)
- Internet Explorer 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later)

Note Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for using the controller GUI and web authentication.

MIB Files

Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com. Only one MIB is posted per major release (6.0, 5.2, 5.1, and so on). If an updated MIB becomes available, the previous version is removed from the Software Center and replaced by the new version.

New Features

This maintenance release does not introduce new features.

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 releases. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software release 3.2.78.4 or later releases, 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 To use the Cisco WiSM in the Cisco 7609 and 7613 Series Routers, the routers must be running Cisco IOS Release 12.2(18)SXF5 or later releases.

Note The Cisco Wireless LAN Controller Network Module is supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2, 12.4(11)T3, and 12.5.

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, 12.2(35)SE or later releases, 12.2(37)SE or later releases, 12.2(44)SE or later releases, or 12.2(46)SE or later releases. The following Cisco IOS Releases and any variants are not supported: 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 software feature sets (IP Base, IP Service, and Advanced IP Services) are supported for use with the controller.

Note You can use the 2112 and 2125 controllers only with software release 5.1.151.0 or later releases.

Finding the Software Release

To find the software release running on your controller, click **Monitor** and look at the Software Version field under Controller Summary on the controller GUI or enter **show sysinfo** on the controller CLI.

Special Rules for Upgrading to Controller Software Release 6.0.199.0

Caution Before upgrading your controller to software release 6.0.199.0, you must comply with the following rules.

- Before you download a software image or an ER.aes file to a 2100 series controller or a controller network module, use the **show memory statistics** CLI command to see the current amount of free memory. If the controller has less than 90 MB of free memory, you need to reboot it before downloading the file.
- Before you use an AP801 series lightweight access point with controller software release 6.0.199.0, you must upgrade the software in the Cisco 860 and 880 Series Integrated Services Routers (ISRs) to Cisco IOS 12.4(22)T and the software in the Cisco 890 Series Integrated Services Router to Cisco IOS 12.4(22)YB.
- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 6.0.199.0 is larger 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 tftpd and the TFTP server within the WCS. If you attempt to download the 6.0.199.0 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 you are upgrading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 6.0.199.0. Table 1 shows the upgrade path that you must follow before downloading software release 6.0.199.0.

Table 1 Upgrade Path to Controller Software Release 6.0.199.0

Current Software Release	Upgrade Path to 6.0.199.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 or later 4.0 release, then upgrade to 4.2.176.0, before upgrading to 6.0.199.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 6.0.199.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 6.0.199.0.
4.1.191.xM	Upgrade to 4.1.192.35M and then to 6.0.182.0 before upgrading to 6.0.199.0.
4.1.192.xM	You can upgrade directly to 6.0.199.0.
4.2.130.0 or earlier 4.2 release	Upgrade to 4.2.176.0 before upgrading to 6.0.199.0.
4.2.173.0 or later 4.2 release	You can upgrade directly to 6.0.199.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 6.0.199.0.
5.1.151.0 or later 5.1 release	You can upgrade directly to 6.0.199.0.
5.2.157.0 or later 5.2 release	You can upgrade directly to 6.0.199.0.
6.0.188.0 or later 6.0 release	You can upgrade directly to 6.0.199.0.
6.0.196.0 or later 6.0 release	You can upgrade directly to 6.0.199.0.

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 6.0.199.0 software. In large networks, it can take some time to download the software on each access point.

Note You cannot install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0ER.aes file on Cisco 5500 Controller platform.

- For WiSM and standalone 4400 Controllers, we recommend that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file. This file resolves CSCsm03461 and is necessary in order for you to view the version information for ER.aes files in the output of the **show sysinfo** CLI command. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and "N/A" appears in the Emergency Image Version field in the output of this command.

  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 (5.2.157.0 ER.aes) ensures that the boot software 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.

Software Release Support for Access Points

Table 2 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Table 2 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	AIR-AP1020	3.0.100.0	4.2.207.0
	AIR-AP1030	3.0.100.0	4.2.207.0
	Airespace AS1200	—	4.0
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—

Table 2 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M

Table 2 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later releases[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later releases[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later releases[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later releases[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later releases[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later releases[1]	—
	AIR_LAP1523CM	6.0.196.0	
	AIR-LAP1524SB	-A, C and N: 6.0 or later releases	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later releases[1]	—

[1] These access points are supported in the separate 4.1.19x.x Mesh Software Release train or with Release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 Release trains.

Special Rules for Upgrading to Controller Software 6.0.199.0 in Mesh Networks

Caution Before upgrading your controller to software release 6.0.199.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 3 outlines the upgrade compatibility of controller mesh and nonmesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

- You can upgrade from 4.1.192.22M and 4.1.192.35M to 6.0.182.0 without any configuration file loss. See Table 3 for the available upgrade paths.

  Note If you downgrade to a mesh release, you must then reconfigure the controller. We recommend that you save the configuration from the mesh release before upgrading to release 6.0.199.0 for the first time. Then, you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 6.0.199.0 to a mesh release (for example, 4.1.190.5, 4.1.191.22M, or 4.1.192.xM) without losing your configuration settings.
- Configuration files are in the binary state immediately after an upgrade from a mesh release to controller software release 6.0.199.0. After reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.
- If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 6.0.199.0, the controller might reboot without a crash file. To work around this problem, manually reset the controller without saving the configuration after you upgrade the controller to software release 6.0.199.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 3 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases

Upgrade to	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
Upgrade from																													
6.0.182.0	Y	Y	Y	Y																									
4.1.192.35M				Y	Y																								
4.1.192.22M				Y	Y	Y																							

Table 3 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases (Continued)

Upgrade to	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
4.1.191.24M						Y	–																						
4.1.190.5						Y[1]	Y	–																					
4.1.185.0							Y	Y[2]	–																				
4.1.181.0								Y[2]	Y[2]																				
4.1.171.0								Y[2]	Y[2]	–																			
4.0.219.0									Y[2]	Y[2]	–																		
4.0.217.204							Y[2]		Y[2]	Y[2]	Y[2]	–																	
4.0.217.0									Y[2]	Y[2]	Y[2]	Y[3]	–																
4.0.216.0									Y[2]	Y[2]	Y[2]	Y[3]	Y	–															
4.0.206.0									Y[2]	Y[2]	Y[2]	Y[3]	Y		–														
4.0.179.11													Y		Y[4]	–													
4.0.179.8													Y		Y[4]	Y	–												
4.0.155.5													Y		Y[4]	Y	Y	–											
4.0.155.0													Y		Y[4]	Y	Y	Y	–										
3.2.195.10													Y		Y[4]	Y	Y	Y		–									
3.2.193.5													Y		Y[4]	Y	Y	Y		Y	–								
3.2.171.6													Y		Y[4]	Y	Y	Y		Y		–							
3.2.171.5													Y		Y[4]	Y	Y	Y		Y		Y	–						
3.2.150.10													Y		Y[4]	Y	Y	Y		Y		Y		–					
3.2.150.6													Y		Y[4]	Y	Y	Y		Y		Y		Y	–				

Table 3 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases (Continued)

Upgrade to	6.0.199.0	6.0.196.0	6.0.188.0	6.0.182.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
3.2.116.21													Y		Y[4]	Y	Y	Y		Y		Y		Y		–			
3.2.78.0													Y		Y[4]	Y	Y	Y		Y		Y		Y		Y	–		
3.1.111.0																				Y		Y		Y		Y	Y	–	
3.1.105.0																				Y		Y		Y		Y	Y	Y	–
3.1.59.24																				Y		Y		Y		Y	Y	Y	Y

[1] You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.

[2] Customers who require dynamic frequency selection (DFS) functionality should not use this release. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.

[3] Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.

[4] An upgrade to 4.0.206.0 is not allowed in the following country codes when operating with the following access points: Australia (1505 and 1510), Brazil (1505 and 1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and 1510), New Zealand (1505 and 1510), and Russia (1505 and 1510). Note: The 1505 mesh access point is not supported in release 5.0 and later releases. The 1510 mesh access point is supported only in mesh releases 4.1.190.5, 4.1.191.22M, and 4.1.192.xxM.

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. Up to 10 access points can be concurrently upgraded from the controller.

Note The Cisco 5500 Series Controllers can download the 6.0.199.0 software to 100 access points simultaneously.

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 releases, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note In controller software release 5.2 or later releases, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 6.0.196.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group. Access point groups do not enable WLANs to be transmitted on per radio interface of AP.

Note If a WiSM controller is heavily loaded with access points and clients and is running heavy traffic, software upgrade sometimes causes Ethernet receive-path lockup and the hardware watchdog sometimes trips. You might need to reset the controller to return to normal operation.

Note Do not install the 6.0.199.0 controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller, and then install the other file and reboot the controller.

To upgrade the controller software using the controller GUI, follow these steps:

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

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

Step 2 Obtain the 6.0.199.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com as follows:

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

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.

e. Click a controller series.

f. If necessary, click a controller model.

g. If you chose Standalone Controllers in Step d., click **Wireless LAN Controller Software**.

h. If you chose Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) in Step e., click **Wireless Services Modules (WiSM) Software**.

i. Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

   - **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.
   - **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
   - **Deferred (DF)**—These software releases have been deferred. We recommend that you migrate to an upgraded release.

j. Click a software release number.

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

l. Click **Download**.

m. Read Cisco's End User Software License Agreement and then click **Agree**.

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 6.0.199.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 Disable any WLANs on the controller.

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

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

Step 8 From the Transfer Mode drop-down box, choose **TFTP** or **FTP**.

Step 9 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 10 If you are using a TFTP server, 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 11 In the File Path field, enter the directory path of the software.

Step 12 In the File Name field, enter the name of the software file (*filename*.aes).

Step 13 If you are using an FTP server, follow these steps:

a. In the Server Login Username field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 14 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm your decision to reboot the controller.

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 6.0.199.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Reenable the WLANs.

Step 20 For Cisco WiSMs, reenable the controller port channel on the Catalyst switch.

Step 21 Reenable your 802.11a and 802.11b/g networks.

Step 22 If desired, reload your latest configuration file to the controller.

Step 23 To verify that the 6.0.199.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 24 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Emergency Image Version field.

Note If you do not install the 5.2.157.0 ER.aes file, the Emergency Image Version field shows “N/A.”

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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280

Warning **This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

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.** Statement 1024

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

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.** Statement 339

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

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

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

See 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.

Using the Cisco 5500 Series Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

Note The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.

Note Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

USB Console OS Compatibility

- Microsoft Windows 2000, XP, Vista (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

To install the Cisco Windows USB console driver, follow these steps:

Step 1 Follow these steps to download the USB_Console.inf driver file:

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

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243

b. Click **Wireless LAN Controllers**.

c. Click **Standalone Controllers**.

d. Click **Cisco 5500 Series Wireless LAN Controllers**.

e. Click **Cisco 5508 Wireless LAN Controller**.

f. Choose the USB driver file.

g. Save the file to your hard drive.

Step 2 Connect the Type A connector to a USB port on your PC.

Step 3 Connect the mini Type B connector to the USB console port on the controller.

Step 4 When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

Note Some systems might also require an additional system file. You can download the Usbser.sys file from this URL:
http://support.microsoft.com/kb/918365

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, change the Cisco USB systems management console COM port to an unused port of COM 4 or lower. To do so, follow these steps:

Step 1 From your Windows desktop, right-click **My Computer** and choose **Manage**.

Step 2 From the list on the left side, choose **Device Manager**.

Step 3 From the device list on the right side, double-click **Ports (COM & LPT)**.

Step 4 Right-click **Cisco USB System Management Console 0108** and choose **Properties**.

Step 5 Click the **Port Settings** tab and click the **Advanced** button.

Step 6 From the COM Port Number drop-down box, choose an unused COM port of 4 or lower.

Step 7 Click **OK** to save; then close the Advanced Settings dialog box.

Step 8 Click **OK** to save; then close the Communications Port Properties dialog box.

Important Notes for Controllers and Nonmesh Access Points

This section describes important information about controllers and nonmesh lightweight access points.

Increase in the IGMP Timeout Value from 30 Seconds to 120 Minutes

To set the IGMP timeout, enter a value between 30 and 7200 seconds in the IGMP Timeout field. The controller sends three queries in one timeout value at an interval of *timeout* /3 (if the timeout value is more than 360 seconds, controller sends one query every 120 seconds, irrespective of the value configured) to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value (if the timeout value is more than 360 seconds, controller waits for 360 seconds irrespective of the value configured) to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

ARP Requests Sometimes Fail for Access Points Connected Directly to Cisco 2100 Series Controllers

Cisco 2100 Series Controllers do not support ARP requests from access points connected directly to a port on the controller unless there is an interface configured on that controller port. ARP requests from the access point cannot reach the gateway on the interface VLAN and the access point might lose its connection to the controller.

To work around this limitation, configure the access point’s default gateway to match the controller’s management IP address, or connect the access point to a switch port between the access point and the 2100 series controller.

WPlus License Features Included in Base License

All features included in a Wireless LAN Controller WPlus license are now included in the base license; this change is introduced in release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing.

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:

- If you have a WPlus license and you upgrade from 6.0.18x to 6.0.199.0, your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 6.0.199.0 to 6.0.196 or 6.0.188, the license file in 6.0.199.0 contains both Basic and WPlus license features, so you will not see any disruption in feature availability and operation.

- If you have a base license and you downgrade from 6.0.199.0 to 6.0.196 or 6.0.188, when you downgrade, you lose all WPlus features.

Note Some references to Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 6.0.199.0. However, WLC WPlus license features have been included in the Base license, so you can ignore those references.

Additive Licenses Available for Cisco 5500 Series Controllers

You can now purchase licenses to support additional access points on Cisco 5500 Series Controllers. The new additive licenses (for 25, 50, or 100 access points) can be upgraded from all license tiers (12, 25, 50, 100, and 250 access points). The additive licenses are supported through both rehosting and RMAs.

One-Time Password (OTP) Support

One Time Passwords (OTP) are supported on the Wireless Lan Controller (WLC) using TACACS and RADIUS. In this configuration, the controller acts as a transparent pass-through device. The controller forwards all client requests to the TACACS/RADIUS server without inspecting the client behavior. When using OTP, the client must only establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.

RADIUS Called-station-id and Calling-station-id Attributes

In software releases prior to 6.0, the controller sends uppercase alpha characters in the MAC address. In software release 6.0 or later releases, the controller sends lowercase alpha characters in the MAC address for the RADIUS called-station-id and calling-station-id attributes. If you enabled these attributes for 802.1X authentication in previous releases and upgrade to software release 6.0, client authentication fails. Therefore, you must change the MAC addresses to lowercase characters on the RADIUS server before upgrading to software release 6.0.

Access Point Groups

You can create up to 50 access point groups for Cisco 2100 Series Controllers and controller network modules and up to 192 access point groups for Cisco 4400 Series Controllers, Cisco 5500 Series Controllers, the Cisco WiSM, and the 3750G wireless LAN controller switch.

Using Access Points in Sniffer Mode

You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. To disable IP-MAC address binding, enter this command using the controller CLI: **config network ip-mac-binding disable**.

WLAN 1 must be enabled in order to use an access point in sniffer mode if the access point is joined to a 5500 series controller, a 2100 series controller, or a controller network module running software release 6.0. If WLAN 1 is disabled, the access point cannot send packets.

Inter-Release Controller Mobility

When controllers in the mobility list are running different software releases (such as 5.0, 5.1, 5.2, and 6.0), Layer 2 or Layer 3 client roaming is not supported between GD to ED. It is supported only between controllers running the same and GD release such as 6.0 and 4.2.

Guest tunneling works only between controllers running the same software release or between controllers running software release 4.2 and controllers running any later software release (for example, 4.2 to 5.0, 4.2 to 5.1, 4.2 to 5.2, or 4.2 to 6.0). Guest tunneling does not work among controllers running other combinations of software.

RLDP Limitations in This Release

Rogue Location Discovery Protocol (RLDP) is a controller feature that detects the presence of rogue access points that are connected to your wired network. In this software release, RLDP operates with these limitations:

- RLDP detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast BSSID (that is, the access point broadcasts its SSID in beacons).
- RLDP detects only rogue access points that are on the same network. In other words, if an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.
- RLDP does not work on 5-GHz dynamic frequency selection (DFS) channels.
- If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue at any time.

Also, in controller software release 6.0, the rogue containment packet transmission times have changed as follows:

- For monitor mode, rogue containment deauthentication packets are still sent at 100-msec intervals.
- For non-monitor mode, deauthentication packets are sent at 500 msec (minimum). In previous releases, they are sent at 100-msec intervals.

Internal DHCP Server

When clients use the controller’s internal DHCP server, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

Bootloader Menu

When you plug a controller into an AC power source, the bootup script and power-on self-test run to initialize the system. During this time, you can press **Esc** to display the bootloader Boot Options Menu. The menu options for the Cisco 5500 Series Controllers are different than for other controller platforms.

Bootloader Menu for Cisco 5500 Series Controllers

```
   Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Change active boot image
 4. Clear Configuration
 5. Format FLASH Drive
 6. Manually update images
Please enter your choice:
```

Bootloader Menu for Other Controller Platforms

```
   Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Manually update images
 4. Change active boot image
 5. Clear Configuration
Please enter your choice:
```

Enter **1** to run the current software, enter **2** to run the previous software, or enter **4** (on a 5500 series controller) or **5** (on another controller platform) to run the current software and set the controller configuration to factory defaults. Do not choose the other options unless directed to do so.

Note Only options 1 through 3 are available on Cisco 5500 Series Controllers in FIPS mode.

Note See the Installation Guide or Quick Start Guide for your controller for more details on running the bootup script and power-on self-test.

Fragmented Pings

Cisco 5500 Series Controllers do not support fragmented pings on any interface. Similarly, Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch do not support fragmented pings on the AP-manager interface.

802.11g Controller and 802.11b Clients

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully associate to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, disable any channels (such as channel 14 in Japan) that allow associations from 802.11b client devices.

FIPS 140-2

The Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch have received NIST FIPS 140-2 Level 2 certification. Click this link to view the NIST Security Policies and compliant software versions:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

CAPWAP Problems with Firewalls and ACLs

If you have a firewall or access control list (ACL) between the controller and its access points that allows LWAPP traffic, before upgrading to software release 5.2 or later releases and CAPWAP, you should allow CAPWAP traffic from the access points to the controller by opening the following destination ports:

- UDP 5246
- UDP 5247

The access points use a random UDP source port to reach these destination ports on the controller. In controller software release 5.2, LWAPP was removed and replaced by CAPWAP, but if you have a new out-of-the-box access point, it could try to use LWAPP to contact the controller before downloading the CAPWAP image from the controller. Once the access point downloads the CAPWAP image from the controller, it uses only CAPWAP to communicate with the controller.

Note After 60 seconds of trying to join a controller with CAPWAP, the access point falls back to using LWAPP. If it cannot find a controller using LWAPP within 60 seconds, it tries again to join a controller using CAPWAP. The access point repeats this cycle of switching from CAPWAP to LWAPP and back again every 60 seconds until it joins a controller.

Note An access point with the LWAPP recovery image (an access point converted from autonomous mode or an out-of-the-box access point) uses only LWAPP to try to join a controller before downloading the CAPWAP image from the controller.

Messages Appearing Upon Controller Bootup

Several messages might flood the message logs when the controller boots up. These messages appear because of a failure to read or delete several different configuration files. These are low-severity messages that can safely be ignored. They do not affect controller functionality. These are some examples:

```
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
sshpmInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
bcastInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
```

Web Authentication Redirects

The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Note For Cisco 5500 Series Controllers, Cisco 2100 Series Controllers, and controller network modules, you must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

Cisco 1250 Series Access Points are not supported for use with the Cisco 7920 IP phone. They can, however, be used with the Cisco 7921 and 7925 IP phones.

Crash Files for Cisco 1250 Series Access Points

The Cisco 1250 Series Access Points may contain a bootloader older than version 12.4(10b)JA. Units with old bootloaders do not generate a crash log when a crash occurs. The crash log is disabled so that a crash does not corrupt the flash file system. Units with bootloader versions 12.4(10b)JA or later versions generate a crash log if the access point is associated to a controller running software release 4.2.112.0 or later releases.

New Cisco 1250 Series Access Points shipped from the factory contain new bootloader images, which fixes the flash file system after it is corrupted during a crash (without losing files). This new bootloader automatically sets a new CRASH_LOG environment variable to "yes," which enables a crash log to be generated following a crash but only on controllers running software release 4.2.112.0 or later releases. Therefore, no user configuration is needed to enable a crash log on new Cisco 1250 Series Access Points shipped from the factory.

This example shows how to enable debugging on access point AP01:

```
debug ap enable AP01
```

This example shows how to debug the **show version** command on access point AP02:

```
debug ap command show version AP002
```

Information similar to the following appears:

```
Tue July 06 09:31:38 2010: AP001b.d513.1754: BOOTLDR: C1250 Boot Loader
(C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

This example shows how to display the access point version number:

```
show version
```

Information similar to the following appears:

```
BOOTLDR: C1250 Boot Loader (C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Configuration File Stored in XML

In controller software release 4.2.61.0 and later releases, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore you cannot download a binary configuration file onto a controller running software release 4.2.61.0 or later releases. However, when you upgrade a controller from a previous software release to 4.2.61.0 or later releases, the configuration file is migrated and converted to XML.

Note Do not download a configuration file to your controller that was uploaded from a different controller platform. For example, a Cisco 5500 Series Controller does not support the configuration file from a Cisco 4400 Series or 2100 Series Controller.

In controller software release 4.2 or later releases, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in a binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2 or later releases. However, when you upgrade a controller from a previous software release to 4.2 or later releases, the configuration file is migrated and converted to XML.

Note Controller software release 5.2 or later releases enable you to read and modify the configuration file. See the "Editing Configuration Files" section on page 30 for details. Controller software releases prior to 5.2 do not allow configuration files to be modified. If you attempt to make changes to a 4.2, 5.0, or 5.1 configuration file and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

Uploading Configuration Files

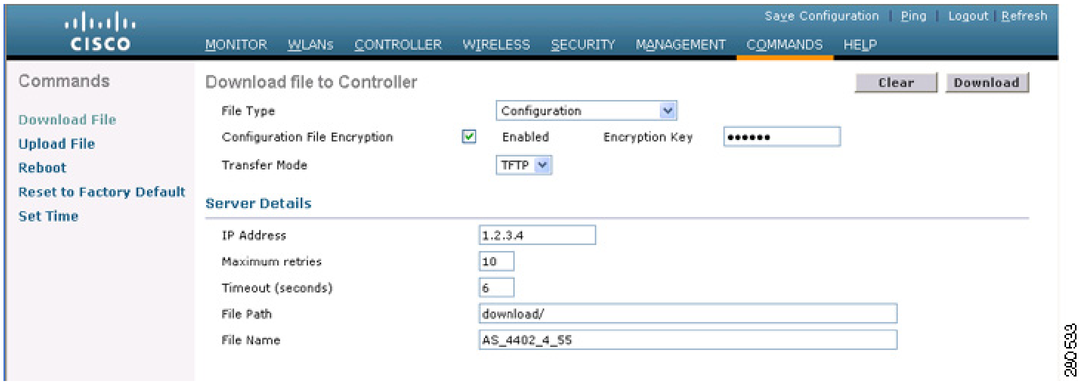
You can upload configuration files using either the GUI or the CLI.

Using the GUI to Upload Configuration Files

To upload a configuration file to a server using the controller GUI, follow these steps:

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page (see Figure 1-1).

Figure 1-1 Upload File from Controller Page



Download file to Controller

File Type: Configuration

Configuration File Encryption: ☑ Enabled Encryption Key: ••••••

Transfer Mode: TFTP

Server Details

IP Address: 1.2.3.4

Maximum retries: 10

Timeout (seconds): 6

File Path: download/

File Name: AS_4402_4_55

Step 2 From the File Type drop-down list, choose **Configuration**.

Step 3 Encrypt the configuration file by selecting the **Configuration File Encryption** check box and entering the encryption key in the Encryption Key text box.

Step 4 From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 5 In the IP Address text box, enter the IP address of the TFTP or FTP server.

Step 6 In the File Path text box, enter the directory path of the configuration file.

Step 7 In the File Name text box, enter the name of the configuration file.

Step 8 If you are using an FTP server, follow these steps:

a. In the Server Login Username text box, enter the username to log into the FTP server.

b. In the Server Login Password text box, enter the password to log into the FTP server.

c. In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 9 Click **Upload** to upload the configuration file to the TFTP or FTP server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

Using the CLI to Upload Configuration Files

To upload a configuration file to a server using the controller CLI, follow these steps:

Step 1 Specify the transfer mode used to upload the configuration file by entering this command:

transfer upload mode {**tftp** | **ftp**}

Step 2 Specify the type of file to be uploaded by entering this command:

transfer upload datatype config

Step 3 Encrypt the configuration file by entering these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to encrypt the file.

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:

transfer upload path *server-path-to-file*

Step 6 Specify the name of the configuration file to be uploaded by entering this command:

transfer upload filename *filename*

Step 7 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the upload occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 8 Initiate the upload process by entering this command:

transfer upload start

Step 9 When prompted to confirm the current settings, answer **y**.

Information similar to the following appears:

```
Mode........................................... TFTP
TFTP Server IP................................. 10.10.10.4
TFTP Path...................................... Config/
TFTP Filename.................................. AS_4402_4_2_55_8_Config.xml
Data Type...................................... Config File
Encryption..................................... Disabled

**************************************************
***  WARNING: Config File Encryption Disabled  ***
**************************************************

Are you sure you want to start? (y/N) y

File transfer operation completed successfully.
```

If the upload fails, repeat this procedure and try again.

Downloading Configuration Files

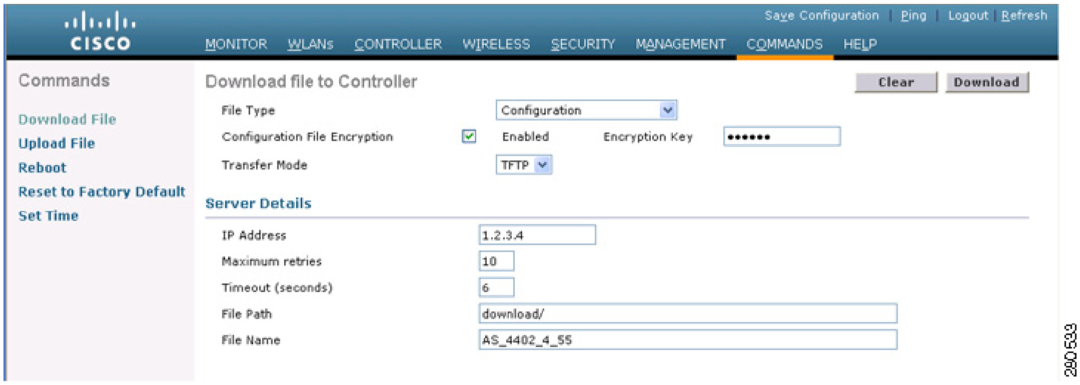
You can download configuration files using either the GUI or the CLI.

Using the GUI to Download Configuration Files

To download a configuration file to the controller using the controller GUI, follow these steps:

Step 1 Choose **Commands** > **Download File** to open the Download File to Controller page (see Figure 1-2).

Figure 1-2 Download File to Controller Page



Download file to Controller

File Type: Configuration

Configuration File Encryption ☑ Enabled Encryption Key ••••••

Transfer Mode: TFTP

Server Details

IP Address: 1.2.3.4

Maximum retries: 10

Timeout (seconds): 6

File Path: download/

File Name: AS_4402_4_55

Step 2 From the File Type drop-down list, choose **Configuration**.

Step 3 If the configuration file is encrypted, select the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the Encryption Key text box.

Note The key that you enter here should match the one entered during the upload process.

Step 4 From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 5 In the IP Address text box, enter the IP address of the TFTP or FTP server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times that the TFTP server attempts to download the configuration file in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the Timeout text box.

Step 7 In the File Path text box, enter the directory path of the configuration file.

Step 8 In the File Name text box, enter the name of the configuration file.

Step 9 If you are using an FTP server, follow these steps:

a. In the Server Login Username text box, enter the username to log into the FTP server.

b. In the Server Login Password text box, enter the password to log into the FTP server.

c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the file to the controller. A message appears indicating the status of the download, and the controller reboots automatically. If the download fails, repeat this procedure and try again.

Using the CLI to Download Configuration Files

To download a configuration file to the controller using the controller CLI, follow these steps:

Note The controller does not support incremental configuration downloads. The configuration file contains all mandatory commands (all interface address commands, mgmtuser with read-write permission commands, and interface port or LAG enable or disable commands) required to successfully complete the download. For example, if you download only the **config time ntp server** *index server_address* command as part of the configuration file, the download fails. Only the commands present in the configuration file are applied to the controller, and any configuration in the controller prior to the download is removed.

Step 1 Specify the transfer mode used to download the configuration file by entering this command:

transfer download mode {**tftp** | **ftp**}

Step 2 Specify the type of file to be downloaded by entering this command:

transfer download datatype config

Step 3 If the configuration file is encrypted, enter these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to decrypt the file

Note The key that you enter here should match the one entered during the upload process.

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:

transfer download path *server-path-to-file*

Step 6 Specify the name of the configuration file to be downloaded by entering this command:

transfer download filename *filename*

Step 7 If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the download occurs:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the *port* parameter is 21.

Step 9 View the updated settings by entering this command:

transfer download start

Step 10 When prompted to confirm the current settings and start the download process, answer **y**.

Information similar to the following appears:

```
Mode............................................. TFTP
TFTP Server IP................................... 10.10.10.4
TFTP Path........................................ Config/
TFTP Filename.................................... AS_4402_4_2_55_8_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

**************************************************
***  WARNING: Config File Encryption Disabled  ***
**************************************************

Are you sure you want to start? (y/N) y

File transfer operation completed successfully.
```

If the download fails, repeat this procedure and try again.

Saving Configurations

Controllers contain two kinds of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to nonvolatile RAM (NVRAM) using one of these commands:

- **save config**—Saves the configuration from volatile RAM to NVRAM without resetting the controller.
- **reset system**—Prompts you to confirm that you want to save configuration changes before the controller reboots.
- **logout**—Prompts you to confirm that you want to save configuration changes before you log out.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP or FTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

To edit the controller's configuration file, follow these steps:

Step 1 Upload the configuration file to a TFTP or FTP server by performing one of the following:

- Upload the file using the controller GUI. Follow the instructions in the "Using the GUI to Upload Configuration Files" section on page 24.
- Upload the file using the controller CLI. Follow the instructions in the "Using the CLI to Upload Configuration Files" section on page 25.

Step 2 Read or edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file.

Note To edit the configuration file, you can use either Notepad or WordPad on Windows or the VI editor on Linux.

Step 3 Save your changes to the configuration file on the server.

Step 4 Download the configuration file to the controller by performing one of the following:

- Download the file using the controller GUI. Follow the instructions in the "Using the GUI to Download Configuration Files" section on page 26.
- Download the file using the controller CLI. Follow the instructions in the "Using the CLI to Download Configuration Files" section on page 27.

The controller converts the configuration file to an XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command:

show invalid-config

Note You cannot execute this command after the **clear config** or **save config** command.

Step 5 If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis. To do so, perform one of the following:

- Upload the invalid configuration using the controller GUI. Follow the instructions in the "Using the GUI to Upload Configuration Files" section on page 24 but choose **Invalid Config** from the File Type drop-down list in Step 2 and skip Step 3.
- Upload the invalid configuration using the controller CLI. Follow the instructions in the "Using the CLI to Upload Configuration Files" section on page 25 but enter the transfer **upload datatype invalid-config** command in Step 2 and skip Step 3.

Step 6 The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

Step 7 Save your changes by entering this command:

save config

LWAPP Mode Changes

When you upgrade to controller software release 5.0.148.0 or later releases, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 6.0.199.0, 6.0.196.0, 6.0.188.0, 5.2.178.0, 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points might not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions transmit multicast frames at the highest configured basic rate and management frames at lowest basic mandatory rates. This can cause reliability problems. Access points running LWAPP or autonomous Cisco IOS should transmit multicast and management frames at the lowest configured basic rate. Such behavior is necessary to provide good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, then it may be useful to shrink the cell size and disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Disabling Radio Bands

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

40-MHz Channels in the 2.4-GHz Band

This is not supported in 6.0.199.0 release.

802.11a Channels 120, 124, and 128 Disabled

802.11a channels 120, 124, and 128 are disabled to achieve compliance with draft EN 301 893 version 1.5.1 on the following -E regulatory domain products: AP1131AG, AP1243AG, and AP1252AG.

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2106 controllers: “Rx Multicast Queue is full on Controller.” This message does not appear on Cisco 4400 Series Controllers because the 4400 NPU filters ARP packets while all forwarding (multicast or otherwise) and multicast replication are done in the software on the 2106.

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 releases, 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.

MAC Filtering for WGB Wired Clients

Controller software release 4.1.178.0 or later releases 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 4.1.185.0 or later releases, 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. We recommend that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Setting the Date and Time on the Controller

Cisco Aironet lightweight access points do not connect to the 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.

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later releases, if a location appliance (release 3.1 or later releases) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, we highly recommend that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* for instructions for setting the time and date on the controller.

Note The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on Greenwich Mean Time (GMT).

FCC DFS Support on Cisco 1130 Series Access Points

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on 1130 series access points 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. The Cisco 1130 Series Access Points with FCC DFS support have an FCC ID *LDK102054E* sticker. The Cisco 1130 Series Access Points without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. The Cisco 1130 Series Access Points that are operating in the United States, Canada, or the Philippines, have an FCC ID *E* sticker, are running the 4.1.171.0 software release or later releases, and can use channels 100 through 140 in the UNII-2 band.

Inaccurate Transmit Power Display

After you change the position of the 802.11a radio antenna for a lightweight Cisco 1200 or Cisco 1230 Series Access Point, the power setting is not updated in the controller GUI and CLI. Regardless of the user display, the internal data is updated, and the transmit power output is changed accordingly. To see the correct transmit power display values, reboot the access point after changing the antenna's position. (CSCsf02280)

Setting the Retransmit Timeout Value for TACACS+ Servers

We recommend 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.
```

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:

- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Add new or modify existing SNMP v3 users
- Install a license, change the license feature set, or change the priority of an AP-count evaluation license on a Cisco 5500 Series Controller

Cisco 2106 Controller LEDs

The Cisco 2106 Series 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.

Rate-Limiting on the Controller

Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). We recommend 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, we recommend that you reapply the **config advanced rate enable** command after testing is complete.

GLBP Not Supported

Controller software release 4.2 or later releases is not compatible with the Gateway Load Balancing Protocol (GLBP). Make sure to configure the controller's default gateway to a fixed address and not to the GLBP virtual address.

Cisco 4400 Series Controllers Do Not Forward Subnet Broadcasts through the Guest Tunnel

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

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.

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 mgmtuser add *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, see the *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.

RADIUS Servers

This product has been tested with CiscoSecure ACS 4.2 and later releases 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.

Using the Backup Image

The controller bootloader 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 2: Run Backup Image** from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the controller.

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.

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, We strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0,* 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, we strongly advise that you change these values. See the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0,* 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 Cisco 2100 Series Controllers

This hardware feature is not supported on Cisco 2100 Series Controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Port mirroring
- AppleTalk

- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Features Not Supported on Cisco 5500 Series Controllers

These software features are not supported on Cisco 5500 Series Controllers:

- For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.
- Asymmetric mobility tunneling.
- Port mirroring.
- Layer 2 access control list (ACL) support.
- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE).

Note The Cisco 5500 Series Controllers bridge these packets by default. If desired, you can use ACLs to block the bridging of these protocols.

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.

2106 Image Not Supported for 3504 Controllers

The 2106 controller image is supported for use with only Cisco 2100 Series Controllers. Do not install the 2106 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Important Notes for Controllers and Mesh Access Points

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

Features Not Supported on Mesh Networks

The following controller features are not supported on mesh networks:

- Multi-country support
- Load-based CAC (Mesh networks support only bandwidth-based, or static, CAC.)

- High availability (fast heartbeat and primary discovery join timer)
- Access point join priority (Mesh access points have a fixed priority.)
- Locally significant certificate
- Location-based services

Caveats

The following sections lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 6.0.199.0. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats

Table 4 lists open caveats in controller software release 6.0.199.0.

Table 4 Open Caveats

ID Number	Caveat Title
CSCtb94670	Controller outputs decrypt error traplog at client reauth timing.
CSCtc03575	The controller fails to redirect web authentication to an external server.
CSCtc05478	The **debug pm ssh-engine enable packet** command is not working.
CSCtd01625	The TLS and SSL security information needs to be updated.
CSCtd70053	Guest mobility anchoring fails when the client roams between two controllers.
CSCtf39826	AP1131 stops responding to the Polycom phone.
CSCtf87279	A-MDSU EAPOL key is sent to the client on reassociation.
CSCtf90579	When using TACACS/RADIUS authentication for lobby admin, an error message appears when you attempt to edit the fields in the created guest user role.
CSCtg41911	The radio stops transmitting packets for several seconds under mc and psp.

Table 4 Open Caveats (Continued)

ID Number	Caveat Title
CSCtg42079	Need to document new world-mode commands in the user guides.
CSCtg45014	The CAPWAP control traffic has incorrect DSCP marking.
CSCtg51702	Degraded voice performance on hreap local switching with TKIP and CCM.
CSCtg59220	Channel utilization climbs quickly with 18 to 20 video clients.
CSCtg62441	Unknown messages are displayed on the controller CLI.
CSCtg96725	The mesh testbed is UP even when the network is disabled.
CSCtg97178	After downgrading, the message "File/Socket handle is Invalid. Handle = 0" appears.
CSCtg98317	The controller displays a message to reboot when it is enabling https.
CSCtg99403	An HREAP group allows an invalid access point MAC address.
CSCth00509	There is some issue with MAC filtering.
CSCth01275	The controller has usability, grammar, and spelling errors.
CSCth01325	The advanced search autonomous access point with 11n support is not working.
CSCth04469	The rogue was autocontained but displayed as manually contained.
CSCth05257	The controller CLI allows you to configure an invalid service port IP address.
CSCth08840	Controller license information displays blank on other than root users.
CSCth09931	An Mbuf-related message appears in the console when the code downloads.
CSCth12916	A wireless client is not getting an IP address when it is associated to the H-REAP access point.
CSCth16351	The instruction on how to use the **show macfilter detail <MAC addr>** command to display the details of a MAC filter entry is not correct.
CSCtg09159	The radio may get stuck when it is in the RESET or DOWN state.
CSCth20570	The Cisco 5500 Series Controller has a known CPU ACL problem.
CSCth20581	The clear counter feature does not work when the counter is disabled in the controller GUI.
CSCsy19477	The wrong messages are showing up on the message log/trap for the guest users.
CSCte24079	The Cisco 2106 Controller LAN hangs after high load with duplex mismatch.
CSCth43447	WiSM crashes on the task "spamReceiveTask".
CSCsz14243	Unable to enable the WLAN while access points are joining.
CSCtc45090	The controller sends the wrong MAC address in an ARP response, which causes mobility flapping.
CSCta40160	The message log is continuously flooded and the "Dropping primary discovery request from an AP has already joined the WLC" message appears.
CSCtc32748	Noise/channel measurements were not done on all the DCA channels.
CSCtb62191	Upon a dot1x wired supplicant PAC refresh, an error message displaying invalid TEAP data appears.
CSCtc10068	Cisco 1140 access points are trying to join the LWAPP controller.

Table 4 Open Caveats (Continued)

ID Number	Caveat Title
CSCtc49270	Clients cannot be deleted from an exclusion list if they are not present in an association list.
CSCte93549	The dot11a radios were not able to pass the traffic since the tx queue was getting filled.
CSCtd99602	When the wired guest users trigger a web authentication page for the first attempt to browse the http server, the Web Auth Page displays and when the user logs in, the session expires.
CSCtd86886	Wism generates a traceback in the message log file.
CSCtd90304	The error %MM-3-MEMORY_READ_ERROR: mm_mobile.c:464 Error reading mobility appears across controllers on WiSM blades.
CSCtd62937	The **show ap summary** command does not show the access point names.
CSCte55370	The controller crashes during the ping of virtual devices.
CSCte38645	The RADIUS attribute NAS-Port (5) is not included in the access request for web authentication.
CSCte39477	The external Web Servers field needs to be always displayed in the controller GUI.
CSCte43427	Webauth authentication is allowed for MAC filter entries and non netusers.
CSCtb16583	An access point changes from static IP to DHCP and does not revert back to static.
CSCtf90722	ACL on WLC4400/WiSM can cause low throughput and packet loss.

Resolved Caveats

Table 5 lists caveats resolved in controller software release 6.0.199.0.

Table 5 Resolved Caveats

ID Number	Caveat Title
CSCtf63030	Radio get stuck when it is in the RESET or DOWN state.
CSCta91358	HREAP is locking up due to a wedge input queue on the radio interface.
CSCtb02136	AP1252 with AP groups and HREAP do not broadcast SSIDs.
CSCth05209	An OEAP configuration option needs to be removed in an unsupported platform.
CSCth02673	Errors occur when you apply the WLAN template with security as the WEP.
CSCtg93517	The wrong error message appeared while the H-REAP access point was added to a different H-Group.
CSCsx62302	REAP VLAN support mapping on an access point is lost when you upgrade from 4.2.176 to 6.0.182.
CSCtg93928	A traceback occurred on the mesh access point.
CSCsy90434	The controller command line displays that diversity was enabled for the 1522a radio.

Table 5 Resolved Caveats (Continued)

ID Number	Caveat Title
CSCtg94715	Lock Assert dtlARPTask has caused the Cisco 5500 Series Controller to crash.
CSCtg74904	The Cisco 1142 Access Point stopped transmitting and receiving on its radio.
CSCth11525	A WLAN gets disabled after you add a new SSID to an existing access point group.
CSCsy93463	Debug the output through Telnet and SSH sessions.
CSCsy99905	RLDP constantly finds wired threats only when manually used.
CSCth09687	The controller GUI has a problem when configuring new ACL rules.
CSCsz19203	The controller crashes at SSHpmMainTask.
CSCsz37520	Noise was not factored in Channel Util calculations for AP1140.
CSCsz38828	AMAC radio core dumps: the transmitter has stopped working.
CSCsz40659	Need to reboot the wireless controller after an upgrade.
CSCsz42048	An inconsistency has occurred in the neighbor RSSI measurements.
CSCsz84895	An association response has the wrong set of supported rates for the 11b device.
CSCta04008	The call station type on the controller does not state that it is applicable to non-802.1X devices only.
CSCta13941	An access point is rejecting the association request with the status code 13.
CSCta34765	The controller console displays that invalid behavior occurred when you entered the **config mirror port** command.
CSCta41584	The backup port was not active when the primary port was disabled on the controller.
CSCta49375	The Cisco 4404 Controller crashes when you restart the sig11 at nPCSL_timer.
CSCta58642	LAP1252-P seems to have violated the maximum power levels in the regulatory domain.
CSCta71448	Reduce the severity of the error msg: %APF-1-CHANGE_ORPHAN_PKT_IP.
CSCtb20125	CCMP displays errors when the radio configuration is changed.
CSCtb34971	When the Controller WISM loads third-party certificates for web authentication, HTTPS port 443 is disabled.
CSCtb39368	The webauth custom page fails with some file extensions.
CSCtb39612	The WGA two device solution displays the “Cannot find MSCB for NPU SCB on console” message.
CSCtb42260	Enabling broadcast forwarding versus multicast forwarding through the controller CLI.
CSCtb44059	The controller should send the DHCP packets to the proper DHCP server.
CSCtb45178	Insufficient memory or a traceback occurred on AP1130 and AP1232.
CSCtb63297	A file read error message was reported in message log.
CSCtb69778	The output of the **show log ip-port hash** command was not correct in Telnet or SSH sessions. Instead, the output displayed results in the console window.
CSCtb92872	The WiSM with no access points crashed and the controller is unresponsive and you have to reset the hardware module to bring it up.

Table 5 Resolved Caveats (Continued)

ID Number	Caveat Title
CSCtc01748	The Controller 2106 kernal panic crashed and hung while running combination stress test.
CSCtc13337	Even after the clients are associated to the controller, the message log displays an error saying no ACLS was defined on the controller.
CSCtc13378	The Cisco 5508 Controller crashed on the apfProbeThread.
CSCtc22661	An MFP anomaly was detected on deauthenticated frames.
CSCtc23210	MC2UC: Fragmentation has caused fewer clients to connect.
CSCtc23277	Radio driver is consuming all of the WLAN pool buffers.
CSCtc23789	The AP 1140 and 1250 radios were down and the interface was stuck in the reset state.
CSCtc29509	A predownload of the image has stopped after completing 18 out of the 230 access points on the controller.
CSCtc41797	RLDP does not work for G-only APs.
CSCtc44480	The access points were still transmitting ad-hoc deauths even after auto-contain was disabled.
CSCtc50424	The Cisco 5500 controller crashes and an error message “cond pbuf->dataLen <= 2048 failed” appears in the crashlog.
CSCtc51076	The “config spanningtree port mode off” settings are not saved in the backup configuration file.
CSCtc57611	Delay in Music on Hold on 7925 with HREAP AP.
CSCtc67372	On the controller with some access points, the SSH/Telnet session hangs with sh run output with paging disabled.
CSCtc73503	The radios are showing a Tx power level of 0.
CSCtc73527	Low latency MAC is not supported on the 802.11n APs.
CSCtc90985	The DMA input queue is overrun by fast Ethernet bursts.
CSCtc95434	An FTP transfer does not work on Cisco 2100 Controllers.
CSCtc97144	The 1800-seconds session that occurs after the session timeout has been fixed when H_REAP is in the standalone mode.
CSCtc97595	Only one of many gratuitous ARP packets is forwarded to the client.
CSCtd04572	Video metrics fixes and enhancements.
CSCtd06186	Directed broadcast does not work when IGMP snooping is enabled.
CSCtd21859	WLAN CKIP PSK is deleted when the Apply button is applied.
CSCtd23497	1242 AP HREAP Mode crashes after%CAPWAP-5-CHANGED the state to Join.
CSCtd26168	Incorrect source MAC address in the ARP request when the controller is in lag mode.
CSCtd26794	5508 DP was crashing and fragmentation consumes all pbufs.
CSCtd28542	The controller was crashing on EmWeb due to an access point configuration change.
CSCtd28757	The LDAP user password length needs to be increased.

Table 5 Resolved Caveats (Continued)

ID Number	Caveat Title
CSCtd30669	WLAN security settings and session timeouts are changed after restoration.
CSCtd59231	The master bit configuration was not saved in xml.
CSCtd60522	The configuration backup adds the wrong 802.11a channel list.
CSCtd72649	The Cisco 4400 Controller crashes at osapi_task.c:3660.
CSCtd74472	The Cisco 5500 Controller crashes with the OSAPI reaper task and throws a null tunnel pointer exception.
CSCtd75089	The controller needs to have the **“devshellsysapiDumpMbufStatus”** command to show mbuf usage.
CSCtd75094	The access point crashed while clearing the CAPWAP MGIDs for the new client.
CSCtd86901	The mobility anchor configuration for WLAN is lost while copying the configuration through auto installation.
CSCtd92105	The controller reloads and the DHCP task reaper is reset.
CSCtd97011	When the AMAC radio core dump is observed, the neighbor discovery frames are stuck.
CSCtd99288	The client authentication trapflag cannot be configured through the CLI.
CSCtd99659	An SNMP agent inserts null data during the mesh link test.
CSCte08090	A TFTP upload fails while trying to upload a packet capture to the Windows TFTP server.
CSCte19262	The client is deauthenticated after the key exchange and displays an error message “Unable to locate AP 00:00:00:00:00:00”.
CSCte27052	An inconsistency in the AAA Override feature occurred.
CSCte36493	The controller GUI displays a guest LAN error when the ingress is set to None on the anchor WLAN controller.
CSCte43508	5508 DP CRASH: buffer leaks due to ARP storm.
CSCte51177	The SNMP TRAP port number is not reflected in the configuration file of the controller.
CSCte55458	The web authentication page takes a long time to display under a heavy load.
CSCte62815	The Cisco 5508 Controller is not passing OSPF multicast traffic.
CSCte74879	The controller 5508 agentSwitchInfoPowerSupply MIB was not working.
CSCte76854	Unable to enable a WLAN on the Cisco 5508 Controller.
CSCte78472	An invalid PHY rate is returned on an ADDTS response.
CSCte79131	Containment details for the ad-hoc rogue is incorrect in the controller GUI.
CSCte79305	Auto containment for wired rogue access points does not contain wired rogues.
CSCte81420	When the access point crash was in process, the message “Dot11 driver” dot11_rate_is_allowed appears.
CSCte89891	The radio stops transmitting beacons periodically.
CSCte90918	WiSM locks-up during the upgrade with a full load of access points and clients.
CSCte92365	The auto immune attacks fix does not cover the incorrectly formatted association request.

Table 5 Resolved Caveats (Continued)

ID Number	Caveat Title
CSCte95626	The Cisco 5508 Controller was not forwarding 100% of packets for the Gigabit line burst.
CSCte96140	Ethernet bridging breaks when the Ethernet interface of AP 1242 is flapped.
CSCtf03121	An optical SFP misconnect causes the Cisco 5508 Controller to disable its ports.
CSCtf03958	The WLAN Load Balance and Band Select should display Global Disabled as apply.
CSCtf06314	The WCS access point current associate client list is not up to date.
CSCtf06931	The controller emWeb crashes while running the ewaFormSubmit_blacklistclient_list.
CSCtf08553	The system log is not sent to the server that is on the same subnet as the dynamic interface.
CSCtf23682	An access point cannot join with the multicast MAC address as the gateway (checkpoint).
CSCtf27580	The Ethernet interface input queue wedge is from the broadcast/uniGRE traffic.
CSCtf28217	An access point unexpectedly joins the controller in bridge mode instead of local mode or H-REAP.
CSCtf33859	The client state is run with no IP address.
CSCtf34858	The client cannot transmit the traffic if it reassociates to an access point within 20 seconds.
CSCtf36051	The CPU ACL is not filtering after a reload.
CSCtf50921	Acct-Input-Octets counters do not reset for every accounting stop.
CSCtf53521	Directed broadcast does not work when the IGMP snooping is enabled.
CSCtf71637	The username entry in the accounting stop did not match the accounting start.
CSCtf94670	emWeb task crashed at usmWebGetSfpType.
CSCtf94679	The used memory increases by 25-MB immediately after bootup.
CSCtg10321	The Cisco 5500 controller crashes when all ports are disabled.
CSCtg34627	The video queue constrain limit allows only 9 to 10 clients of the 5-Mb stream.
CSCtg55102	AssocFailPayload causes a payload error at the controller.
CSCtg98413	There is a discrepancy between the help on the CLI and the actual code.
CSCth00490	The Dyn-int template with secondary port of 7 is getting applied while applying a dynamic interface.
CSCth02608	RRM RF group Leader Election did not occur.
CSCte55219	AMC radio core dumps with reason “transmitter seems to have stopped” due to a large number of uplink frames in the inprog queue.
CSCtf69598	There is a memory leakage in the access point upon a CCKM failure.
CSCtg71658	Access point level resets to 0 while upgrading from 5.0 to 6.0.
CSCtf65636	The access points that are crashed from the data TLB misses exception.
CSCth16398	Downloadable logs should include primaries.
CSCtd43906	RAP, which is a mesh access point, does not recover after the radar was detected.

Table 5 Resolved Caveats (Continued)

ID Number	Caveat Title
CSCtf84965	CCKM roam fails with OEAP.
CSCtg89404	Association response to client is sent with AID 0.

If You Need More Information

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

http://tools.cisco.com/Support/BugToolKit/

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

Troubleshooting

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

http://www.cisco.com/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, see these documents:

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.