Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 6.0.188.0

Last Revised: November, 2009

These release notes describe open and resolved caveats for software release 6.0.188.0 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 6.0.188.0 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 6.0.170.0
- Cisco WCS Navigator 1.5.170.0
- Location appliance software release 6.0.97.0
- Cisco 2700 Series Location Appliances
- Mobility services engine software release 6.0.97.0 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 6.0.188.0 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 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

The following new features are available in controller software release 6.0.188.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* for more details and configuration instructions.

AP Image Predownload

This feature allows you to download the upgrade image to the controller, then download the image to the access points while the network is still up. A new CLI allows you to specify the boot image for both devices and to reset the access points when the controller resets.

Ability to Limit AP Transmit Power

You use this feature to configure the maximum or minimum transmitting power limits that will used by dynamic power assignment for a given radio.

RRM will chose the closest power level avaible on the radio when using these configured limits. For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm unless the access point is configured manually.

RRM Fixes for Medical Devices

This feature improves the way that QoS interacts with the RRM scan defer feature. In deployments with certain power-save clients, you sometimes need to defer RRM's normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information).

You can use a client's WMM UP marking to tell the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Use this controller CLI command to configure this feature for a sepcific WLAN:

config wlan channel-scan defer-priority *priority* [**enable | disable**] *WLAN-id*

where *priority* = 0 through 7 for user priority (this value should be set for 6 on the client and on the WLAN).

Use this command to configure the amount of time that scanning will be deferred following an UP packet in the queue:

config wlan channel-scan defer-time *msec WLAN-id*

Enter the time value in miliseconds (ms); the valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.

You can also configure this feature on the controller GUI by selecting WLANs, and either editing an existing WLAN or creating a new one. On the WLANs > Edit page, click the **Advanced** tab. Under Off Channel Scanning Defer, select the scan defer priorities and enter the defer time in milliseconds.

Note Off Chanel Scanning is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off Channel Scanning is responsible for rogue detection. Devices that need to defer Of f Channel Scanning should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that off-channel scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off Channel Scanning, such as monitor access points, or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they where received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. These are the marking results of each QoS policy:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

Inter-Release Controller Mobility (IRCM)

This feature supports seamless mobility and Cisco Unified wireless network (CUWN) services across controllers with different software versions.

CUWN Service	4.2.x.x	5.0.x.x	5.1.x.x	6.0.x.x
Layer 2 and Layer 3 Roaming	X	–	–	X
Guest Access/Termination	X	X	X	X
Rogue Detection	X	–	–	X
Fast Roaming (CCKM) in a mobility group	X	–	–	X
Location Services	X	–	–	X
Radio Resource Management (RRM)	X	–	–	X
Management Frame Protection (MFP)	X	–	–	X
AP Failover	X	–	–	X

Note IRCM is supported on GD releases only; ED releases, such as 5.2.x, are not supported.

RRM is supported between controllers running different versions of code. However, different RF groups will form for the controllers running different code levels. Therefore, separate RF groups do not have the ability to interact with one another, resulting in two groups of radios calculating power and channel separately.

The effect on the network depends on how close the two RF groups are to one another. For example, if you have two controllers, one running software release 4.2.X.X and one running software release 6.0.X.X, and both controllers service access points that are on the same floor, there will be some impact at the boundary between the two groups of access points on channel and TX power decisions.

If you implement on neighboring floors, the result might be greater channel overlap (interference among access points), but TX power would likely not be affected. Non-neighboring floors would be fine. Implementing mixed controllers releases in a random deployment would likely result in significant issues with TX power assignments but would have a minor impact on channel assignments.

Aggressive Load Balancing Enhancement

The enhancement to Aggressive Load Balancing allows you to configure load balancing per WLAN. In previous releases, load balancing was configured globally. Use this CLI command to configure load balancing for a specific WLAN:

config wlan load-balance allow *wlan*

Band Direction

The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. You can use this feature to combat these sources of interference and improve overall network performance. Band direction enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

Using the controller CLI **config band-select** and **config wlan band-select** commands, you can globally enable band selection on the controller, or you can enable or disable band selection for a particular WLAN. This is useful if you want to disable band selection for a select group of clients (such as time-sensitive voice clients).

Transaction Power Level Assignment

The TPC algorithm balances RF power in many diverse RF environments. Automatic power control may not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings only apply to access points that are attached to a controller from which they are configured; it is not a global RRM command. The default settings disable this feature, and you should use care when overriding TPC recommendations.

The range for these parameters is -126 to 126 dBM. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

Software Release Information

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

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

Note 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.

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, 12.2(37)SE or later, 12.2(44)SE or later, or 12.2(46)SE or later. 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.

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 6.0.188.0

Caution Before upgrading your controller to software release 6.0.188.0, 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 6.0.188.0, 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 6.0.188.0 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 6.0.188.0 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 6.0.188.0. Table 1 shows the upgrade path that you must follow before downloading software release 6.0.188.0.

Table 1 Upgrade Path to Controller Software Release 6.0.188.0

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

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

- Cisco recommends that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file on all controller platforms. 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	—
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	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[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. These access points are not supported in the 4.2, 5.0, or 5.1 Release trains.

Special Rules for Upgrading to Controller Software 6.0.188.0 in Mesh Networks

Caution Before upgrading your controller to software release 6.0.188.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 3 outlines the upgrade compatibility of controller mesh and non-mesh 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 4.1.192.135M 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. Cisco recommends that you save the configuration from the mesh release before upgrading to release 6.0.188.0 for the first time. Then you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 6.0.188.0 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 upgrade from a mesh release to controller software release 6.0.188.0. 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 6.0.188.0, 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 6.0.188.0. 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 Non-Mesh Releases

Upgrade to / Upgrade from	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
4.1.192.35M		Y	Y																								
4.1.192.22M		Y	Y	Y																							
4.1.191.24M				Y	–																						

Table 3 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases (continued)

Upgrade to	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
4.1.190.5				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 Non-Mesh Releases (continued)

Upgrade to	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. 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 5500 series controllers can download the 6.0.188.0 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, 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, 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 6.0.188.0, 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 Do not install the 6.0.188.0 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; then install the other file and reboot the controller.

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

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

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

Step 2 Follow these steps to obtain the 6.0.188.0 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:

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. Cisco recommends 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 6.0.188.0 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 Click **Commands** > **Download File** to open the Download File to Controller page.

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

Step 8 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.

Note Do not wait to reboot the controller. Reboot it immediately after downloading the software. Otherwise, the access points might start downloading the software before the controller is running it.

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 6.0.188.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Re-enable the WLANs.

Step 20 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 21 Re-enable 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 6.0.188.0 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

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

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

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

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

Using the Cisco 5500 Series Controller USB Console Port

The USB console port on the 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 the Microsoft website

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 Non-Mesh Access Points

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

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-thru 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, 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 2100 series controllers and controller network modules and up to 192 access point groups for 4400 series controllers, 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 5500 series controllers are different than for other controller platforms.

Bootloader Menu for 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 5500 series controllers in FIPS mode.

Note Refer to 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 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 5500 series controllers, 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 1250 Series Access Points

The 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 generate a crash log if the access point is associated to a controller running software release 4.2.112.0 or later.

New 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. Therefore, no user configuration is needed to enable a crash log on new 1250 series access points shipped from the factory.

These examples show the output from the CLI commands (in bold) that you use to check the bootloader version on lightweight and autonomous 1250 series access points:

Commands entered on the controller CLI:

debug ap enable AP001b.d513.1754

debug ap command "show version | include BOOTLDR" AP001b.d513.1754

```
Thu Apr 23 09:31:38 2009: AP001b.d513.1754: BOOTLDR: C1250 Boot Loader
(C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Command entered on the access point CLI:

show version | include BOOTLDR

```
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, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. When you upgrade a controller to 4.2.61.0 or a later software release, the binary configuration file is migrated and converted to XML.

Note You cannot download a binary configuration file onto a controller running software release 6.0.188.0. Also, do not attempt to make changes to the configuration file. If you do so 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.

Note You cannot modify the configuration files for 2000, 4000, and 4100 series controllers. The ability to modify configuration files is available in controller software release 5.2 or later, and these controllers support only earlier software releases (up to the 4.2 release for 2000 series controllers and up to the 3.2 release for 4000 and 4100 series controllers).

LWAPP Mode Changes

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

If you downgrade from controller software release 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

Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference is likely to occur.

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.

Impact of External Antenna Gain on Transmit Power

In controller software release 4.2 or later, external antenna gain is factored into the maximum transmit power of the access point. Therefore, when you upgrade from an earlier software release to 4.2 or later, you might see a decrease in transmit power output.

Supporting Oversized Access Point Images

Controller software release 4.2 or later allows you to upgrade to an oversized access point image by deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB.

Note As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Follow these steps to recover the access point using the TFTP recovery procedure.

Step 1 Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you may remove the TFTP server.

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

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, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, Cisco highly recommends 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 5.2* 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 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. 1130 series access points with FCC DFS support have an FCC ID *LDK102054E* sticker. 1130 series access points without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. 1130 series access points that are operating in the United States, Canada, or the Philippines; have an FCC ID *E* sticker; and are running the 4.1.171.0 software release or later 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 1200 or 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

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

Configuring an Access Point's Prestandard Power Setting

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

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

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

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

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

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

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

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 5500 series controller

2106 Controller LEDs

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

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

Rate-Limiting on the Controller

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

Pings Supported to the Management Interface of the Controller

Controller software release 4.1.185.0 or later is designed to support ICMP pings to the management interface either from a wireless client or a wired host. ICMP pings to other interfaces configured on the controller are not supported.

Pinging from a Network Device to a Controller Dynamic Interface

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

GLBP Not Supported

Controller software release 4.2 or later 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.

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

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

Connecting 1100 and 1300 Series Access Points

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

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

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

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

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

"ERROR!!! Command is disabled."

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

Exclusion List 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 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, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* 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 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

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

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- VPN passthrough option

  Note You can replicate this functionality on a 2100 series controller by creating an open WLAN using an ACL.

- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Spanning Tree Protocol (STP)
- Port mirroring
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Features Not Supported on 5500 Series Controllers

These software features are not supported on 5500 series controllers:

- Static AP-manager interface

Note For 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
- Spanning Tree Protocol (STP)
- Port mirroring
- Layer 2 access control list (ACL) support
- VPN termination (such as IPSec and L2TP)
- VPN passthrough option

Note You can replicate this functionality on a 5500 series controller by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)

Note The 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 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.

Running a 3504 Image on a 2106 Series Controller

It is possible to run a 3504 controller image on a 2106 series controller, but Cisco Aironet 1130, 1200, and 1240 series access points will not be able to connect to the controller.

Upgrading External Web Authentication

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

1. For 5500 series controllers, 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.
2. For 4400 series controllers and the Cisco WiSM, instead of using a preauthentication ACL, the network manager must configure the external web server IP address using this command:

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

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

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

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

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

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

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

function loadAction(){
     var url = window.location.href;
     var args = new Object();
     var query = location.search.substring(1);
     var pairs = query.split("&");
     for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
```

```
          args[argname] = unescape(value);
     }
     //alert( "AP MAC Address is " + args.ap_mac);
     //alert( "The Switch URL is " + args.switch_url);
     document.forms[0].action = args.switch_url;

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

}

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

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

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

<tr align="center">

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

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

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

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)
- EAP-FASTv1 and 802.1X authentication
- Access point join priority (Mesh access points have a fixed priority.)
- Locally significant certificate
- Location-based services

Caveats

The following sections lists open and resolved caveats for Cisco controllers and lightweight access points for version 6.0.188.0. 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:

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

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

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

Open Caveats

Major Open Caveats

Table 4 lists major open caveats in controller software release 6.0.188.0.

Table 4 Major Open Caveats

ID Number	Caveat Title
CSCtc14910	AP 1140 not joinning WLC and logging tracebacks.
CSCtc22700	AP 1240 beacons getting disabled while probes enabled on WLC 6.0.182
CSCtc70615	AP1142 reset from watchdog timer expired
CSCtc70838	AP radio UP transmitting only beacons
CSCtc85444	WLC locks up on SNMP task when pushing AP Group template from WCS
CSCtg81397	External webauth is broken in HREAP local switching.

Moderate Open Caveats

Table 5 lists moderate open caveats in controller software release 6.0.188.0.

Table 5 Moderate Open Caveats

ID Number	Caveat Title
CSCtc31663	Wism running 6.0 hangs due to memory leak
CSCtc41293	Controller doesn't act upon receiving ICMP fragmented needed packet
CSCtc44480	H:APs transmitting ad-hoc deauths even after auto-contain is disabled
CSCtc52255	6.0 1522 on non-dfs backhaul channel changes channels after radar event
CSCtc52412	Issue with client mobility across SSIDs on the same radio
CSCtc68378	Choppy Multicast MOH to 7925 with severe packet loss on HREAP
CSCtc14970	1121 shows high channel utilization until it is reset
CSCtb96750	AP Fallback causes client drop with HREAP
CSCta06193	CCXv5: RF Parameters values do not match with CCXv5 Specification
CSCta91358	H-REAP locking up due to wedge input queue on radio interface.
CSCtb17261	NEC: 802.11x re-auth failed to associate w/AP due to EAPOL-key timeout
CSCtb74239	WISM crashed on task sshpmMainTask System Crash
CSCtc05478	deb pm ssh-engine enable packet not working
CSCtc10068	1140 APs trying to join LWAPP controller.
CSCtc13378	5508 Systemcrash on apfProbeThread
CSCtc23789	AP1140/1250 radio down - interface stuck in reset
CSCtc32748	Noise/Channel measurements not done on all DCA channels
CSCtc37889	LAP can't join when static IP address is configured
CSCtc49270	Clients can't be deleted from exclusion list if not present in ass. list
CSCtc57611	Delay in Music on Hold on 7925 with HREAP AP
CSCtc67372	Sh run/sh tech hangs on SSH with paging disabled
CSCtc73414	AP not generating trap during radio UP -> radio DOWN transition

Table 5 Moderate Open Caveats (continued)

ID Number	Caveat Title
CSCtc73527	Make Low Latency MAC a no op for 11n APs, till CSCsy66246 is addressed
CSCtc82624	CISCO-LWAPP-AP-MIB Missing trap definitions
CSCtc87659	AP console does not display if it got controller address from DHCP
CSCtc91742	AP radio may go down
CSCtc95434	FTP transfer does not work on 2100
CSCtc97078	Memory corruption in CAPWAP 1130
CSCtc97115	Memory corruption in 1230 capwap (WLC 6.0.182.0)
CSCtc97144	Fixed 1800 sec session timeout when H-REAP standalone mode

Table 6 lists minor open caveats in controller software release 6.0.188.0.

Table 6 Minor Open Caveats

ID Number	Caveat Title
CSCsd96350	Should allow clearing internal-dhcp lease
CSCsv21441	Wireless controller unicast arp issues with redundant gateways
CSCta77755	Not able to backup/transfer third party certificates
CSCta93754	Unable to upload customized web bundle from WLC
CSCtc58032	Add watchdog to monitor for admin UP and radio DOWN or RESET state
CSCtf90722	ACL on WLC4400/WiSM can cause low throughput and packet loss.

Resolved Caveats

Table 7 lists caveats resolved in controller software release 6.0.188.0.

Table 7 Resolved Caveats

ID Number	Caveat Title
CSCsm19182	GH DFS triggered , D1 interface down with no channel available
CSCsy95660	1140: Tx lockup with beacons enabled probes disabled after rate config
CSCsz64049	WLC crash - nf_iterate causes kernel panic/exception
CSCta40728	OEAP Alpha WLC's crashed
CSCsm19182	GH DFS triggered , D1 interface down with no channel available
CSCsy95660	1140: Tx lockup with beacons enabled probes disabled after rate config
CSCso36248	LDAP username limited to 24 characters in 4.2.112.0
CSCsy30722	next hop address stored in capwap doesn't get updated on rcving GRAT ARP
CSCsy80680	Client stuck in 8021X_REQD state after mobility event
CSCsy97077	WLC Controller 'show run-config' is truncated, not complete, incomplete

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz12429	H: marvell xmtter stopped due to stuck AMSDUs for a deleted client
CSCsz48244	4.2 Mobility Control path flapping up/down
CSCsz71946	Lethium: DOT11-4-CCMP_REPLAY: AES-CCMP TSC replays seen in alpha nw.
CSCsz80820	Primary Discovery Request not processed for AP priority scenario
CSCsz87643	Management interface unreachable via different subnet
CSCsz90584	Group Transmit Key does not always refresh when expected
CSCsz92558	Ethernet interface stats of AP are not displayed for non-mesh APs on WLC
CSCta03016	4404 Controller crash in 5.2.188.0 image
CSCta05979	WLC can't do LDAP auth with AD when AD messages contain searchResRef
CSCta09160	Need 802.1q tag in EoIP tunnel to be the same between controllers.
CSCta29484	Radio stops beaconing for 10-second period
CSCta32912	WLC 5508 - SFP Validation mechanism may rejects Cisco sold SFP's
CSCta34714	D3 Web-auth redirections fails during failover scenarios
CSCta42012	Mesh - Root AP do not recreate subinterface at fallback
CSCta53985	Mac Filtering with WPA doesn't authenticate with external Radius Servers
CSCta67367	After downloading configuration file, original configuration was no
CSCtb02314	AP Fallback fails to primary when using CAPWAP / LWAPP WLC in same MG
CSCtb06469	c1200 APs locks up due to possible memory leak
CSCtb12031	1142 / 1252 inconsistently ACKs Vocera (gen1) badge.
CSCtb27438	Rogue Ad-Hoc is detected as rogue AP
CSCtb29243	ARP storm on inter-controller NAC scenario for quarantined client
CSCtb50732	Reaper Reset on osapiBsnTimer
CSCtb58091	WLC CPU Spike with emWeb - Controller Not Responding - No crash
CSCtb64994	Intermittent Webadmin and Webauth access on WiSM running 5.2.193
CSCtb67889	GUI does not match CLI functionality for broadcast/mulitcast forwarding
CSCtb74037	snmp walk shows password for entire group
CSCtb75305	WLC lets all WEBAUTH_REQD traffic through
CSCtb83470	AP 1252 intermittently only sends 2 buffered multicast pkts per DTIM
CSCtb87326	Enabling NAT Address and TACACs crashes 5508
CSCtb96750	AP Fallback causes client drop with HREAP
CSCtc15346	AP1252 fails to retransmit missing AMPDU packet in response to block ack
CSCtc54572	Crash on 1240 in CDP processing, AP on third-party switch
CSCsz12429	H: marvell xmtter stopped due to stuck AMSDUs for a deleted client
CSCsz90584	Group Transmit Key does not always refresh when expected
CSCsz92558	Ethernet interface stats of AP are not displayed for non-mesh APs on WLC

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCta29484	Radio stops beaconing for 10-second period
CSCta42012	Mesh - Root AP do not recreate subinterface at fallback
CSCtb02314	AP Fallback fails to primary when using CAPWAP / LWAPP WLC in same MG
CSCtb06469	c1200 APs locks up due to possible memory leak
CSCtb27438	Rogue Ad-Hoc is detected as rogue AP
CSCsq63937	WLC: SNMP object agentTransferUploadMode can be set to null
CSCsr10874	Additional client stats
CSCsu70287	Low Upstream/ bi-dir tput for large packet sizes, 512 - 1400 byte pkt
CSCsx41062	WLC rejects apparently valid NTP packets
CSCsx62293	Misleading error message when enabling/disabling 802.11g network on 5.2
CSCsx71175	WLC broadcast dhcp does not comply with RFC 1542
CSCsx94354	AP rejects DHCP offer with bad option 7 (log server) value
CSCsy16021	Local EAP: Checkbox needed on wlan to enable/disable local/remote Auth
CSCsy17745	"lwapp ap" CLI always returns "ERROR!!! Command is disabled."
CSCsy24030	Make world-mode changes persistent (CSCsy15893)
CSCsy71912	Duplicated redirect URL with Web Auth and Proxy Server
CSCsy71960	1242 AP ignores primary WLC to join wrong WLC
CSCsy83568	DHCP Debug output not as verbose as internal scope vs. external
CSCsz10515	H: Beta: CLI Truncated
CSCsz27295	GH: rogue containment packets sent even though rogue containment off
CSCsz31934	WLC forwards traffic from WLAN to MAC-spoofing wireless client
CSCsz32424	Rogue not detected on wire using the arp
CSCsz49863	WLC Local EAP auth periodically fails with 792x phone using EAP-FAST
CSCsz53516	DHCP fallback with static IP takes 4 hrs
CSCsz53825	WLC shows medium power for AP1250 even when switch provides 20W
CSCsz56454	WLC traplogs flagging Cisco AP's as impersonators
CSCsz58917	Radio Reset messages with RLDP
CSCsz62286	GH: ARP fails for default GW of mgmt int, which is the virtual HSRP GW
CSCsz67652	DOT11-3-RADIO_INVALID_FREQ_FOR_CHAN Frequency not found 133
CSCsz72416	Unexpected vlan is assigned due to failed to aaa override
CSCsz76796	PMK cache isn't updated
CSCsz78168	APs on same controller in same mobility group reported as rogues
CSCsz79621	Inter frame delay causing reassembly issues, breaking EAP-TLS auth
CSCsz80918	debug capwap not filtered by mac address
CSCsz82548	Clients can communicate even though clients auth status is "No"

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz88122	AIR-WLC4404-100-K9 crashed with a reason of Reaper Reset at task sshpmM
CSCsz88241	Per user bandwidth contracts stop functioning
CSCsz95595	Permit all IOS CLI commands in TELNET/ssh sessions
CSCta03125	No CLASS in accounting if user assoc after idle-timeout with PMKID
CSCta04267	Show certificate summary wrongly indicates third party cert installed
CSCta06244	WLAN configuration not same when downloading backup config via TFTP
CSCta08186	WLC doesn't support case-sensitive dynamic interfaces
CSCta09996	Sometimes LAP can't join to WLC via alternative port in port redundancy
CSCta11373	Unable to create guest user via lobby admin account on WLC GUI
CSCta17517	SIM-3-PORT messages aren't generated with LAG mode.
CSCta28431	On reboot dot1x credentials are not saved on 1140 APs registered to WLC
CSCta28666	Config mesh linktest RSSI output is wrong.
CSCta28829	6.0 WLC mac-delimiter keeps getting reset to 'hypen' after a reboot
CSCta30165	Provide backwards compatible option for letter case of call station id
CSCta34294	RFID Sequence Control is zero
CSCta38050	GUI /screens/spam/cell_list.html no longer has Port column
CSCta45032	New filed in WEB UI to show if a rogue was contained manually or not.
CSCta45156	Upgrade to 6.0.182.0 Webauth login page text views as one long sentence
CSCta47390	Need to clarify error message for anchor and IPV6 configuration
CSCta49183	Speed/duplex configuration is not available via the CLI for the WLC
CSCta52813	--More-- or (q)uit prompt in sh run-config does not stop the output
CSCta54945	LDAP bind password limited to 24 characters due to CSCso36248
CSCta58254	5.2.157.0 ER.aes is lost after Boot Option 5
CSCta64876	Site Override Setting and invalid value 0 for WLAN
CSCta75636	WLC does not allow 24 mobility group members
CSCta78236	Change min/max rogue RSSI rule values.
CSCta88592	WCS 6.0.132.0 don't show Mesh AP Root in Map view
CSCta97447	WiSM telnet access still works with telnet disabled
CSCtb20402	H: Can not telnet/ssh into 2106 from default gateway
CSCtb27192	WLC GUI Client Disabled List Truncated
CSCtb32061	HREAP pulls DHCP in Vlan 1 with Static Address and VLAN Mappings
CSCtb36008	RRM settings is not saved to Flash/Uploaded configuration file
CSCtb56664	Remove Over The Air Provisioning (OTAP) in Access Points
CSCtb61628	SNMP Trap Controls setting is not succeeded on 5.2
CSCtb64579	Wired Guest accessUser is not redirected to Webauth page after some time

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtb88018	AIR-CT5508- Unable to install license file
CSCtb93729	Authentication trap flag does not get saved on reboot.
CSCsx94354	AP rejects DHCP offer with bad option 7 (log server) value
CSCsy17745	"lwapp ap" CLI always returns "ERROR!!! Command is disabled."
CSCsy71960	1242 AP ignores primary WLC to join wrong WLC
CSCsz32424	Rogue not detected on wire using the arp
CSCsz53516	DHCP fallback with static IP takes 4 hrs
CSCsz53825	WLC shows medium power for AP1250 even when switch provides 20W
CSCsz67652	DOT11-3-RADIO_INVALID_FREQ_FOR_CHAN Frequency not found 133
CSCsz95595	Permit all IOS CLI commands in TELNET/ssh sessions
CSCta28431	On reboot dot1x credentials are not saved on 1140 APs registered to WLC
CSCta28666	Config mesh linktest RSSI output is wrong.
CSCtb32061	HREAP pulls DHCP in Vlan 1 with Static Address and VLAN Mappings
CSCsv83207	bsnMobileStationReasonCode missing in BsnMobileStationTable MIB
CSCsy23704	HREAP/Monitor/wIPS AP1242/1252 stuck in CFG/IMAGE/JOIN states
CSCso50723	WLC2106 EAP-FAST PAC provision failed due to slow DiffieHellman
CSCsr89694	Mobility control path between controllers on 4.2.130 are flapping
CSCsv56016	WLC showing incorrect message for valid IP address of syslog host
CSCsx29643	DCA extended channel corruption and wrong 40Mhz assignment on 2.4G
CSCsx48164	Insufficient debugs for troubleshooting webauth under heavy load
CSCsy65401	wlc on 5.2 code does not retain customized webuth setting after reboot
CSCsy88329	AP fails on downloading code - Bad Record MAC - DTLS Encrypted Alerts
CSCsz15249	WLC failed to handle out-of-sequence DTLS records
CSCsz40659	Need to reboot wireless controller for upgrade to work
CSCsz58995	Reaper reset crash on WLC with 1 monitor AP
CSCta01750	Crash by Deadlock on spamReceive Task
CSCtc76304	HMR1: WPA config restore fails with dhcp-required enabled.
CSCtc79776	HMR1: APs are crashing when Infra MFP is globablly enabled
CSCsv14863	WLC sends and displays channel 0 and power level 0 settings to AP
CSCsv34136	WLC should not enforce source port check on RFC3576 Disconnect-Request
CSCsv39950	WLC crash - 'apfMsCreateDeadlock+76'
CSCsv97224	Custome web not selected still user prompted with custom page
CSCsw80042	1140 Does not join Controller due to use of Ethernet MAC address
CSCsx14840	LAG: management Interface change between port BIA and lag port address
CSCsx57919	Heitz: Radius auth fails with wpa1/2-psk+webauth combination
CSCsy72769	TALWAR: SSH cons stalled when doing show run-config with paging disabled

Table 7 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz05894	H: Need cli/debug cli command for sshpmApiDeleteRules
CSCsz46308	H: Debug messages fill up message logs

If You Need More Information

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

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

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

Troubleshooting

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

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

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

Documentation Updates

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

Omissions

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

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

Related Documentation

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

- The quick start guide 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/c/en/us/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/c/en/us/td/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.
