Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.0.98.0

April 2011

These release notes describe open and resolved caveats for release 7.0.98.0 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, 1200, 1230AG, 1240, 1250, 1300, AP3500, AP1260, AP 1040, 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 7.0.98.0 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 7.0.164
- Cisco WCS Navigator 1.5.X.X
- Location appliance software release 6.0.X.X
- Mobility services engine software release 6.0.X.X 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, 3310 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 7.0.98.0 release does not support the NM-AIR-WLC6 platform. The NME-AIR-WLC platform is supported.

- 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 600, 1261 (single radio), 1505, 1510, and 1550 access points.

- Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, AP1260, 1300, AP3500, AP 1040 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).

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 (7.0.98.0, 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 7.0.98.0.

Note See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*, for more details and configuration instructions.

Cisco CleanAir

Interference Detection and Classification — CleanAir can classify over 20 different types of interference within 5 to 30 seconds. A custom chipset is optimized to allow detection of non-Wi-Fi wireless transmissions while simultaneously serving network traffic. Because the detection and classification takes place on inline silicon, rather than in software that consumes processing power, the 3500 Series produces interference visualizations that are much more detailed and precise than those produced by competing systems. This feature enables more intelligent decisions and policies, for automatic remedial action and faster troubleshooting.

Per-Interference Severity Impact — CleanAir provides full visibility into the performance and security of the wireless network with an easy to read air quality index that identifies problem areas and locates them in the context of access point, floor, building, and campus. An air quality index provides a snapshot of the performance and impact of interference on the wireless network. Network administrators can set alerts so that they are notified when air quality falls below a desired threshold. The system can also be configured to automatically enforce security or management policies. Cisco CleanAir generates reports to help network administrators prioritize interference issues that require immediate attention and easily drill down into the details for further network analysis.

Air Quality by Access Point — Administrators can now get an air quality rating on a per radio basis to gauge the impact of interference on the network. This feature provides advanced troubleshooting capabilities that allow organizations to view and use real-time interference data from individual CleanAir access points through the WLAN controller GUI or CLI. Administrators can quickly understand the severity and impact of non-Wi-Fi interference on network performance. This feature enables more intelligent decisions and policies for automatic remedial action and faster troubleshooting.

Air Quality Index Alarm Threshold — This feature provides 24 x 7, on-demand network monitoring. It automatically sends alerts when user-defined thresholds are exceeded for enhanced visibility and control. Air quality thresholds generate alerts, are user configurable and can be used by any SNMP trap receiver for simple integration into existing network management infrastructure.

Rapid Update Mode — Real-time air quality charts show interferers per CleanAir access point. Power and channel utilization is updated at 30-second intervals. Organizations can use these charts to quickly view the impact of interference in near real-time and on a per radio, per channel basis.

Spectrum Expert Connect Mode — Any CleanAir access point can be configured as a network-connected sensor. Administrators can instantaneously access any network location covered by a CleanAir access point using the Spectrum Expert configuration. This feature improves response time and eliminates the need for travel to analyze interference data.

Interference Alarms Sent as SNMP Messages — This feature allows the use of industry-standard SNMP interfaces to monitor the presence and severity of non-Wi-Fi interference on many network management platforms. Each time an interference device is classified by a CleanAir access point, details about the device type and severity of impact are transmitted via Simple Network Management Protocol (SNMP) messages.

Spectrum Management Information Base (MIB) — This feature allows organizations and integrators to create their own suite of network monitoring applications using CleanAir data. An industry-standard spectrum MIB was created to support third-party products in integrating with CleanAir technology.

Event-Driven Radio Resource Management — Interference data from Wi-Fi and non-Wi-Fi devices is detected and classified by CleanAir access points and then integrated into radio resource management (RRM) technology for automatic interference mitigation. RRM intelligently and automatically adjusts network settings and channels to avoid RF interference and optimize network performance. This feature increases network reliability and reduces false positives associated with measurements based on Wi-Fi only.

Persistent Device Avoidance—CleanAir access points remember intermittent yet destructive interference and avoid the channels with the interference. CleanAir can determine if interference is persistent from a stationary source, even from an intermittent device such as a microwave oven, video camera, or network bridge link. The access points within range of the interference will change channels and will remember to avoid the impacted channels in the future.

Support of 500 Access Points per Cisco 5500 Series Wireless Controller

A single Cisco 5500 Series Wireless Controller can now support up to 500 Cisco Aironet Access Points.

Cisco 5508 Series Controllers Location Support

The Cisco 5508 Series Controller can now support up to 7000 clients and 5000 RFID tags when using the location support.

Cisco Video Stream Technology

A new system wide set of features of the Cisco Unified Wireless Network enables reliable and consistent delivery of multicast streaming video over the WLAN.

Enhanced Functionality for Wireless Controller Base Licenses

Cisco OfficeExtend, Enterprise Wireless Mesh and Control and Provisioning of Wireless Access Points (CAPWAP) data encryption advanced features are now included in the wireless controller base license.

Passive Client Support

Passive client support establishes TCP/IP communication with wireless clients configured with static IP addresses without any manual configuration changes on the client. With this feature, the controller supports clients that associate with the network and go into sleep mode without requiring reauthentication.

Note Passive Client feature is supported on the Cisco 2100 and 5508 Series Controllers.

Enhanced Access Point Update and Joining Capability

The controller can handle up to 500 simultaneous access point joins and access point image downloads.

SIP Call Admission Control

SIP call admission control provides bandwidth reservation for Session Initiation Protocol (SIP)-based voice calls. Historically, bandwidth is reserved via Traffic Specification (TSpec) but most SIP clients do not support TSpec, which prevents bandwidth reservation. This feature enables the Controller to provision the bandwidth requirement for SIP calls and allocate or reserve bandwidth on per-usage or per-call basis.

This feature is applicable for non-TSPEC based SIP Calls. SIP Call Snooping should be enabled, only if there are non-TSPEC SIP based clients. We recommend that you use the SIP CAC feature only with static CAC.

Note Do not use SIP CAC with Load-based CAC.

Load-based CAC statistics are based on the AP Radio statistics that take into consideration 802.11e QoS information in the 802.11 packets. If there are any SIP-based voice calls from clients that do not have 802.11e QoS support, those calls will not be taken into account to limit calls based on Load-based CAC.

Max Call Limits for SIP CAC

You can configure the SIP CAC feature to set a maximum call limit. This feature must be configured only for SIP-based CAC to limit the number of calls per radio. By default, this feature is disabled. The default value for maximum number of calls is 0, which indicates there is no check for Max call limit.

Note The Max call limit feature is applicable only for non-TSPEC SIP based Calls, even though it counts TSPEC based calls if configured. This feature has a known limitation wherein, there is no option to set a limit for roaming-in calls. The Max Call limit includes both direct and roaming-in calls. If the maximum call limit is reached, new or roaming-in call will fail.

Per WLAN Radius Source Support

The controller uses the management interface as identity. If the RADIUS server is on a directly connected dynamic interface, the traffic is sourced from the dynamic interface. Otherwise, the management IP address is used.

If the feature is enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on the WLAN.

You can configure this feature by entering the following command:

```
(Cisco Controller) > config wlan radius_server overwrite-interface enable <wlan-id>
```

FIPS Support

Cisco Controller Release 7.0.98.0 has been awarded Federal Information Processing Standard (FIPS) 140-2 validation. The following Cisco WLAN controllers and access points have received FIPS 140-2 Level 2 validation: the Cisco 5508 WLAN Controller; the Cisco Wireless Integrated Services Module (WiSM); the Cisco 4400 Series WLAN Controllers; the Cisco 3750G WLAN Controller; the Cisco Aironet Lightweight Access Points: 3502i, 3502e, 1262, 1142, 1252, 1524, 1522, 1131, and 1242. The NIST Security Policies and FIPS certificates for these modules can be downloaded at the NIST web site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Software Release Information

The 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, you should 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 7.0.98.0

Before upgrading your controller to software release 7.0.98.0, 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 7.0.98.0, 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 7.0.98.0 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 7.0.98.0 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.
- The AP-count evaluation licenses for the 7.0 and the 6.0 releases are different. If you downgrade from a 7.0 release to a 6.0 release, you must activate the AP-count evaluation license of the 6.0 release after you downgrade. Similarly, if you upgrade from a 6.0 release to a 7.0 release, you must activate the AP-count evaluation license of the 7.0 release after you upgrade. If you do not activate the AP-count license, then the AP-count is shown as 0.
- 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 7.0.98.0. Table 1 shows the upgrade path that you must follow before downloading software release 7.0.98.0.

Table 1 Upgrade Path to Controller Software Release 7.0.98.0

Current Software Release	Upgrade Path to 7.0.98.0 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 7.0.98.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 7.0.98.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 7.0.98.0.
4.1.191.xM	Upgrade to 4.1.192.35M and then to 6.0.182.0 before upgrading to 7.0.98.0.
4.1.192.xM	You can upgrade directly to 7.0.98.0.
4.2.130.0 or earlier 4.2 release	Upgrade to 4.2.176.0 before upgrading to 7.0.98.0.
4.2.173.0 or later 4.2 release	You can upgrade directly to 7.0.98.0.
4.2.209.0 or later 4.2 release	You can upgrade directly to 7.0.98.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 7.0.98.0.
5.1.151.0 or later 5.1 release	Upgrade to a 5.2 or a 6.0 release and then upgrade to 7.0.98.0.
5.2.157.0 or later 5.2 release	You can upgrade directly to 7.0.98.0.
6.0.188.0 or later 6.0 release	You can upgrade directly to 7.0.98.0.
6.0.196.0 or later 6.0 release	You can upgrade directly to 7.0.98.0.

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

- We recommend 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 You cannot install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file on Cisco 5500 Series Controller platform.

  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	7.0.x.x
	AIR-LAP1131	3.1.59.24	
	AIR-LAP1141N	5.2.157.0	
	AIR-LAP1142N	5.2.157.0	

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	N/A	—
3500 Series	AIR-CAP3501E	7.0.98.0	
	AIR-CAP3501I	7.0.98.0	
	AIR-CAP3502E	7.0.98.0	
	AIR-CAP3502I	7.0.98.0	
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[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-LAP1523CM	7.0.98.0 or later.	
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.98.0 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 or with release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 Releases.

Interoperability With Other Clients

This section describes the interoperability of the version of controller software with other client devices.

Table 3 describes the configuration used for testing the clients.

Table 3 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.0.98.0
Controller	Cisco 4400 Series Controller and Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, AP 3500e and AP3500i
Radio	802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2
Type of tests	Connectivity, traffic, and roaming between two access points

Table 4 lists the versions of the clients. The traffic tests included data or voice. The clients included laptops, handheld devices, phones, and printers.

Table 4 Client Type

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5
Intel 5100/5300/6200/6300	13.1.1.1
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1520/Broadcom 43224HMS	5.60.48.18
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
Handheld Devices	
Falcon 4200/WinCE 4.2	5.60.21
Intermec CK31/WinCE 4.2:	3.00.19.0748
Intermec CN3/Windows Mobile 5.0	3.25.15.0065
Psion 7535/WinCE 5.0	1.02.09
Psion WAP/WinCE 5.0	1.02.42
Symbol 8846/Pocket PC 4.20	2.4.2273
Symbol MC70 /Windows Mobile 5.0	3.0.0.226
Symbol MC9060/Pocket PC 4.2	3.1.7
Symbol MC9090/WinCE 5.0	3.1.7
Phones and Printers	

Table 4 Client Type (continued)

Ascom i75	1.4.25
Nokia e61	3.0633.09.04
Spectralink 8030	104.025
Spectralink e340/PTE110	110.036/091.047/104.025
Spectralink i640/PTX110	110.036/091.047/104.025
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.269
Zebra QL320	HTNVK49s
Monarch 9855	3.2AB
Cisco 7921G	CP7921G-1.3.4.LOADS
Cisco 7925G	CP7925G-1.3.4.LOADS

Special Rules for Upgrading to Controller Software 7.0.98.0 in Mesh Networks

Caution Before upgrading your controller to software release 7.0.98.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 5 outlines the upgrade compatibility of controller mesh and nonmesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

The software upgrade notes are as follows:

- 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 5 for the available upgrade paths.

  Note If you downgrade to a mesh release, you must then reconfigure the controller. We recommend that you save the configuration from the mesh release before upgrading to release 7.0.98.0 for the first time. Then, you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 7.0.98.0 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 7.0.98.0. After a 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 6.0.182.0, 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 7.0.98.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 5 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases

Upgrade to / Upgrade from	7.0.98.0	6.0.196.0	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	–																						
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	–										

Table 5 Upgrade Compatibility Matrix for Controller Mesh and Nonmesh Releases (continued)

Upgrade to	7.0.98.0	6.0.196.0	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
3.2.195.10												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	–				
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 7.0.98.0 software to 500 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 7.0.98.0, 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.

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

Note Do not install the 7.0.98.0 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.

Note When upgrading from 5.2.193.0 to 7.0.98.0 release, access points with names that contain spaces will lose their configured name after the space. For example, if an access point was named “APTestName 12”, after upgrade, when the access point rejoins the controller, the name is truncated to “APTestName”.

Note If the SSID is associated with a dynamic interface, then the DHCP Option 82 that you configure must be enabled on the dynamic interface. Otherwise, the upgrade may not occur as expected.

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

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

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

Step 2 Follow these steps to obtain the 7.0.98.0 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. We recommend that you migrate to an upgraded release.

j. Click a software release number.

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

l. Click **Download**.

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

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 7.0.98.0 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 list, choose **Code**.

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

Step 9 In the IP Address text box, 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 for the Maximum Retries text field, and 6 seconds for the Timeout text field 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 text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout text box.

Step 11 In the File Path text box, enter the directory path of the software.

Step 12 In the File Name text box, 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 text box, enter the username to log into the FTP server.

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

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

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

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

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

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

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 7.0.98.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Reenable the WLANs.

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

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

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

Step 23 To verify that the 7.0.98.0 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 list, choose an unused COM port of 4 or lower.

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

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

Important Notes for Controllers and Nonmesh Access Points

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

Upgrading to 6.0.199.4 or 7.0.98.0 Can Disrupt DHCP Service When Using Controller's Internal DHCP Feature

Upgrading to controller release 6.0.196.0 or 7.0.98.0 can cause client devices to fail to complete DHCP. To work around this problem, use an external DHCP server, such as a router or a Layer-3 switch. This defect is described in CSCth68708, which is visible in the Bug Toolkit on Cisco.com at this URL:

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

WPlus License Features Included in Base License

All features included in a Wireless LAN Controller WPlus license are now included in the base license; this change is introduced in release 7.0.98.0. There are no changes to WCS BASE and PLUS licensing.

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

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

- If you have a WPlus license and you upgrade from 6.0.18x to 7.0.98.0: Your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 7.0.98.0 to 6.0.196.0, 6.0.188 or 6.0.182, the license file in 7.0.98.0 contains both Basic and WPlus license features, so you will not see any disruption in feature availability and operation.
- If you have a base license and you downgrade from 7.0.98.0, 6.0.196.0, 6.0.188.0 or 6.0.182.0, when you downgrade, you lose all WPlus features.

Note Some references to Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 7.0.98.0. However, WLC WPlus license features have been included in the Base license, so you can ignore those references.

Additive Licenses Available for 5500 Series Controllers

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

One-Time Password (OTP) Support

One Time Passwords (OTP) are supported on the Wireless Lan Controller (WLC) using TACACS and RADIUS. In this configuration, the controller acts as a transparent passthrough 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 alphabetic characters in the MAC address. In software release 6.0 or later, the controller sends lowercase alphabetic 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 300 access point groups for 4400 series controllers, 500 AP Groups on 5500 Series Controllers, and 192 access point groups for 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. However, this works when the managed access point is a monitor mode AP on a DFS channel.

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 with 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 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.

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 fix 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 7.0.98.0. 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 7.0.98.0, 6.0.196.0, 6.0.188.0, 5.2.178.0, 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points might not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

WLC GARP Behavior

The dynamic interface gateway fails first and controller receives the GARP for the dynamic interface from the switch and sends it accordingly to the client. After the controller sends out the GARP, the getway for the ap manager fails and this packet is dropped. The solution for this problem is as follows:

- Configure the ap-manager on a lower vlan so that the controller gets the GARP for ap-manager first, and then updates the ARP cache and sends out the GARPs that comes successively for the dynamic interface gateways through the new gateway. This way the GARPs do not get dropped and the clients does not disconnect.
- Stack-mac persistent timer 0 command on stack SW. If it is set to 0, mac address of stack SW is never changed to another one, so that the controller need not update the ARP table.

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, which 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 nonmulticast clients.

Disabling Radio Bands

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

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, AP1242AG, 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.

Note The Transmit Power level can range between -10 dBM to 30 dBM.

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.

To recover the access point using the TFTP recovery procedure, follow these steps:

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. We recommend that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Setting the Date and Time on the Controller

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

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, 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, we highly recommend that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*, for instructions for setting the time and date on the controller.

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

FCC DFS Support on 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

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

Configuring an Access Point's Prestandard Power Setting

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

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

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

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

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

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

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

Controller Functions that Require a Reboot

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

- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- 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). We recommend that you always run the controller with the default **config advanced rate enable** command in effect in order to rate-limit traffic to the controller and protect against denial-of-service

(DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, we recommend that you reapply the **config advanced rate enable** command after testing is complete.

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 Support

This version of Controller software release 7.0.98.0 is compatible with the Gateway Load Balancing Protocol (GLBP).

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.

Enabling/Disabling Band Selection and Client Load Balancing

It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing is enabled globally by default.

Changing the IOS LWAPP Access Point Password

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

config ap mgmtuser add *user_id* **password** *password* {*Cisco_AP* | **all**}

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

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

There are some cases where the prestage 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 7.0,* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0,* for configuration instructions.

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

DirectStream Feature Is Not Supported With WGB

The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied. This feature is not supported in 7.0 release.

Controller does not Support Transmitting Jumbo Frames

The controller does not support transmitting jumbo frames. To avoid having the WLC transmit CAPWAP packets to the AP that necessitates fragmentation and reassembly, reduces the MTU/MSS on the client side. For example, the TCP MSS Adjust feature can be leveraged here.

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>
```

Switch Port and Controller Port

When the port status on the controller changes, the switch status does not get changed. This is a known issue. For example, when the controller port goes down, the switch port is still in administrable state. This has been resolved in Cisco 5500 Series Controllers.

Issues With mac-address CLI for Unified and Autonomous Access Points

The unified and autonomous access point do not support the **mac-address** command for the wireless interfaces. When invoked, the command executes, but can cause the access point to fail.

Default A-MPDU settings

By default, Aggregated MAC Protocol Data Unit (A-MPDU) is enabled for priority level 0, 4 and 5 and the rest are disabled. In releases prior to 6.0 release, only priority 0 was enabled by default. The video performance is enhanced when priorities 4 and 5 are enabled for A-MPDU aggregation.

Important Notes for Controllers and Mesh Access Points

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

New Features

The following new features are available in controller software release 7.0.98.0.

Note See the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*, for more details and configuration instructions.

Backhaul Channel Deselection on Serial Backhaul Access Point

This feature enables you to configure a set of channels available to be assigned for the serial backhaul RAPs/MAPs. Normally, channels are selected by the user for RAPs, and the MAPs automatically tune to RAP channels (for AP1522 and AP1522PS) or select channels automatically (AP1524SB and AP1523CV). With the 7.0.98.0 release, there is a connect between the DCA list and serial backhaul mesh access points, only if someone uses (enables) this feature.

Serial Backhaul Launch for Rest of the World (ROW)

From software release 7.0.98.0 release or later releases, new 1524 SKUs are released, with both 802.11a radio units that supports an entire 5-GHz band from 4.9-GHz to 5-GHz and radios can operate in UNII-2 (5.25 - 5.35-GHz), UNII-2 plus (5.47 - 5.725-GHz), and upper ISM (5.725 - 5.850-GHz) bands.

The public safety band (4.94 to 4.99 GHz) is not supported for backhaul and client access.

With the expansion of the channel set, DFS-enabled channels, radar detection, and automatic channel reassignment in case of radar detection on RAP/MAPs are also supported. When there is a channel change, the change is propagated to the corresponding parent/child access point (if applicable) so that the change is synchronized between the parent and child and there is no link downtime. For example, if radar is detected on the uplink radio of a child access point, the parent is informed so that it can change the channel of the downlink radio. The parent informs the child about the channel change, so that the child access point can set the new channel on its uplink radio and does not have to scan again to rejoin the parent on the new channel.

Universal Client Access on Serial Backhaul Access Points

The serial backhaul access point consists of three radio slots. Radios in slot 0 operate in a 2.4-GHz band and are used for client access. The downlink and uplink radios operate in a 5-GHz band and are primarily used for backhaul. With the Universal Client Access feature, client access is allowed over slot 1 radios with the extended universal client access feature and client access is also allowed over slot 2 radios.

The two 802.11a backhaul radios use the same MAC address. There may be instances where the same WLAN maps to the same BSSID on more than one slot.

Note This feature is intended only for WGB clients and not for typical Wireless clients.

By default, client access is disabled over both the backhaul radios.

Cable Modem Serial Access from Access Point

This feature enables you to execute commands to the cable modem from the privileged mode of the CLI. This command takes a text string and sends it to the cable modem UART interface. The Cable modem interprets the text string as one of its own CLI commands. The response is captured and displayed to the IOS console. Up to 9600 characters are displayed from the cable modem. Any text beyond the 9600 characters is truncated. The modem CLI commands can be used on Mesh APs that have devices connected to the UART port.

Wireless Client Support for WGB

A Workgroup Bridge (WGB) is a small standalone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB is associated with the root AP through the wireless interface. Thus, wired clients get access to the wireless network.

In the current architecture, while an autonomous AP functions as a workgroup bridge, only one radio interface is used for controller connectivity, an Ethernet interface is used for wired client connectivity, and another radio interface is used for wireless client connectivity. In a practical scenario, dot11radio 1 (5 GHz) can be used to connect to the controller (using a mesh infrastructure), an Ethernet interface can be used for wired clients, and dot11radio 0 (2.4 GHz) can be used for wireless client connectivity. This scenario can improve the serviceability of a workgroup bridge without any extra cost. Depending on your network requirements, dot11radio 1 or dot11radio 0 can be used for client association or controller connectivity.

With the 7.0.98.0 release, the wireless clients on the second radio of the WGB are not dissociated by the WGB when it loses its uplink to a wireless infrastructure or in a roaming scenario. Access points with two radios certainly gives better advantage because one radio can be used for client access and the other radio can be used for accessing the access points. Also, wireless clients on the second radio do not get

disassociated by the WGB when it loses its uplink or in a roaming scenario. In this scenario, you must configure one radio as Root (radio role) and the second radio as WGB (radio role). All wireless clients connecting to the radio with role Root will belong to the same WLAN and the same VLAN which the WGB joins on the radio configured as role WGB.

Note If one radio is configured as a WGB, then the second radio cannot be a WGB or a Repeater.

Separation of Ethernet Clients Behind WGB

This feature provides a way for the Administrator to have wired clients behind a WGB in different VLANS. This feature also provides the QoS support to prioritize packets from WGB wired clients in the Mesh Backhaul based on DSCP/dot1p values, when a WGB is associated to a Mesh Access Point. Multicast support is provided for WGB wired VLAN clients by implementing IGMP Snooping in the Workgroup-Bridge. For using this feature, the WGB must use a release later than 12.4(21a)JA1, which has support for VLAN separation. This feature does not support downstream broadcasting of per-VLAN. However, you can replicate broadcast packets to all VLANS behind the Workgroup-bridge using the CLI.

Note We recommend that you enable the IGMP feature for this feature to work.

Note Broadcasts received to a controller form a VLAN other than the VLAN of the WGB will not work.

Note Dynamic interfaces should be configured on the Controllers for all the VLANs configured in the WGB and the switch connecting the WGB. Layer-2 multicast is not supported for WGB Ethernet clients. The same native VLAN should be configured in the Controller, Workgroup-Bridge, and the switch connecting the Workgroup-Bridge.

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 Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 7.0.98.0. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

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

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

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

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

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

Open Caveats

Table 6 lists open caveats in controller software release 7.0.98.0.

Table 6 Open Caveats

Identifier	Headline
CSCth37733	Multicast does not work without fragmentation if IGMP snooping is enabled.
CSCth02374	HREAP central switching TCP performance is better than local switching.
CSCtf36053	Any CPU ACL blocks the service port that offers DHCP.
CSCtg66175	RLDP does not work on the CT5500 or WLC2100 when using HREAP access points.
CSCtd21754	When using the outdoor Mesh AP 1522, if you disable the 'b' radio either using the GUI/CLI, on rebooting the AP, the 'b' radio is enabled (that is, the status is UP) by default.
CSCtb72660	NEC SIP CAC: Load-based CAC does not work with non-WMM clients.
CSCtf38802	SIP calls on roaming with a CAC failure connect back without reserved bandwidth.
CSCtg65856	Counters do not clear during an intracontroller roaming of SIP-reserved bandwidth calls.
CSCtg74333	Addition of VOICE_CALL_FAILURE_5 Enum to QOS MIB.
CSCsj33229	Unable to ping APs directly connected to a 2106 controller.

Table 6 Open Caveats (continued)

Identifier	Headline
CSCso22875	APs disconnect during a code upgrade.
CSCsv54436	SSH to controller is sometimes denied with an error message “Sorry, telnet is not allowed on this port”.
CSCsw93671	Packets sourced from the service port are sent from the controller when they are not connected.
CSCsy18685	The default group for ap-groups does not contain all SSIDs.
CSCsy62007	When a client is in the DHCP required state, the WLC drops a DHCP Inform packet.
CSCtd14642	The WLC crashes at sshpmReceiveTask on 5.2.193.
CSCte53175	The per-user bandwidth contract blocks all traffic when set to 0.
CSCtf27464	The management interface does not use an HSRP MAC address when replying.
CSCtf44335	Clients are not removed from Temporary Exclusion List after 60 seconds.
CSCtf51294	Cannot clear webauth bundle from the controller.
CSCtf62737	WLC URL sanitation issue.
CSCtf78029	SNMP traps for the 1231 AP also sent for Interface:1(unknown type).
CSCtf90579	With TACACS/RADIUS auth, the lobby admin is unable to edit the Guest user role.
CSCtf91342	After a bad UN is used, the LDAP server not functional for 15 minutes.
CSCtf97171	5508 port channel goes down under load when connected to HP Procurve.
CSCtg09589	A duplex mismatch occurs when a 1140 AP is directly connected to the 2100 WLC.
CSCtg21950	WGB intracontroller roaming must update its clients without an IAPP frame.
CSCtg23396	The **show dhcp stats** command does not display output when DHCP Proxy is changed to enabled.
CSCtg23491	The WLC does not process flooded unicast traffic properly.
CSCtg23618	WiSM is unreachable outside of Catalyst 6500 Series Switch.
CSCtg24959	The wireless NAC traffic sent on an access VLAN though the client is in quarantine.
CSCtg30694	The WLCWebauth client never has to reauthenticate even after a session timeout.
CSCtg51544	MSFT: Multiple SSH sessions can cause an arrow key failure and the password is visible.
CSCtg51702	Degraded voice performance occurs on HREAP local switching with TKIP and CCKM.
CSCtg55102	HREAP: AssocFailPayload causes a payload error at WLC.
CSCtg58982	AP interface UP trap is missing.

Table 6 Open Caveats (continued)

Identifier	Headline
CSCtg66192	After some period of time in operation, the Cisco 5508 Series Controller controller stops working. The alarm light displays solid amber, the system light displays amber, and the console access is lost. Rebooting controller has no effect.
CSCtg67029	The **show client tsm** command does not display full output.
CSCtg68301	The WLC is not making an NPU entry for clients after sending the gratuitous ARP.
CSCtg68437	Cannot create a WLAN with the WPA-PSK from the template.
CSCtg70271	While running the **debug client <mac_address>** on a Webauth error, the following error was displayed: `*May 04 15:52:58.248: 00:1d:e0:b6:3e:0b 192.168.252.119 WEBAUTH_REQD (8) Reached ERROR: from line 4055` This error message needs to be more clear.
CSCtg70274	The HREAP AP and WLC out of sync with initial client association.
CSCtg80606	The LAP did not join the CT5508 with multiple AP managers.
CSCtg81397	External webauth is broken in HREAP local switching.
CSCtg84677	AP deauthenticated when the power capability is unacceptable 0x000a.
CSCtg87389	Talwar crashes on dtlArpTask.
CSCtg88213	Upgrading 4.1.192.35M to 6.0.196.0 loses all configuration.
CSCtg90114	The WLC acting as a guest anchor does not forward DHCP requests to the anchor controller.
CSCtg92171	The WLC stops responding to the network.
CSCtg93001	The HREAP client can authorize but does not associate - the wrong MAC was used for AUTH.
CSCtg94715	A lock assert dtlARPTask caused the 5500 WLC to crash.
CSCtg96045	An RLDP has failed due to rate mismatch with the Rogue AP.
CSCtd78471	A mobile scan process misses probe responses and is doing bad parent roaming.
CSCtd90106	1242 APs periodically fail during a CTK refresh.
CSCte86144	The AP crashes with %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header.
CSCtf06857	The 1240 IOS AP crashes with %SYS-2-MALLOCFAIL.
CSCtg03203	The 1142/1252 APs recognize 802.11n HT-enabled clients as legacy ones.
CSCtg25046	WGB: An EAP frame has dropped due to a delay on dot1x initi.
CSCtg44663	WGB: Multiple parents created during roaming traffic were disrupted.
CSCtg50410	An ARP table with a BVI1 interface is updated with a transparent ARP reply.
CSCtg73740	The AP should default AAA ports to 1812/1813 not 1645/1646.

Table 6 Open Caveats (continued)

Identifier	Headline
CSCtg57607	The WGB fails to send an IAPP update.
CSCtg95111	The AP, which is not correctly primed, keeps reconnecting with the master.
CSCtk53680	WiSM unable to transfer the coredump via FTP when running low on memory.
CSCtl44908	The DCA channel lists change when the Wireless LAN Controller is upgraded to 7.0.x from 4.2.
CSCtl95978	The Wireless LAN Controller does not appear to respond to SNMP requests if the source address of the request comes from a subnet that is configured as a dynamic interface.
CSCtg09393	RRM TPC— The minimum power level assignment is not working for levels below 4.
CSCud20593	The Cisco TrustSec SXP feature is not supported.

Resolved Caveats

Table 7 lists caveats resolved in controller software release 7.0.98.0.

Table 7 Resolved Caveats

ID Numbers	Caveat Title
CSCsq63937	WLC: SNMP object agentTransferUploadMode can be set to NULL.
CSCsr10874	Additional client statistics are required.
CSCsv12308	AP-Manager uses the last MAC address of its gateway instead of the new address.
CSCsw29804	WLC: AppleTalk does not work with the Lexmark Printer.
CSCsx14840	LAG: A management interface change has occurred between port BIA and LAG port address.
CSCsx50408	The LWAP DOS Attack trap message does not record the source MAC address.
CSCsx71175	WLC broadcast DHCP does not comply with RFC 1542.
CSCsy28323	MFP scalability improvement.
CSCsy65347	QoS profiles per-user bandwidth contracts are not restricting traffic.
CSCsy71960	The 1242 AP ignores the primary WLC to join the wrong WLC.
CSCsy80680	The client is stuck in the 8021X_REQD state after a mobility event.
CSCsz64049	WLC crash - nf_iterate causes a kernel panic/exception.
CSCsz76796	The PMK cache is not updated after a refresh authentication.
CSCsz80820	The primary discovery request is not processed for an access point priority scenario.
CSCsz87643	The management interface is unreachable via a different subnet.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCta09996	Sometimes the LAP cannot join the WLC via an alternative port in port redundancy.
CSCta18874	The WCS startup fails for non-U.S. locale installations.
CSCta29484	The radio stops beaconing for a 10-second period.
CSCta30165	Provide backward compatibility for letter case of the call station ID: CALLING_STATION_ID and CALLED_STATION_ID as per the 6.0 release.
CSCta34714	D3 Web-auth redirections fail during failover scenarios.
CSCta38050	The GUI /screens/spam/cell_list.html no longer has a Port column.
CSCta40160	A dropped primary discovery request from an AP has already been joined to the WLC.
CSCta45156	Upgrading to 6.0.182.0 Webauth login page text displays as one long sentence.
CSCta49183	The speed/duplex configuration is not available via the CLI for the WLC.
CSCta88592	WCS 6.0.132.0 does not show the Mesh AP Root in the Map view.
CSCta91358	HREAP is locking up due to a wedge input queue on the radio interface.
CSCta93380	WLC on 4.2.205.0 drops the boot packet.
CSCtb02136	The AP1252 with AP Groups and HREAP will not broadcast an SSID.
CSCtb20402	Cannot TELNET/SSH into 2106 from the default gateway.
CSCtb34971	WLC WISM loading third party CERT for web-auth disables HTTPS port 443.
CSCtb36010	Lightweight AP responds on port 22 when SSH is disabled.
CSCtb41486	The **show ap image** predownload version column shows the wrong version. This is seen in the HMR release.
CSCtb42260	Enabling broadcast forwarding verses multicast forwarding via the CLI.
CSCtb45178	Insufficient memory/traceback on the AP1130 and AP1232.
CSCtb50732	Reaper Reset on osapiBsnTimer.
CSCtb52563	WLC 4.2.205.0 crashes at spam_CCM_decrypt+124.
CSCtb58091	WLC CPU Spike with emWeb - Controller Not Responding - No crash.
CSCtb63297	File read errors in msglog.
CSCtb64579	Wired Guest access user is not redirected to webauth page after sometime (approximately 10 minutes) before logging in, which results in a timeout.
CSCtb64994	Intermittent Webadmin and Webauth access on WiSM running 5.2.193.
CSCtb67889	The GUI does not match the CLI functionality for broadcast/multicast forwarding.
CSCtb74239	The WISM crashes on task sshpmMainTask System Crash.
CSCtb93729	The authentication trap flag does not get saved on the reboot.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtb96750	AP Fallback causes a client drop with HREAP.
CSCtc01947	Initial CAPWAP packets are sent to the burned-in MAC address by the controller in HSRP.
CSCtc03575	The controller fails to redirect web authentication to an external server.
CSCtc05478	The **debug pm ssh-engine enable packet** command does not work.
CSCtc10068	The 1140 series access point tries to join the LWAPP controller. The 1140 series AP should never attempt to join a LWAPP controller because controllers running 5.2 or later releases support 1140 series APs.
CSCtc13474	No mobility record was found for the peer error seen for the self IP address.
CSCtc14910	The 1140 Series AP does not join the WLC and logging tracebacks.
CSCtc15346	The AP1252 fails to retransmit a missing AMPDU packet in response to block ACK.
CSCtc23789	AP radio down - interface is stuck in reset.
CSCtc32748	Noise and channel measurements are not done on all DCA channels.
CSCtc45090	The controller sends the wrong MAC in the ARP response, which can cause mobility flapping.
CSCtc49270	Clients cannot be deleted from the exclusion list if they are not present in the association list.
CSCtc49690	WCS: Audit mismatch occurs for the LAG mode.
CSCtc57611	Delay in music on hold on 7925 with the HREAP AP.
CSCtc73527	Make low latency MAC a no op for 11n APs till CSCsy66246 is addressed.
CSCtc85444	The WLC locks up on an SNMP task when pushing the AP Group template from the WCS.
CSCtc97144	Fixed 1800-second session timeout occurs when HREAP is in the standalone mode.
CSCtd01611	Important TLS/SSL security update.
CSCtd02336	Exception: AesEventGen:fireEventTo displayed when synchronizing network design, without having any NB event notifications enabled.
CSCtd17116	Emergency image version shows up as N/A.
CSCtd25303	A wrong message appears on the GUI when the controller image is upgraded while the AP downloads the image.
CSCtd26168	Incorrect source MAC is in the ARP request when the WLC is in LAG mode.
CSCtd26408	WCS 4.2.110.0 cannot modify external web auth redirection URL for WLANs.
CSCtd34312	The 5508 Web Auth breaks with multicast MAC as the gateway.
CSCtd44718	Add user input required commands to the CLI template parser.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtd49103	The AP in the static address uses the wrong syslog and the LEDs turn off for some seconds.
CSCtd60522	WLC - Config back add wrong 802.11a channel list.
CSCtd62937	The **show ap summary** does not show the AP names.
CSCtd67660	Current message-digest algorithm for self-signed certificate allows collisions.
CSCtd70053	Guest mobility anchoring fails when roaming between controllers.
CSCtd70812	Rogue AP report does not produce consistent results.
CSCtd72234	4.2 Mesh MAC auth to external RADIUS has Authenticator all zeros.
CSCtd73371	The WLC shared memory allocation failed after web pass through enabled.
CSCtd75089	The WLC needs **show** command to display mbuf usage.
CSCtd82509	The WLC crashes at findContextInfo+268.
CSCtd84522	The fiber port (gig3) does not create VLAN subinterfaces when bridging.
CSCtd86886	The WISM may generate a traceback in the msglog.
CSCtd90304	Error %MM-3-MEMORY_READ_ERROR: mm_mobile.c:464 Error reading mobility memory seen when using WISM blades.
CSCtd92105	Reaper reset in DHCP task.
CSCtd99328	Migration of autonomous AP {AIR-AP1131G-A-K9} to LWAPP failure.
CSCtd99602	Wired Guest: DHCP required breaks web auth following session timeout.
CSCte08090	AW: TFTP upload is broken for the Packet Capture to Windows TFTP server.
CSCte08161	Cannot get IP address from the server if key-management is WPA Optional.
CSCte11997	AIRESPACE-WIRELESS-MIB on Cisco.com is having incomplete traps.
CSCte27052	WLC 6.0 - Inconsistency in the AAA Override feature.
CSCte38645	RADIUS Attribute NAS-Port(5) not included in Access-Request for Web-Auth.
CSCte39477	Web GUI: External web servers field needs to always be displayed.
CSCte43508	5508 DP CRASH: buffer leak is due to an ARP storm.
CSCte51177	SNMP TRAP port number not reflected in the config file of the controller.
CSCte55458	Web-Auth: Web page takes a long time to display under a heavy load.
CSCte92365	Auto Immune part II: AP side.
CSCte92886	4.2 Mesh controller Memory Leak in EAP Framework.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtf08553	Syslog is not sent to server that is on the same subnet as the dynamic interface.
CSCtf14288	Input validation limitation within the WCS search fields.
CSCtf17352	The MSE goes unreachable because of out-of-memory error.
CSCtf17441	WCS - Certain APs are missing from the AP summary reports.
CSCtf23682	5508 - The AP cannot join with multicast MAC as the gateway (checkpoint).
CSCtf25486	An error appears when randomly enabling WPA WLANS on the controller.
CSCtf28217	The AP unexpectedly joins WLC in bridge mode instead of local or HREAP.
CSCtf39285	The 5500 WLC will accept a 4400 4.2.x.x image.
CSCtf51287	The **show exclusion list** command does not display excluded clients, only disabled clients
CSCtf51758	Session cookie and scripting code issues.
CSCtf53344	LWAP DOS Attack trap message does not record the source MAC address.
CSCtf81266	APF-1-ROGUE_CLIENT_UPDATE_FAILED filling up the syslog
CSCtf94589	An AP MAC address discrepancy occurs in aggressive load balancing packets.
CSCtg14415	There is a potential issue in webacs/monitorMapListAction.do
CSCtg14532	The controller PMKID debug output indicates "No valid PMKID" but PMKID works.
CSCtg29286	WCS: An e-mail notification/status change for the scheduled guest template fails.
CSCtg33854	Several XSS (Cross Side Scripting) vulnerabilities on different WCS URLs.
CSCtg71658	The access point power level is reset to 0 when upgrading from 5.0 to 6.0.196.158.
CSCtc52412	Issue with client mobility across SSIDs on the same radio.
CSCsx20463	Difficult to differentiate between lowercase and uppercase L on guest credentials.
CSCsx96043	The client count graph in the home page is not showing autonomous clients.
CSCsy90434	The WLC command line displays diversity is enabled for a 1522 "a" radio.
CSCsy99905	RLDP only consistently finds wired threats when manually used.
CSCsz14243	Cannot enable the WLAN while the APs are joining.
CSCsz19203	Controller crash at SSHpmMainTask.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCsz38828	AMAC radio experiences core dump: the transmitter seems to have stopped.
CSCsz40659	The wireless controller must be rebooted for an upgrade to work.
CSCsz84895	An association response has the wrong set of supported rates to the 11b device.
CSCta04008	The call station type on the controller should state as applicable to non-802.1x only.
CSCta13941	An AP rejects an association request with status code 13.
CSCta34765	Invalid behavior occurs when executing the **config mirror port** command.
CSCta41584	The backup port is not active when the primary port is disabled on the controller.
CSCta71448	Reduce the severity of the error msg: “%APF-1-CHANGE_ORPHAN_PKT_IP”
CSCtb16583	An AP changes from static IP to DHCP and does not covert back to static IP.
CSCtb20125	CCMP errors occur on key rotation.
CSCtb39368	Webauth custom page fails with some file extensions.
CSCtb39612	WGA two box solutions displays the following error: “Cannot find MSCB for NPU SCB” on the console.
CSCtb58698	After upgrading the alpha WCS from 6.0 to 7.0, WCS generates a license error.
CSCtb62191	Error: Invalid TEAP data error is displayed when LAP dot1x wired supplicant PAC refreshes.
CSCtb92872	WiSM: System crash - Task "cids-cl Task" taking too much CPU.
CSCtc13378	The Cisco 5508 Series Controller displays a system crash on apfProbeThread.
CSCtc15533	AW: CPU ACL counters not working on the Cisco 5508 Series Controller.
CSCtc18467	An MSDU frame is transmitted with the same sequence as a normal data frame.
CSCtc41797	RLDP does not work for G-only APs.
CSCtc44480	An access point transmits ad-hoc deauthentication even after auto-contain is disabled.
CSCtc50424	Cisco 5500 Series Controller DP crashes under condition 'pbuf->dataLen <= 2048' (also MFP Errors).
CSCtc51076	Setting the spanning tree port mode off does not save it to the uploaded configuration.
CSCtc56702	The wrong warning appears for the ssh/telnet template.
CSCtc67372	The commands **show run** or **show tech** hangs on SSH/telnet with paging disabled.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtc73503	Radios are showing Tx power level 0.
CSCtc90985	The DMA input queue is overrun by fast Ethernet bursts.
CSCtc95434	An FTP transfer does not work on the Cisco 2100 Series Controller.
CSCtc97595	Only one of many gratuitous ARP packets are forwarded to the client.
CSCtd06186	Directed broadcast does not work when IGMP snooping enabled.
CSCtd21859	WLAN CKIP PSK is deleted when you press the Apply button.
CSCtd23497	1242 AP HREAP Mode crashes after displaying the following error: %CAPWAP-5-CHANGED state to join.
CSCtd26794	Cisco 5508 Series Controller DP CRASH- Fragmentation consumes all pbufs.
CSCtd28542	The controller crashes on emWeb due to an AP config change.
CSCtd28757	The LDAP user password length needs to be increased.
CSCtd30669	The WLAN security setting and session timeout are changed after the restoration.
CSCtd42314	The WCS - CLI template should continue operation when one command errors out.
CSCtd59231	The master bit config is not saved in the XML configuration.
CSCtd74615	The WCS NTP template fails on a rewrite/over write when three entries exist in the WLC.
CSCtd75094	An AP crashes when it clears the CAPWAP MGIDs for new clients.
CSCtd97011	AMAC radio core dump: Neighbor Discovery frames stuck.
CSCtd98538	WCS - Lobby admin cannot login. The HTTP 500 Error is displayed.
CSCtd99288	The client authentication trap flag cannot be configured via CLI.
CSCtd99659	The SNMP Agent inserts nulls during the mesh link test.
CSCte19262	Client Deauthenticated - Unable to locate AP 00:00:00:00:00:00.
CSCte55370	The WLC crashes during a ping of a virtual interface.
CSCte61754	Permission is denied for show status filter in the guest users controller template.
CSCte62815	The Cisco 5508 Series Controller does not pass OSPF multicast traffic.
CSCte74879	The Cisco 5508 Series Controller agentSwitchInfoPowerSupply MIB does not work.
CSCte75474	An issue occurs with template discovery for system general templates.
CSCte78472	An invalid PHY rate is returned on the ADDTS response.
CSCte81420	Crash in process: "Dot11 driver " dot11_rate_is_allowed.
CSCte81786	The **dbadmin remotebackup** command generates errors and does not perform an FTP backup.
CSCte96140	Ethernet bridging breaks when the Ethernet interface of AP 1242 is flapped.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtf03121	The Cisco 5500 Series Controller optical SFP misconnect causes a hung port.
CSCtf06931	Controller emWeb crashes when running 6.0.188.0 ewaFormSubmit_blacklistclient_list
CSCtf07885	Need a pop-up window in the AP Group page that mentions about HREAP VLAN mapping.
CSCtf13873	Duplicate IPs are not reported correctly on the WCS under alarms.
CSCtf30942	The WCS autonomous AP incorrectly displays the down alarm.
CSCtf35333	Issues occur with Reflected XSS.
CSCtf50921	Acct-Input-Octets counters are not reset with the accounting stop.
CSCtf71637	The username entry in the accounting stop does not match to the accounting start.
CSCtf84301	WCS: Unable to disable “Trace Display Values” once it is enabled.
CSCtg06954	Navigator: Data cleanup on WCS causes a client count graph discrepancy.
CSCtg16331	The JVM crashes in the WCS.
CSCtg17101	The WCS should generate an alarm when a configuration backup fails for a controller.
CSCtg42601	WCS allows "+" (Plus Sign) in the AP group name breaks the controller configuration via GUI.
CSCtg42627	CLI Allows "+" (Plus Sign) in AP group name breaks the controller configuration via GUI.
CSCtg47863	The WCS does not retain the key/certificate across upgrades.
CSCtg57691	An edit link on the AP list page displays a Permission Denied error on the GUI.
CSCtf34858	The client cannot transmit traffic if it reassociates to an AP within 20 seconds.
CSCte89891	The radio may stop transmitting beacons periodically.
CSCtf27580	Ethernet interface input queue wedge from broadcast/uniGRE traffic.
CSCta13941	An AP rejects an association request with status code 13.
CSCsx62302	The REAP VLAN support mapping on an AP was lost on an upgrade from 4.2.176 to 6.0.182.
CSCte55219	A radio core dump occurs due to large number of uplink frames in an in-progress queue.
CSCtf69598	A memory leak occurs in AP on CCKM Failure.
CSCtd43906	The RAP does not transmit after coming up when it is shut down due to radar.
CSCsr89694	The mobility control path between controllers on 4.2.130 are flapping.
CSCsv81229	TKIP Encryption Issue.
CSCsx99923	BDPUs are shown as FCS errors when in 5.2.178.0.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCsy30722	The next hop address stored in CAPWAP does not get updated on receiving the GRAT ARP request or reply.
CSCsy74355	If the service port does not have a static IP address and DHCP is not selected, a configuration restore will fail by displaying an error when the **debug transfer all enable** command is executed.
CSCsy76154	No LAG—WLC sometimes uses wrong port MAC address to send packet.
CSCsy96551	The internal WLC-DHCP functionality does not send out NAK.
CSCsy97077	The controller **show run-config** command is truncated and incomplete.
CSCsz22520	You cannot uncheck DHCP required without removing the DHCP override configuration on a WLAN.
CSCsz30842	The Local EAP function is not available in AIR-WLC526-K9.
CSCsz48244	In version 4.2 the Mobility Control path for the controller to the DMZ displays flapping up/down
CSCsz48475	The controller ignores radius packets on dynamic interface.
CSCsz50130	In 4.1 and later, after using the command **config wlan security tkip hold-down <0-60 seconds> <wlan id>** to change scan time for MIC errors, the parameter is reset upon reboot even after saving the configuration.
CSCsz57758	LAP1140 constantly boot-loads after downloading the image.
CSCsz92558	The ethernet interface statistics of AP are not displayed for non-mesh APs on WLC.
CSCta03016	The Cisco 4404 Series Controller crashes in 5.2.188.0 image.
CSCta05979	WLC cannot perform an LDAP authentication with AD when AD messages contain searchResRef.
CSCta09160	Need 802.1q tag in EoIP tunnel to be the same between controllers.
CSCta32912	WLC 5508 - SFP validation mechanism may reject Cisco sold SFP's.
CSCta53985	The MAC Filtering with WPA does not authenticate with external Radius Servers.
CSCta67367	After downloading configuration file, original configuration does not get restored.
CSCtb12031	The 1142 /1252 access points inconsistently acknowledge Vocera (gen1) badge.
CSCtb29243	When using the NAC scenario using multiple controllers, ARP flood spikes are observed (around 2500-5000 requests) on regular basis
CSCtb74037	An SNMP walk shows password for entire group.
CSCtb75305	The Cisco 4404 Series Controller lets all WEBAUTH_REQD traffic through.
CSCtb87326	When enabling NAT Address and TACACs, a 5508 controller crashes.
CSCtc41293	The controller does not act upon receiving ICMP fragmented needed packet.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtd16938	A WLC crash after passing invalid arguments to emweb.
CSCtd86437	An error occurs while trying to update code or ER image on Cisco 4400 Series Controller.
CSCtd91013	A memory corruption crash occurs on Cisco 5500 Series Controller.
CSCte01087	An AP running 6.0.188.0 cannot join Cisco 5508 Series Controller. The MAC addresses do not begin with 00.
CSCsi46897	A PRE crash occurs after snmpwalk on mib cbQosSetStatsTable.
CSCsm19182	When GH DFS is triggered, the D1 interface goes down with no channel available.
CSCsw49486	The AP CAPWAP client process crashed.
CSCsx49415	The 1230 APs run out of memory with cause memory fragmentation.
CSCsx49921	The CAPWAP DTLS join reassemble issue with handshake 'wrong signature size'.
CSCsy48084	A 1200 APs cannot join 5.2 controller with one radio.
CSCsy95660	In a 1140 AP, the Tx lockup with beacons enabled probes are disabled after rate config.
CSCsz15011	The auto smartport is seeing AIR-AP1231G-A-K9 access point as LWAP and thus applies the LWAP macro to the interface.
CSCsz47181	The AP1130 crashed during system upgrade.
CSCsz92558	The ethernet interface statistics of an AP are not displayed for non-mesh APs on WLC.
CSCta42012	Mesh - Root AP do not recreate subinterface at fallback.
CSCtb02314	An AP Fallback fails to primary when using CAPWAP / LWAPP WLC in same MG.
CSCtb06469	The c1200 APs locks up due to possible memory leak.
CSCtb27438	Rogue ad-hoc is detected as rogue AP.
CSCtb83470	AP intermittently only sends 2 buffered multicast packets per DTIM.
CSCtb95396	Need to turn off spread on Cascade PCIe clocks in IOS.
CSCtc15696	FFT: 1250 and 1130 APs flash getting erased.
CSCtc22803	Need to turn off spread on Cascade PCIe clocks in boot loader.
CSCtc54572	The 1240 access point crashes in CDP processing when AP is on third-party switch.
CSCtc78925	PPTP does not connect through IOS based AP.
CSCtd32790	The AP keeps the MAC entry from the Gi0 interface and not timeout.
CSCte15213	An AP in wIPS submode detects valid APs as soft APs.
CSCte43374	The WGB connection is broken under EAPoL logoff attack.
CSCte44083	An AP crash occurs with traceback=mvl_receive_packet+0x128.
CSCtf63030	Radio may get stuck in RESET or DOWN state.
CSCte93549	Dot11a radio is not able to pass traffic, tx queue is filled.

Table 7 Resolved Caveats (continued)

ID Numbers	Caveat Title
CSCtg89404	Association response to client is sent with AID 0.
CSCtb86685	Discrepancy between PoE CLI, WebUI, and WCS.
CSCtc11873	CPU ACL does not block existing TCP connection.

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*

You can access these documents from this link:

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.