Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.171.0

April 26, 2007

These release notes describe open and resolved caveats for software release 4.1.171.0 for Cisco 2000, 2100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 4.1.171.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 2.01
- Cisco Wireless Control System (WCS) software release 4.1.83.0
- Cisco Wireless Control System (WCS) Navigator 1.0.83.0
- Location appliance software release 3.0.37.0
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points

Controller Requirements

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

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

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

Software Release Information

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

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

Note The Cisco WiSM is supported on Cisco 7609 and 7613 Series Routers running only Cisco IOS Release 12.2(18)SXF5 or later.

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

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

Finding the Software Release

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

Upgrading to a New Software Release

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

Caution Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image! Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Special Rules for Upgrading to Controller Software Release 4.1.171.0

Caution Before upgrading your controller to software release 4.1.171.0, you must comply with the following rules.

- Controller software release 4.1.171.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 4.1.171.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
- If your controller is running software release 3.2.195.10 or a later 3.2 release or 4.0.206.0 or a later 4.0 release, you can upgrade your controller directly to software release 4.1.171.0 If your controller is running an earlier 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 4.1.171.0. Table 1 shows the upgrade path that you must follow prior to downloading software release 4.1.171.0.

Table 1 Upgrade Path to Controller Software Release 4.1.171.0

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

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 4.1.171.0 software. In large networks, it may take some time to download the software on each access point.

- Cisco recommends that you also install the Cisco Unified Wireless Network Controller Boot Software 4.1.171.0 ER.aes file on the controller. This file resolves bootloader defects and is necessary to ensure proper operation of the controller. The ER.aes file is required for the Cisco WiSM, Catalyst 3750G Wireless LAN Controller Switch, and 4400 series controllers.

Note The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (4.1.171.0 ER.aes) ensures that the bootloader modifications in all of the previous and current boot software ER.aes files are installed.

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

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

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

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

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

Step 3 Disable any WLANs on the controller.

Step 4 Follow these steps to obtain the 4.1.171.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 4.1.171.0 ER.aes file from the Software Center on Cisco.com:

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

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

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

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

e. Click the name of a controller.

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

g. Click a controller software release.

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

i. Click **Download**.

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

k. Save the file to your hard drive.

l. Repeat steps a. to k. to download the remaining file (either the 4.1.171.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.1.171.0 ER.aes file).

Step 5 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 4.1.171.0 ER.aes file to the default directory on your TFTP server.

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

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

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

Step 9 The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

Step 10 In the File Path field, enter the directory path of the software.

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

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

Step 13 Repeat Step 6 to Step 12 to install the remaining file (either the 4.1.171.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.1.171.0 ER.aes file).

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

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

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

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

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

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

Step 20 To verify that the 4.1.171.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 21 To verify that the Cisco Unified Wireless Network Controller Boot Software 4.1.171.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Bootloader Version field.

Note You can use this command to verify the boot software version on all controllers except the 2106. The Bootloader Version field remains at 4.0.190.0 for the 2106 controller, so you cannot tell which ER.aes file is installed.

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	—	4.0.219.0

Table 2 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M

Table 2 Software Support for Access Points (Continued)

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

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

New and Changed Information

New Features

The following new features are available in controller software release 4.1.171.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1* for details and configuration instructions for each of these features.

New Controller Module

- **Cisco Wireless LAN Controller Network Module-Enhanced (WLCM-E)**—The enhanced controller network module within the Cisco 28/37/38xx Series Integrated Services Router can support up to 8 or 12 access points (and up to 256 or 350 clients, respectively). It supports these access points through a gigabit Ethernet distribution system port that connects the router and the integrated controller.

New Controller Features

- **TACACS+ support**—Terminal Access Controller Access Control System Plus (TACACS+) is a client/server protocol that provides centralized security for users attempting to gain management access to a controller. It provides authentication, authorization, and accounting (AAA) services.
- **Local EAP**—Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST with PACs, EAP-FAST with certificates, and EAP-TLS authentication between the controller and wireless clients.

  Note Local EAP is designed as a backup authentication system. If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

- **LDAP database support**—You can configure a Lightweight Directory Access Protocol (LDAP) server as a backend database for use with local EAP. The controller queries the LDAP server for the credentials (username and password) of a particular user and uses them to authenticate the user.

  Note The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with protected access credentials (PACs) are not supported for use with the LDAP backend database.

- **Access control list (ACL) enhancements**—You can now apply an ACL to the controller central processing unit (CPU) or to a WLAN. An ACL is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). After ACLs are configured on the controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, and now to a WLAN to control data traffic to and from wireless clients or to the controller CPU to control all traffic destined for the CPU.
- **Load-based call admission control (CAC) for VoWLAN**—This feature allows lightweight access points and controllers to consider three additional variables when deciding how many voice calls to allow on the network: the bandwidth used by all traffic types, co-channel access point loads, and co-located channel interference. The access point accounts for these three new variables when determining if there is sufficient bandwidth to support a new VoWLAN call. Previously, only bandwidth-based CAC was supported.

Note Load-based CAC is supported only on lightweight access points (except the Cisco Airespace 1000 series access points and the Cisco Aironet 1500 series access points, which support only bandwidth-based CAC). If you enable load-based CAC in a network that contains a mixture of AP1000s and other lightweight access points, the AP1000s use bandwidth-based CAC while the other lightweight access points used load-based CAC. If you disable load-based CAC, all of the access points start using bandwidth-based CAC.

- **Symmetric mobility tunneling**—Using this feature, a foreign controller now sends a Layer 3 roaming client's packet back to its anchor controller through EtherIP tunneling rather than through a dynamic interface. The source IP address of the packet then becomes the management IP address of the foreign controller, allowing upstream routers that have reverse path filtering (RPF) to forward packets rather than discard them because the source IP address of the non-tunneled packet does not match the router subnet.
- **Guest N+1 redundancy and mobility failover**—Mobility group members can now send ping requests to one another to check the data and control paths among them to find failed members and reroute clients. This functionality provides guest N+1 redundancy for guest tunneling and mobility failover for regular mobility. Guest N+1 redundancy allows detection of failed anchors. Once a failed anchor controller is detected, all of the clients anchored to this controller are deauthenticated so that they can quickly become anchored to another controller. This same functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.
- **Workgroup bridge (WGB) support**—Cisco Aironet autonomous access points operating in WGB mode can now associate to Cisco Aironet lightweight access points (except Cisco Airespace AP1000 series access points) to provide an 802.11 wireless connection to wired devices. The WGB is supported only in client mode and not in infrastructure mode and must run Cisco IOS Release 12.4(3g)JA or later (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later (on 16-MB access points). WGB functionality is not supported for use with hybrid REAP.

  The autonomous WGB access point learns the MAC address of the wired client and then informs the lightweight access point and controller that the device is operating on the wireless network. This scenario provides transparent bridging for wired clients and secure roaming.
- **High-density networking**—High-density networking is introduced in this software release through the exclusive Cisco and Intel Business Class Wireless Suite Version 2 collaboration. To optimize wireless LAN capacity and improve overall network performance in dense, multi-cell wireless networks, this release introduces high-density (or pico cell mode) parameters on the controller. Using these parameters, you can manually specify global values for receiver sensitivity threshold, clear channel assessment (CCA) sensitivity threshold, and transmit power values across all Cisco lightweight access points registered to a given controller. High-density networking is supported on all Cisco lightweight access points (except the wireless mesh access points) and on notebooks using the Intel PRO/Wireless 3945ABG and Intel Wireless WiFi Link 4965AG clients.
- **Regulatory domain update for Japan**—The Japanese regulations allow the regulatory domain that is programmed into an access point's radio to be migrated from the -J domain to the -U domain. New access points for the Japanese market contain radios that are configured for the -P regulatory domain. -J radios are no longer being sold. In order to make sure that your existing -J radios work together with the new -P radios in one network, you need to migrate your -J radios to the -U domain.
- **Multiple country code support**—This release allows you to configure up to 20 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller. This feature is not supported for use with Cisco Aironet mesh access points.

- **Dynamic frequency selection (DFS)**—This release adds DFS functionality to the -A (U.S., Canada, and Philippines), -N (Mexico, Australia, Hong Kong, India, and New Zealand), and -T (Taiwan) regulatory domains. Prior to this release, DFS was already enabled for many other regulatory domains, including -E, -J, and -K . DFS is enabled automatically on the following Cisco lightweight access points that are configured for use in these regulatory domains: AP1130, AP1230, and AP1240. DFS affects channels 52 to 64 and 100 to 140 of the 802.11a radio. The access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them.

  Note FCC DFS is enabled only for AP1130s with a new FCC ID. Refer to the "FCC DFS Support on AP1130s" section on page 16 for details.

- **Addition of troubleshooting CLI commands**—Four controller CLI commands have been added to this release to aid in gathering information and debugging issues: **show process cpu**, **show process memory**, **show tech-support**, and **show running-config**.

New CCXv4 and CCXv5 Features

- **Client management frame protection (MFP)**—Client MFP is now available for CCXv5 client devices. In the previous 4.0 software release, only infrastructure MFP, which protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by access points, was available. In this release, the new client MFP feature allows a client to detect a spoofed management frame at the first instance of an attack and generate an intrusion detection system (IDS) alert to the device interface.
- **Expedited bandwidth requests**—This feature enables CCXv5 clients to attach a priority to specific types of call requests, such as emergency 911 calls, or to specific devices that are tagged as high priority, such as a senior executive's call from an IP soft phone while on a business trip.
- **Radio measurement requests enhancement**—The radio measurement request feature has been expanded to enable the controller to obtain information on the radio environment from the client's perspective (rather than from just that of the access point). In this case, the access points issue unicast radio measurement requests to a particular CCXv4 client. The client then sends various measurement reports back to the access point and onto the controller. These reports include information on the radio environment and data used to interpret the location of the clients.

New Location Features

- **Support for Cisco format RFID tags**—The controller supports both Aeroscout format RFID tags and now Cisco format RFID tags. The Location Appliance uses the Location Protocol (LOCP) to receive chokepoint, battery status, vendor-specific, telemetry, and emergency information for Cisco format tags.
- **Location enhancements**—This release improves location accuracy by gathering received signal strength indicator (RSSI) measurements from access points all around the client of interest. This new controller CLI command enables you to view the current location configuration values: **show advanced location summary**.

New Mesh Features

- **Mesh high-speed roaming**—This release supports high-speed roaming of CCXv4-compliant clients at speeds up to 70 mph in outdoor mesh deployments. An example application might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network.
- **Mesh background scanning**—This feature allows Cisco Aironet 1505 and 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points.
- **Routing around interference**—You can configure a wireless secondary backhaul between two Cisco Aironet 1510 Access Points to provide a temporary path for traffic that cannot be sent on the primary backhaul due to intermittent interference. Traffic is automatically diverted, as necessary, packet by packet from the primary backhaul to the secondary backhaul.
- **Backhaul client access**—When this feature is enabled, Cisco Aironet 1510 Access Points allow wireless client association over the 802.11a radio. This implies that a 1510 access point may carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, the AP1510 carries backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio.
- **Mesh call admission control (CAC)**—You can now configure bandwidth-based, or static, CAC on the controller to manage voice and video quality on the mesh network. This feature enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and comparing it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the access point rejects the call.

  Note For CAC to operate properly with mesh access points, enable bandwidth-based CAC on both the 802.11a and 802.11b/g radios. Also, make sure to keep load-based CAC disabled when using mesh CAC.

- **Mesh security**—You can now define the security mode for mesh access points: either Pre-Shared Key (PSK) or Extensible Authentication Protocol (EAP). Only local authentication is supported for EAP, and it is provided by the controller.
- **Mesh statistics**—You can now view mesh statistics and neighbor statistics for specific access points using the controller GUI or CLI.

GUI Enhancements

- **802.3 bridging enhancement**—You can now configure 802.3 bridging through the controller GUI. Previously, you could configure this feature only through the controller CLI. This feature enables the controller to support 802.3 frames and the applications that use them, such as those typically used for cash registers and cash register servers.
- **Cisco Discovery Protocol (CDP) enhancement—**You can now configure CDP through the controller GUI. Previously, you could configure this feature only through the controller CLI. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices. You can enable CDP on both controllers and access points. In addition, you can view the CDP neighbors on all interfaces and for all access points connected to the controller.

- **RM channel selection**—You can now specify the channels that the dynamic channel allocation (DCA) algorithm considers when selecting the channels to be used for RRM scanning using the controller GUI. Previously, you could configure this feature only through the controller CLI.

Other Changes

These additional changes are applicable to controller software release 4.1.171.0:

- The Airespace AS1200 is not supported for use with controller software release 4.1.171.0. The Airespace AS1200 (not to be confused with the Cisco Aironet AP1200) was never sold by Cisco and predates Cisco's acquisition of Airespace. If you attempt to connect an Airespace AS1200 to a controller running this software, the access point reboots continuously.
- There is no deployment restriction on the number of hybrid-REAP access points per location. However, the minimum bandwidth restriction remains 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.

4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing an antenna, remember:
   a. **Do not** use a metal ladder.
   b. **Do not** work on a wet or windy day.
   c. **Do** dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**
7. If any part of an antenna system should come in contact with a power line, **do not touch it or try to remove it yourself. Call your local power company**. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

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

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

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

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

Important Notes

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

802.11n

802.11n radios are not supported for use with controller software release 4.1.171.0. These radios will be supported in a future controller release. In this release, please disregard any 802.11n-related parameters that appear on the controller GUI pages and any 802.11n-related controller CLI commands.

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.171.0, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. Cisco recommends that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

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

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

FCC DFS Support on AP1130s

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

Pings Supported on the Controller

Controller software release 4.1.171.0 is designed to support ICMP pings to the management interface either from a wireless client or a wired host. ICMP pings to other interfaces configured on the controller are not supported.

Access Point Radios Are Not Enabled After Upgrading to 4.1.171.0

After you upgrade the controller in the Catalyst 3750G Wireless LAN Controller Switch to software release 4.1.171.0, the access point radios are not enabled. This issue occurs because the switch is not correctly recognizing the access points. To work around this issue, uncheck the **CDP State** check box on the AP Configuration > CDP Template page.

Setting the Retransmit Timeout Value for TACACS+ Servers

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

Configuring an Access Point's Pre-Standard Power Setting

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

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

A Cisco pre-standard 15-watt switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco pre-standard 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 pre-standard 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 may need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

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

Using CCKM with CB21AG Client Adapters

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

DHCP Option 60 and 1500 Series Access Points

The VCI string for DHCP option 60 on 1500 series access point changes to "Cisco AP c1500" after the access points are upgraded to controller software release 4.1.171.0

AP1000 and Radar Detection

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

Controller Functions that Require a Reboot

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

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

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

Multicast Queue Depth

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

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

2106 Controller LEDs

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

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

Resetting the Configuration on 2006 Controllers

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

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

Caution Do not attempt to reset the controller's configuration by choosing Option 5, Clear Config from the boot menu unless you have successfully upgraded to the ER.aes image on Cisco.com.

Rate-Limiting on the Controller

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

IPSec Not Supported

Software release 4.1.171.0 does not allow you to choose IPSec as a Layer 3 Security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 Security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 3.2 or wait for a future release.

4400 Series Controllers Do Not Forward Subnet Broadcasts through Guest Tunnel

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

Re-enable Broadcast after Upgrading to Release 4.0.206.0

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

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

config network broadcast enable

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

Service Modules Supported in the Catalyst 6500 Series Switch

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

Connecting 1100 and 1300 Series Access Points

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

Joining Delay for 1500 Series Access Points

The 1500 series access points may take up to 10 minutes to fully join the controller on initial startup.

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

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

Preventing Clients from Accessing the Management Network on a Controller

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

Voice Wireless LAN Configuration

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

Operating Mesh Networks through Switches and Routers

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

Cisco 7920 Wireless IP Phone Support

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

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

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

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

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

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

Changing the IOS LWAPP Access Point Password

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

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

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

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

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

"ERROR!!! Command is disabled."

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

Exclusion List (Blacklist) Client Feature

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

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

RADIUS Servers and the Management VLAN

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

Cisco 1000 Series Access Points and WMM

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

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

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

Lightweight Access Point Connection Limitations

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

RADIUS Servers

This product has been tested with the following RADIUS servers:

- CiscoSecure ACS 3.2, 3.3, and 4.0
- Steel-Belted RADIUS Enterprise edition v4.4.337
- IAS Windows 2003

Management Usernames and Local Netuser Names

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

802.1x and Microsoft Wireless Configuration Manager

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

Using the Backup Image

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

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

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

Home Page Retains Web Authentication Login with IE 5.x

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

Rogue Location Discovery Protocol (RLDP)

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

Ad-Hoc Rogue Containment

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

Changing the Default Values of SNMP Community Strings

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

Changing the Default Values for SNMP v3 Users

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

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

Features Not Supported on 2000 and 2100 Series Controllers

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

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

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

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

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

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

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

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

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.

2006 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2000 Series Controller

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

Upgrading External Web Authentication

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

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

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

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

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

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

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

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

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

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

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

}
```

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

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

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

<tr align="center">

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

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

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

Caveats

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

Open Caveats

These caveats are open in controller software release 4.1.171.0.

Most Significant Open Caveats

These are the most significant open caveats in controller software release 4.1.171.0. You may want to pay special attention to them as they affect some of the new features in this release.

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

  Workaround: Clear the access point's static IP address by hand.

  Note The Mode button does not work on autonomous access points that have been converted to lightweight mode.

- CSCsh63939—Some TACACS+ accounting commands are not logged or are logged incorrectly.

  Examples of unlogged commands:

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

Examples of incorrectly logged commands:

- The **config 802.11b txPower global 1** command is logged as **802.11b txPower global off**.
- On the 2006, 2106, and controller network modules, the IP addresses for some of the commands are displayed in reverse order. The IP address appears as D.C.B.A instead of A.B.C.D. For example, **acl rule destination address test 2 192.168.0.11 255.255.255.0** is logged as **acl rule destination address test 2 11.0.168.192 0.255.255.255**.

Workaround: None at this time.

- CSCsh89752—When the controller is using an external or local authentication server, the username for some EAP-FAST clients may show as "PEAP" followed by the client's MAC address. However, everything works fine, and the client is able to authenticate and pass data.

  Workaround: None at this time.

- CSCsh98959—In controller software release 4.0.206.0 and later, the WLAN override feature does not work properly if the profile name does not match the SSID.

  Workaround: Configure the same profile name and SSID for the WLAN.

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

  Workaround: None at this time.

- CSCsi29976—If you connect an 1130 or 1240 access point to port 7 or port 8 of a 2106 controller with PoE enabled and reboot the access point, the access point powers up, but both radios will be down.

  Workaround: Disable CDP for the access point.

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

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

- CSCsi43822—If you use the controller GUI or CLI to disable and save an existing LDAP server configuration, the LDAP server configuration is re-enabled after a controller reboot.

  Workaround: Remove the LDAP server instead of disabling it.

- CSCsi52637—Access point failover may not function correctly for Cisco WiSM controllers. After access points fail over to the secondary controller, only a few access points initially fall back successfully to the primary. Some may wait for 30 to 40 minutes to fall back, and some never fall back. This issue occurs only when Cisco Aironet 1000 series lightweight access points are present in the network.

  Workaround: Reboot the access point, and make sure that the access point and controller are on different subnets.

- CSCsi53016—You cannot change the serial port baud rate using the controller GUI.

  Workaround: Use the controller CLI.

Additional Open Caveats

These caveats are also open in controller software release 4.1.171.0.

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

  Workaround: Use the CLI configuration wizard.

- CSCsb01983—The controller web configuration wizard is not reachable after making repeated invalid entries for the management interface port. If an operator connects to the wizard on address 192.168.1.1 and enters an invalid port number on the Management Interface page, the operator is redirected at the end of the wizard to the Management Interface page to correct the port. If the operator enters an incorrect port and submits, the wizard becomes inaccessible.

  Workaround: Reboot the controller through the CLI to access the wizard again.

- CSCsb07168—The AP1000 receives packets that are tagged with incorrect received signal strength indicators (RSSIs) on its 802.11a radio when the RSSI value is around –75 dBm. This may slightly offset the location of 802.11a items.

  Workaround: None at this time.

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

  Workaround: Ignore the prompt and exit as usual.

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

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

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

  Workaround: None at this time.

- CSCsc03214 and CSCsg09976—If a WLAN is configured to use web policy for Layer 3 security authentication and is also configured to use the controller's default authentication page, the client cannot access the authentication page using HTTPS.

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

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

  Workaround: Replace the controller.

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

  Workaround: Follow these steps:

  a. Refresh the configuration from the switch to WCS (deleting any differences).
  b. Clear the configuration on the controller.
  c. Complete the setup wizard, making sure to set the same IP address, community string, and country code setting.
  d. Use WCS to restore the configuration to the controller.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: Use the controller CLI.

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

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

- CSCse66714—When you use the controller GUI to set a static IP address on a different subnet than the one the access point is on, the access point reboots, but the GUI page does not refresh. When the access point reboots, it sometimes uses a fallback address, and the display shows the static IP address configuration as well as the IP address it is using.

  Workaround: Check the configuration using the **show ap config** *name* CLI command, which shows the access point using a fallback address.

- CSCse76616—After a reload of the Catalyst 6500 switch and the Supervisor 720, the Supervisor 720 reports a duplicate service port IP address for the WiSM, even though no duplicate IP address for the service port is configured.

  Workaround: None at this time. Functionality is not impacted as a result of messages.

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

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

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

  Workaround: None at this time.

- CSCsg03174—The controller network module in the Cisco 28/37/38xx Series Integrated Services Router does not reject incompatible software.

  Workaround: None at this time.

Caution Make sure you download the proper software images to this controller.

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

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

- CSCsg26982—The 4402 controller may not respond properly to the SNMP server interface discovery.

  Workaround: None at this time.

- CSCsg32267—The controller transmits data at the 1-Mbps rate even though data transmission at this rate is disabled.

  Workaround: None at this time.

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

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

- CSCsg36747—The Clear Counters button on the Controller Statistics page does not clear the controller's counters.

  Workaround: None at this time.

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

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

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

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

- CSCsg72036—A controller running software release 4.0.179.8 occasionally experiences an issue with certain client cards sending bad information to a 1240 series access point, which results in the access point going into discovery mode with the error message "L2 Queue Full."

  Workaround: If the clients are using 802.11x, increase the EAP-Identity-Request Timeout value to 5 seconds and decrease the number of EAP-Identity-Request Max Retries from the default value of 20 to 5 or 6 using the **config advanced eap identity-request-timeout** and **config advanced eap identity-request-retries** CLI commands, respectively.

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

  Workaround: None at this time.

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

  Workaround: Use AES encryption or 802.1x dynamic keys.

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

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

- CSCsg81953—Controllers sometimes report IDS disassociation flood attacks against valid clients in which the attacker's MAC address is that of an access point joined to that controller.

  Workaround: None at this time.

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

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

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

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

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

  Workaround: None at this time.

- CSCsh42173—RFID tags time out quickly when their auto-timeout feature is enabled.

  Workaround: None at this time.

- CSCsh64888—You can use the controller CLI or WCS to place an AP1130AG on the WCS map and to configure an external antenna for it, which should not be possible. You can also configure the gain (in dBm) for the new antenna and save the changes. When you try to access the maps using WCS afterward, you see error messages about the configurations you created for the access point.

  Workaround: None at this time.

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

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

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

- CSCsh73171—When you enable CCKM on the controller for use with CB21AG client adapters, some CCKM configuration settings cause the client to send an association request in the middle of CCKM, thereby resulting in full authentication rather than CCKM. See the "Using CCKM with CB21AG Client Adapters" section on page 17 for details on which CCKM configuration settings do and do not operate properly.

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

- CSCsh77143—When a multicast ARP request is tunnelled using EoIP from an anchor controller to a foreign controller with the proxy ARP disabled, the foreign controller drops the ARP request and does not forward it to the associated client.

  Workaround: None at this time.

- CSCsh88005—When you create a WLAN using the controller GUI, you cannot define a session timeout of 0 for WLANs with PSK encryption.

  Workaround: Create the WLAN with a session timeout of 1800 and then change the timeout value to 0.

- CSCsh88426—You may experience intermittent access to the controller, whereby two gigabit ports are responsive and the other two are not. In this case, you may see console error messages similar to the following: "Msg 'Set system global config' of System Table failed, Id = 0x006e303a error value = 0xfffffffc."

  Workaround: Reboot the controller.

- CSCsh90008—When the configuration between the controller and WCS is not synchronized, the link between the parent and child access points is not drawn. A directional arrow is seen from the child to the parent access point, but the link is not drawn.

  Workaround: Refreshing the configuration from the controller solves the problem after a while.

- CSCsh92460—A TACACS+ user with the Management privilege can add or delete local management users with read-write or lobby-ambassador permission.

  Workaround: Only super users should create and delete management users. Do not create users with the Management privilege in TACACS+ servers.

- CSCsh95128 and CSCsi33506—Rogue Location Detection Protocol (RLDP) does not operate properly for hybrid-REAP access points.

  Workaround: None at this time.

- CSCsh95306—802.1x reauthentication may cause disruptions in voice calls, and there is no way to stop the reauthentication from either the controller GUI or CLI.

  Workaround: Set the WLAN session timeout to a high value, such as 65535 seconds.

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

  Workaround: None at this time.

- CSCsi05989—Client reauthentication does not occur for a WLAN configured for WPA+WPA2+CCKM after the configured session timeout expires. This issue occurs only if the client roams.

  Workaround: None at this time.

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

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

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

  Workaround: None at this time.

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

  config network multicast

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

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

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

  show ap stats 802.11b *Cisco_AP*

  show ap stats 802.11a *Cisco_AP*

  Workaround: None at this time.

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

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

- CSCsi16810—If an access point using infrastructure management frame protection (MFP) goes into the hybrid-REAP standalone mode, the access point ceases to attach MFP message integrity check (MIC) Aironet information elements (IEs) to transmitted frames because infrastructure MFP is not supported in this mode. Access points connected to other controllers within the same mobility group may generate "Missing MIC" alerts under some circumstances.

  If the reason for the access point to go into the standalone mode is that the controller has lost Ethernet connectivity, other access points within the mobility group are not informed that the access point in the standalone mode is no longer transmitting protected frames and may report "Missing MIC" MFP errors until the controller recovers connectivity or the access point joins another controller.

  Workaround: The problem rectifies itself when the controller recovers connectivity or the access point joins another controller. You can safely ignore "Missing MIC" alerts generated under these conditions. No action is necessary.

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

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

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

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

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

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

- CSCsi29308—The **show ap cdp** command does not show the CDP information for all access points.

  Workaround: Use the **show ap cdp** *Cisco_AP* command.

- CSCsi30017—The **session 1 processor 1** command is not working on the Catalyst 3750G Wireless LAN Controller Switch.

  Workaround: Enter this command on the controller:

  config network mgmt-via-dynamic-interface

- CSCsi47353—The Appletalk protocol is not supported in controller software release 4.1.171.0.

  Workaround: None at this time. This issue will be resolved in an upcoming 4.1 release.

- CSCsi49767—If a WLAN is configured with an interface ACL and an access point group has been applied to the access point, the controller may reboot when a client joins the access point.

  Workaround: Do not configure an interface ACL with the access point group feature.

- CSCsi52006—The access point radio operational status is "Down" after setting the access point to factory defaults when using power over Ethernet (PoE) from certain pre-standard 15-Watt switches.

  Workaround: Enter this command on the controller to enable the pre-standard state:

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

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

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

- CSCsi57702—The following controller CLI command to enable global public safety on mesh access points is not supported in software release 4.1.171.0: **config ap public-safety enable all**.

  Workaround: None at this time.

- CSCsi59501—7921 calls do not go through when the hybrid-REAP access point is in standalone mode.

  Workaround: None at this time.

- CSCsi60185—Sometimes wireless clients running 802.1x authentication such as PEAP may not get authenticated while connecting to access points.

  Workaround: Enter this CLI command on the controller to check the EAP-Request Timeout and EAP-Request Max Retries values:

  show advanced eap

  Information similar to the following appears:

  ```
  EAP-Identity-Request Timeout (seconds)..... 1
  EAP-Identity-Request Max Retries.............. 20
  EAP Key-Index for Dynamic WEP................. 0
  EAP Max-Login Ignore Identity Response..... enable
  EAP-Request Timeout (seconds)................. 3
  EAP-Request Max Retries..................... 3
  ```

  If these parameters are not already set to a value of 3, enter these commands to set them to 3:

  config advanced eap request-timeout 3

  config advanced eap request-retries 3

Resolved Caveats

These caveats are resolved in controller software release 4.1.171.0.

- CSCsb55937—VLAN-tagged large ICMP packets that need to be fragmented are not sent by Cisco Aironet 1000 series lightweight access points in direct-connection mode. Ping replies never come back when the access point sends requests to a gateway from a wireless client using large 1500-byte packets and with the RADIUS override configured with any 1p tag.
- CSCsc05495—A controller running software release 3.0.107 intermittently sends a state attribute 24 in an access-request packet.
- CSCsc05574—In the ETSI (-E) regulatory domain, the 2.4-GHz radio in the AP1000 displays the maximum power level as 14.5 dBm when the correct maximum power value should be 14 dBm.
- CSCsc11660—The current country screen is not 100% accurate for all deployment scenarios, which may cause confusion in some instances.
- CSCsc75351—The **debug mac addr** *client_mac_address* command is designed to limit the debug output to the specified single client. In controller software release 3.2.78.0, this command is not filtering client traffic for client MAC addresses entered with and without colons.
- CSCsd76868—When WLAN ID 1 does not exist, the Rogue Location Detection Protocol (RLDP) reports a minor alarm when a critical alarm should be reported.
- CSCsd87382—Bridging functionality for REAP devices is not available on OEM builds of controller software.
- CSCse04713 and CSCsf09647—The AP1000 firmware may drop broadcast frames sent from rogue access points.
- CSCse10109—For WMM clients without TSPEC support, ACM must be disabled for proper QoS mapping.
- CSCse28941—AP1510 mesh access points (MAPs) using dynamic frequency selection (DFS) and deployed in the European Telecommunications Standards Institute (ETSI) domain may detect what they perceive to be radar signals, even if no radar is present.
- CSCse31500 and CSCsc02860—When users download the software image to a Cisco WiSM for the first time, the WiSM fails to download the new image to flash memory.
- CSCse33146—The 802.1x code does not send M5 on the first attempt.
- CSCse33427—The controller CLI commands do not work properly when trying to map port 3 or 4 to an interface on the 4402 controller.
- CSCse40636—On auto-anchor WLANs, the foreign controller incorrectly forwards multicast traffic to the auto-anchor WLAN.
- CSCse65613—You cannot rate limit or block specific multicast or broadcast traffic from the wired network when broadcast/multicast is enabled on the controller. When you enable multicast, you also enable broadcast traffic. However, normal ACLs do not block certain multicast addresses or rate limit broadcasts coming from the wired network. A broadcast storm or large number of multicast packets generated on the wired network are transmitted on the wireless network.
- CSCse85135—When you reset an access point, the following incorrect message appears on the controller GUI: “After reset, AP will associate with Primary Switch if configured else associate with Master Switch.” In reality, the access point looks for its primary, secondary, and tertiary controllers first; then a master controller; and finally the least-loaded controller with available access point ports.

- CSCse93890—The controller and access point clocks are not synchronized. Therefore, the access points may report timestamps that are out of sync with each other and the controller.
- CSCsf08091—You may be unable to create more than 64 interfaces using the controller GUI.
- CSCsf09647—RLDP is not working correctly for autonomous access points converted to lightweight mode if the broadcast DHCP offer is sent by a rogue.
- CSCsf26215—Indoor access points that do not belong to the mesh network may join the mesh controller.
- CSCsf27479 and CSCsd54750—The Cisco WiSM may display numerous timeout messages.
- CSCsf29806, CSCsg70979, and CSCsg71039—When a mesh access point's (MAP's) root access point (RAP) goes down, the MAP falls back to the default bridge group name (BGN) and joins the controller through another RAP. When the first RAP comes back up, the MAP reverts back to the configured BGN and joins the first RAP. However, the first RAP declares the MAP as the default child, and the MAP declares the first RAP as the default parent, which is incorrect.
- CSCsg03023—The controller supports only 500 RFID tags when it is expected to support 5000.
- CSCsg21341—If you change a lightweight access point from DHCP to a static IP address and reboot the access point, it does not attempt to resolve the controller using a DNS of 255.255.255.255 or the DNS server it had when it was using DHCP.
- CSCsg26493 and CSCsg89311—The controller sometimes reboots when downloading a customized web authentication file.
- CSCsg29291—If you change the name of an AP1010 that is connected to a 2106 controller, the AP Name field is not propagated correctly for the beacon within the Aironet information element (IE).
- CSCsg36361—This issue is included in the Cisco Security Advisory "Multiple Vulnerabilities in the Cisco Wireless LAN Controller and Cisco Lightweight Access Points" published at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070412-wlc.
- CSCsg40594—If you connect an access point on a VLAN other than the management VLAN, multicast traffic is fragmented by the controller and sent to the access point with LWAPP encapsulated. Only the IP fragmented packet is received. The first packet is dropped due to the ACL applied, and the access point reboots after several minutes.
- CSCsg40655—The controller should not use two port numbers for different size packets. When the controller encapsulates the UDP payload from a multicast packet, it adds two different distribution ports for small and large packets.
- CSCsg46430—Bridging information always shows the Hop Count as zero.
- CSCsg59589—This issue is included in the Cisco Security Response "Multiple Vulnerabilities in OpenSSL Library" published at http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20061108-openssl.
- CSCsg64309—Roaming fails between hybrid-REAP access points using local switching and web authentication.
- CSCsg64815—The traplog for the 2006 controller and the Controller Network Module has a very large port number.
- CSCsg66265—Client WMM states may not update properly. If a client associates to an access point as WMM capable, disconnects, is changed to non-WMM capable, and finally re-associates, the controller sends traffic to the client with a QoS header.
- CSCsg69021—Fast roaming with WPA2+CCKM on dynamic interfaces may not operate properly.

- CSCsg70979—When a mesh access point (MAP) joins the controller with the default bridge group name (BGN), the MAP BGN should appear as "DEFAULT." However, the MAP BGN value is empty if the MAP does not have a BGN set or if the set value shows up on the controller even though the MAP joined the controller with the "DEFAULT" BGN string.
- CSCsg71421—The **show qos profile** command does not operate properly. The controller does not allow any further input after this command is entered.
- CSCsg71469—When an AP1210 is in the Alert state, it may send deauthentication frames to a rogue access point.
- CSCsg72051—The Wi-Fi Multimedia (WMM) information element broadcast by 1000 series access points is not recognized by some wireless devices. The devices that do not recognize the WMM information element can associate to a 1000 series access point but cannot maintain WMM interoperability with the access point.
- CSCsg75863—If another device on the network takes over the AP-manager IP address, the controller does not defend its AP-manager IP address. As a result, the ARP cache on the default gateway router has with the wrong MAC address, and the access points drop off the controller and bring down the wireless network.

  Note After the default 4-hour ARP refresh interval, the access points rejoin the controller if the device that took over the AP-manager IP address is removed.

- CSCsg83671—There is no way to transfer a core-dump file from the controller to a TFTP server.
- CSCsh04777—The AP1000 does not periodically send neighbor packets on the non-dynamic frequency selection (DFS) channels (36-48). As a result, the access point is hindered from properly forming a neighborhood with other access points in the same RF domain.
- CSCsh11826—After you search by Ethernet MAC address on the controller, the access point list does not appear.
- CSCsh12616—Pango tags do not obtain a DHCP IP address when a mobility group member is defined on the controller.
- CSCsh19882—The IP option in the Protocol drop-down box on the Access Control Lists > Rules > New page should be changed to "IP in IP" because it permits or denies IP-in-IP packets.
- CSCsh20492—When mesh access points (MAPs) have more than one SSID, they may reboot after receiving a configuration request from the controller.
- CSCsh31384—When Ethernet broadcast and multicast are enabled on the controller and a wired host sends broadcast packets, the controller does not forward the packets to the access points.
- CSCsh32320—The Max Retry Count parameter cannot be set to zero.
- CSCsh35306—Unicast ARPs may drop from export-foreign clients because the IP address is not known at the foreign controller.
- CSCsh38353—To enable an SNMP device to determine on which interface a rogue access point is being detected, radioType must be added to the bsnRogueAP table.
- CSCsh42496—Ethernet port settings cannot be changed on IOS-running access points.
- CSCsh44486—A 1200 series access point sometimes reboots when a client device is associated to the radio interface that you are configuring.

- CSCsh47269—In software releases 4.0.179 and earlier, broadcast and multicast forwarding were both controlled with a single global flag that enabled multicast. In software release 4.0.206, these functions were broken into separate configuration flags: one that controls broadcast and one that controls non-broadcast multicast. If you have multicast enabled in software releases 4.0.179 and earlier, the broadcast flag is left disabled after upgrading to software release 4.0.206. As a result, some applications that rely on broadcast do not work after the upgrade.
- CSCsh47364—When access point debugging is enabled on a controller and you enter **debug lwapp** *?* during a telnet or SSH session to the controller, the controller reboots.
- CSCsh47906 and CSCsh50966—The controller sometimes fails to answer unicast ARP requests for the AP-manager interfaces. As a result, there might be sporadic interruptions in connectivity at ARP refresh time, resulting in the periodic loss of associations for access points associated through AP managers other than the first (ap-manager). This scenario is especially likely if the default router is running an IOS version that is subject to CSCeb53542.
- CSCsh48977—The controller IP stack becomes inoperable on a large Layer 2 subnet. The controller stops responding to pings, SNMP, and other management traffic, and RADIUS stops working. Access points stay connected, but client devices are able to associate and pass traffic only on WLANs that do not require authentication.
- CSCsh49310—Clearing the configuration on a 2000 series controller sometimes corrupts the image.
- CSCsh50527—NPU truncates padding from unicast ARP frames. Access points now use the length field in the LWAPP header to determine the number of bytes to transmit over the air. As a result, padding is stripped from unicast ARP frames.
- CSCsh61347—In some regulatory domains outside the U.S. and Canada, mesh access points fail to join a controller after they are upgraded from software release 4.0.179.11 to 4.0.206.
- CSCsh64994—RADIUS account records are not generated when an access point is configured in hybrid-REAP mode with a locally switched SSID.
- CSCsh67106—The AAA interface override results in ACLs that are sometimes not installed.
- CSCsh68089—Access points connected directly to a port on 2000 or 4400 series controllers sometimes fail to receive an IP address through DHCP.
- CSCsh68460—The controller allows the Web Authentication Headline template with an apostrophe to be successfully applied from WCS even though apostrophes are not allowed on the controller.
- CSCsh69985—When a Cisco 7920 phone is associated to a lightweight access point, the controller sometimes fails to forward packets to the phone.
- CSCsh73667—The controller drops the broadcast DHCP offer for the RLDP feature.
- CSCsh74316—In controller software release 4.0.179.8, guest tunneling between a foreign controller and an anchor controller may fail due to a WLAN security policy mismatch.
- CSCsh77760—Access point fallback mode does not work correctly for 1000 series access points when master controller mode is enabled. The access points should leave their controller and migrate to the master controller; however, they stay attached to the current controller.
- CSCsh80542—If the AP1000 has both radios disabled and it receives a new IP address, it does not send the IP address payload to the controller. The result is multiple ARP entries on the controller.
- CSCsh81746—The GE Dash unit requires padding. It is an 802.11 client that discards any received packet that has an 802.11 payload of less than 46 bytes.
- CSCsh84930—The RFID telemetry vendor field does not support up to 128 bytes.
- CSCsh85147—The controller may reboot when handling large telemetry values.

- CSCsh85278 and CSCse42329—When the controller sends an IP packet to a node through its default gateway, it uses the MAC address of the interface where a packet was originated instead of the MAC address learned through the ARP process. This approach impacts failover performance, traffic profiles, and any network designs that rely on the standard behavior of an IP stack.
- CSCsh88784—You cannot change the status of known rogue access points on the controller GUI, and the controller CLI displays no information.
- CSCsi15393—The third RFID tag address is not being configured properly in the radio. As a result, the radio does not always forward the packet received from the tag to the access point.

If You Need More Information

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

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

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

Troubleshooting

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

http://www.cisco.com/en/US/support/index.html

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

Documentation Updates

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

Omissions

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

- DB-9 to DB-9 null modem cable

Related Documentation

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

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

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

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

Obtaining Documentation, Support, and Security Guidelines

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.