Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

November 11, 2008

Controller software release 4.1.185.10 is being released for FIPS customers.

To confirm the FIPS validation status of the 4.1.185.10 release for the Cisco Aironet 1131 and 1242 Lightweight Access Points, Cisco 4402 and 4404 Wireless LAN Controllers, Cisco Wireless Services Modules (WiSMs), and Catalyst 3750G Integrated Wireless LAN Controller Switches, refer to the NIST URLs below. If the 4.1.185.10 release appears on the NIST website, then the modules have been FIPS validated with this release. If the 4.1.185.10 release does not appear on the NIST site, then the modules are in-process for FIPS validation with this release.

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#913

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#955

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#957

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#958

These release notes describe open and resolved caveats for software release 4.1.185.10 for Cisco 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSMs); Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 (1505 and 1510) Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

Cisco Unified Wireless Network Solution Components

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

- Software release 4.1.185.10 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 2.01
- Cisco Wireless Control System (WCS) software release 4.1.91.0
- Cisco Wireless Control System (WCS) Navigator 1.0.91.0
- Location appliance software release 3.0.42.0
- Cisco 2700 Series Location Appliances
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 (1505 and 1510) Series Lightweight Access Points

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

2

OL-17927-01

Special Notice for Mesh Networks

Note Controller software release 4.1.185.10 does not support the new Cisco Aironet 1520 Series Mesh Access Point. If you intend to use this new access point, you must run controller software release 4.1.190.5, which supports mesh access points. If your network contains both 1520 mesh access points and Cisco non-mesh access points (such as 1240 series access points), you need to manage your 1520 mesh access points with one controller and your non-mesh access points with a second controller. If you have 1505 or 1510 mesh access points or both, you should connect them to the same controller as the 1520 mesh access points.

Note Cisco WCS software release 4.1.91.0 may be used to manage both mesh and non-mesh controllers (for example, controllers running software release 4.1.185.10 and 4.1.190.5). You do not need different instances of WCS to manage mesh and non-mesh controllers.

Controller Requirements

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

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

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

Software Release Information

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

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

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

Note 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.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01 **3**

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 LED 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 4.1.185.10

⚠

Caution Before upgrading your controller to software release 4.1.185.10, you must comply with the following rules.

- Controller software release 4.1.185.10 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 4.1.185.10 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), 4.0.206.0 (or a later 4.0 release), or 4.1.171.0 (or a later 4.1 release), you can upgrade your controller directly to software release 4.1.185.10. 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 4.1.185.10. Table 1 shows the upgrade path that you must follow before downloading software release 4.1.185.10.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

4   OL-17927-01

Table 1   Upgrade Path to Controller Software Release 4.1.185.10

Current Software Release	Upgrade Path to 4.1.185.10 Software
3.2.78.0	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.1.185.10.
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 4.1.185.10.
4.0.155.5	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.1.185.10.
4.0.179.11	
4.0.206.0 or later 4.0 release	You can upgrade directly to 4.1.185.10.
4.1.171.0, 4.1.181.0, or 4.1.185.0	You can upgrade directly to 4.1.185.10.

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

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 4.1.185.10 controller software 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**.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01   5

    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.

Step 5 Copy the controller software file (*filename*.aes) 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 After the download is complete, click **Reboot**.

Step 14 If prompted to save your changes, click **Save and Reboot**.

Step 15 Click **OK** to confirm your decision to reboot the controller.

Step 16 After the controller reboots, re-enable the WLANs.

Step 17 Re-enable your 802.11a and 802.11b/g networks.

Step 18 If desired, reload your latest configuration file to the controller.

Step 19 To verify that the 4.1.185.10 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

6

OL-17927-01

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.**

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers) ■

OL-17927-01

7

> ⚠️
>
> **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!**

■ Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

8

OL-17927-01

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 4.1.185.10. In this release, disregard any 802.11n-related parameters that appear on the controller GUI pages and any 802.11n-related controller CLI commands.

Disabling Radio Bands

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

MAC Filtering for WGB Wired Clients

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers) ■

OL-17927-01   **9**

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

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

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

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.185.10, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. Cisco recommends that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

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

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

FCC DFS Support on AP1130s

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

Access Point Radios Are Not Enabled After Upgrading to 4.1.185.10

After you upgrade the controller in the Catalyst 3750G Wireless LAN Controller Switch to software release 4.1.185.10, the access point radios are not enabled. This problem occurs because the switch is not correctly recognizing the access points through CDP and not enabling sufficient inline power for the radios. To work around this issue, uncheck the **CDP State** check box on the AP Configuration > CDP Template page on the controller GUI or enter **config ap cdp disable all** on the controller CLI.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

10

OL-17927-01

Inaccurate Transmit Power Display

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

Setting the Retransmit Timeout Value for TACACS+ Servers

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

Configuring an Access Point's PreStandard Power Setting

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

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

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

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

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

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

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01

11

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 4.1.185.10.

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.

Rate-Limiting on the Controller

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

Pings Supported to the Management Interface of the Controller

Controller software release 4.1.185.10 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.

■ **Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)**

12

OL-17927-01

Pinging from a Network Device to a Controller Dynamic Interface

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

IPSec Not Supported

Software release 4.1.185.10 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 4.0.

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.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01   13

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

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

Preventing Clients from Accessing the Management Network on a Controller

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

Voice Wireless LAN Configuration

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

Conducting a Radio Site Survey for Mesh Deployments

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

For detailed information on conducting site surveys and other factors to consider when planning your network (data rate, distance between access points, interference, and so on), refer to the *Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide* at
http://www.cisco.com/en/US/products/ps6548/tsd_products_support_series_home.html

Operating Mesh Networks through Switches and Routers

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

14

OL-17927-01

Cisco 7921 and 7920 Wireless IP Phone Support

When using Cisco 7921 and 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 7921 or 7920 phone uses the QBSS value to determine if they should associate to 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 7921 or 7920 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 7921 and 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 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.

- For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1* for instructions on enabling load-based CAC and other voice parameters.

- For a mixture of 7921 and 7920 phones, the WMM Policy must be set to Allowed and the 7920 AP CAC must be enabled on the WLAN.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01

15

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.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

16

OL-17927-01

Lightweight Access Point Connection Limitations

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

RADIUS Servers

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

Management Usernames and Local Netuser Names

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

802.1x and Microsoft Wireless Configuration Manager

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

Using the Backup Image

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

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

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

Home Page Retains Web Authentication Login with IE 5.x

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

Rogue Location Discovery Protocol (RLDP)

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01

17

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.

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.

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.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

18

OL-17927-01

```
<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.");
```

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01
19

```
        }

    }

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

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

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

    <tr align="center">

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

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

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

Caveats

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

Open Caveats

These caveats are open in controller software release 4.1.185.10.

- 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.

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

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

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

  Workaround: Manually clear the access point's static IP address.

■ Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

20

OL-17927-01

- CSCsd52483—When you make changes in the bootloader of a controller, 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.

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

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

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

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

  Workaround: Follow these steps to work around this issue:

  a. Configure the controller for Greenwich mean time (GMT), with no time-zone offset.

  b. During standard time, run with the standard offset.

  c. When DST goes into effect, manually configure the controller for the correct local time.

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01

21

- 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.

- 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**.

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

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsh54247—You cannot perform the following logging functions on the controller:

  – Setting the system logging severity to filter out-going syslog messages

  – Setting the syslog facility

  – Configuring multiple syslog servers on the controller

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- 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.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

22

OL-17927-01

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

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

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

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

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

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

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

  Workaround: None.

- CSCsi64689—If the existing power level is lower than power level 5 and you disable and then re-enable the WLAN, the transmit power for LWAPP-enabled access points changes to power level 1.

  Workaround: This is auto-corrected by RRM algorithms in subsequent runs.

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

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

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

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

  a. On the controller GUI, click **Wireless > 802.11a/n**.

  b. Click **DCA** under RRM.

  c. Uncheck all of the channels between 100 to 140.

  d. Click **Apply** to commit your changes.

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

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01   23

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

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

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

  Workaround: None.

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

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

Resolved Caveats

These caveats are resolved in controller software release 4.1.185.10.

- CSCsi91347—When CCXv4 Intel clients run a client bundle version prior to 10.5.1.0, the controller's message log might fill up with messages similar to "iappSocketTask: iappRecvPkt returned error."

- CSCsj56899—The controller does not send the hostname or IP address in the syslog message header, making it difficult to determine which controller sent the message.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

24 OL-17927-01

- CSCsk11540—When an access point joins a controller, duplicate messages are sent to the controller's NPU.

- CSCsk11550—When many access points join a Cisco WiSM, the NPU time message often appears on the console because BsnMDAframeMonitor does not run, the kernel socket buffer for control frames overflows, and ACKs from the NPU are dropped.

- CSCsk11558—When the controller receives LWAPP-encapsulated packets with the fromDS and toDS bits set, these packets are incorrectly queued on the control socket, which could cause ACKs from the NPU to be dropped when the socket buffer fills up.

- CSCsk13125—The **debug** controller CLI commands need to be filtered by MAC address in order to simplify the debugging process for large access point deployments.

- CSCsk13145—The controller sometimes sends LWAPP requests to an unregistered access point.

- CSCso30745—When a packet fails the admission control test, it is forwarded to the CPU instead of being discarded. This incorrect forwarding of many such packets could cause an overload of the CPU and a reaper reset.

- CSCso62922—EAP authentication might fail for clients when the controller is operating under a heavy load. The client responds to the Identity request, but the controller does not to process it and times out the authentication.

- CSCso81725—The controller's broadcast module is replicating CDP packets to all connected access points even if multicast is disabled. In addition, the controller is replicating broadcast orphan packets from a client even when multicast and broadcast are disabled.

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.

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

OL-17927-01　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　**25**

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

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.1.185.10 (For FIPS Customers)

26

OL-17927-01