



Controlling Lightweight Access Points

This chapter describes how to connect access points to the controller and manage access point settings. This chapter contains these sections:

- [Lightweight Access Point Overview, page 7-2](#)
- [Using the DNS for Controller Discovery, page 7-7](#)
- [Dynamic Frequency Selection, page 7-8](#)
- [Autonomous Access Points Converted to Lightweight Mode, page 7-9](#)

Lightweight Access Point Overview

This section describes Cisco lightweight access points.

Cisco 1000 Series IEEE 802.11a/b/g Lightweight Access Points

The Cisco 1000 series lightweight access point is a part of the innovative Cisco Wireless LAN Solution (Cisco Wireless LAN Solution). When associated with controllers as described below, the Cisco 1000 series lightweight access point provides advanced 802.11a and/or 802.11b/g Access Point functions in a single aesthetically pleasing plenum-rated enclosure. [Figure 7-1](#) shows the two types of Cisco 1000 Series IEEE 802.11a/b/g lightweight access point: without and with connectors for external antennas.

Figure 7-1 1000 Series Lightweight Access Points



A. External-Antenna Model B. Internal-Antenna Model

04031951

The Cisco WLAN Solution also offers 802.11a/b/g Cisco 1030 Remote Edge Lightweight Access Points, which are Cisco 1000 series lightweight access points designed for remote deployment, Radio Resource Management (RRM) control via a WAN link, and which include connectors for external antennas.

The Cisco 1000 series lightweight access point is manufactured in a neutral color so it blends into most environments (but can be painted), contains pairs of high-gain internal antennas for unidirectional (180-degree) or omnidirectional (360-degree) coverage, and is plenum-rated for installations in hanging ceiling spaces.

In the Cisco Wireless LAN Solution, most of the processing responsibility is removed from traditional SOHO (small office, home office) access points and resides in the Cisco Wireless LAN Controller.

Cisco 1030 Remote Edge Lightweight Access Points

The only exception to the general rule of lightweight access points being continuously controlled by Cisco Wireless LAN Controllers is the Cisco 1030 IEEE 802.11a/b/g remote edge lightweight access point (Cisco 1030 remote edge lightweight access point). The Cisco 1030 remote edge lightweight access point is intended to be located at a remote site, initially configured by a Cisco Wireless LAN Controller, and normally controlled by a Cisco Wireless LAN Controller.

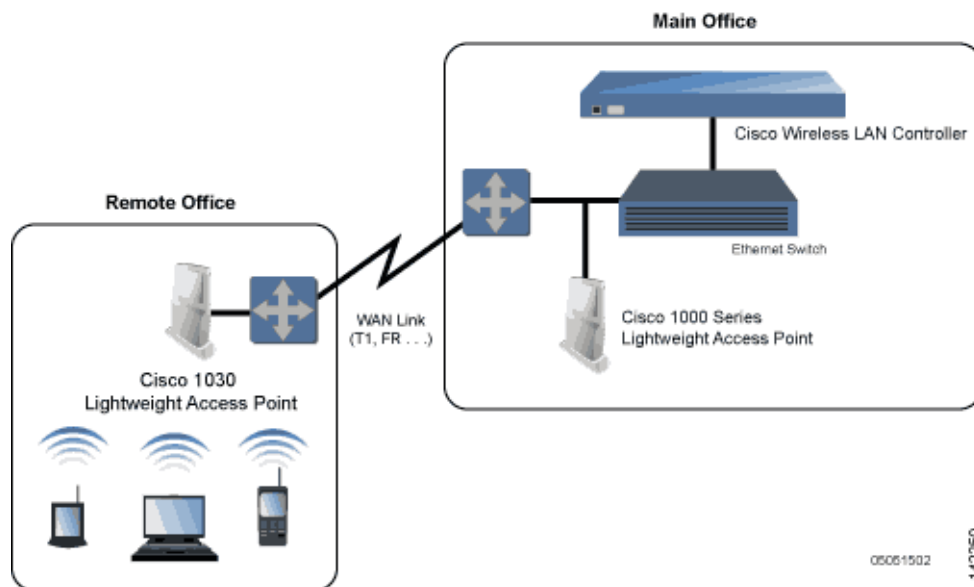
However, because the Cisco 1030 remote edge lightweight access point bridges the client data (compared with other Cisco 1000 series lightweight access points, which pass all client data through their respective Cisco Wireless LAN Controller), if the WAN link breaks between the Cisco 1030 remote edge lightweight access point and its Cisco Wireless LAN Controller, the Cisco 1030 remote edge lightweight access point continues transmitting wireless LAN 1 client data through other Cisco 1030 remote edge lightweight access points on its local subnet. However, it cannot take advantage of features accessed from the Cisco Wireless LAN Controller, such as establishing new VLANs, until communication is reestablished.

The Cisco 1030 remote edge lightweight access point includes the traditional SOHO (small office, home office) AP processing power, and thus can continue operating if the WAN link to its associated Cisco Wireless LAN Controller fails. Because it is configured by its associated Cisco Wireless LAN Controller, it has the same wireless LAN configuration as the rest of the Cisco Wireless LAN Solution. As long as it remains connected to its Cisco Wireless LAN Controller, it varies its transmit power and channel selection under control of the RRM, and performs the same rogue access point location as any other Cisco 1000 series lightweight access point.

Note that the Cisco 1030 remote edge lightweight access point can support multiple wireless LANs while it is connected to its Cisco Wireless LAN Controller. However, when it loses connection to its Cisco Wireless LAN Controller, it supports only one wireless LAN on its local subnet.

Figure 7-2 shows a typical Cisco 1030 remote edge lightweight access point configuration:

Figure 7-2 Typical 1030 Lightweight Access Point Configuration



Note that the Cisco 1030 remote edge lightweight access point must have a DHCP server available on its local subnet, so it can obtain an IP address upon reboot. Also note that the Cisco 1030 remote edge lightweight access points at each remote location must be on the same subnet to allow client roaming.

Cisco 1000 Series Lightweight Access Point Part Numbers

The Cisco 1000 series lightweight access point includes one 802.11a and one 802.11b/g radio. The Cisco 1000 series lightweight access point is available in the following configurations:

- AIR-AP1010-A-K9, AIR-AP1010-C-K9, AIR-AP1010-E-K9, AIR-AP1010-J-K9, AIR-AP1010-N-K9, and AIR-AP1010-S-K9 — AP1010 Cisco 1000 series lightweight access point with four high-gain internal antennas, and no external antenna adapters.
- AIR-AP1020-A-K9, AIR-AP1020-C-K9, AIR-AP1020-E-K9, AIR-AP1020-J-K9, AIR-AP1020-N-K9, and AIR-AP1020-S-K9 — AP1020 Cisco 1000 series lightweight access point with four high-gain internal antennas, and one 5 GHz external antenna adapter and two 2.4 GHz external antenna adapters.
- AIR-AP1030-A-K9, AIR-AP1030-C-K9, AIR-AP1030-E-K9, AIR-AP1030-J-K9, AIR-AP1030-N-K9, and AIR-AP1030-S-K9 — AP1030 Cisco 1000 series lightweight access point (Cisco 1030 remote edge lightweight access point) with four high-gain internal antennas, and one 5 GHz external antenna adapter and two 2.4 GHz external antenna adapters.

Refer to [Appendix D, “Supported Country Codes”](#) for information on supported regulatory domains.

The Cisco 1000 series lightweight access point is shipped with a color-coordinated ceiling mount base and hanging-ceiling rail clips. You can also order projection- and flush-mount sheet metal wall mounting bracket kits. The base, clips, and optional brackets allow quick mounting to ceiling or wall.

The Cisco 1000 series lightweight access point can be powered by Power over Ethernet or by an external power supply. The external power supply model is:

- AIR-PWR-1000 — Optional External 110-220 VAC-to-48 VDC Power Supply for any Cisco 1000 series lightweight access point.

The Single Inline PoE injector model is:

- AIR-PWRINJ-1000AF — Optional Single 802.3af Inline Power over Ethernet Injector for any Cisco 1000 series lightweight access point, powered by 90-250 VAC.

The projection and flush sheet metal wall mount bracket model is:

- AIR-ACC-WBRKT1000 — Optional sheet metal wall-mount bracket kit for any Cisco 1000 series lightweight access point. Includes one projection-mount and one flush-mount bracket per kit.

Cisco 1000 Series Lightweight Access Point External and Internal Antennas

The Cisco 1000 series lightweight access point enclosure contains one 802.11a or one 802.11b/g radio and four (two 802.11a and two 802.11b/g) high-gain antennas, which can be independently enabled or disabled to produce a 180-degree sectorized or 360-degree omnidirectional coverage area.



Note

Cisco 1000 Series lightweight access points must use the factory-supplied internal or external antennas to avoid violating FCC requirements and voiding the user’s authority to operate the equipment.

Note that the wireless LAN operator can disable either one of each pair of the Cisco 1000 series lightweight access point internal antennas to produce a 180-degree sectorized coverage area. This feature can be useful, for instance, for outside-wall mounting locations where coverage is only desired inside the building, and in a back-to-back arrangement that can allow twice as many clients in a given area.

Refer to [Appendix E, “Antenna Patterns for 1000 Series Access Points”](#) for antenna patterns.

External Antenna Connectors

The AP1020 and AP1030 Cisco 1000 series lightweight access points have male reverse-polarity TNC jacks for installations requiring factory-supplied external directional or high-gain antennas. The external antenna option can create more flexibility in Cisco 1000 series lightweight access point antenna placement.



Note

The AP1010 Cisco 1000 Series lightweight access points are designed to be used exclusively with the internal high-gain antennas, and have no jacks for external antennas.

Note that the 802.11b/g 2.4 GHz Left external antenna connector is associated with the internal Side A antenna, and that the 2.4 GHz Right external antenna connector is associated with the internal Side B antenna. When you have 802.11b/g diversity enabled, the Left external or Side A internal antennas are diverse from the Right external or Side B internal antennas.

Also note that the 802.11a 5 GHz Left external antenna connector is separate from the internal antennas, and adds diversity to the 802.11a transmit and receive path. Note that no external 802.11a antennas are certified in FCC-regulated areas, but external 802.11a antennas may be certified for use in other countries.

Antenna Sectorization

Note that the Cisco WLAN Solution supports Antenna Sectorization, which can be used to increase the number of clients and/or client throughput a given air space. Installers can mount two Cisco 1000 series lightweight access points back-to-back, and the Network operator can disable the second antenna in both access points to create a 360-degree coverage area with two sectors.

Installers can also mount Cisco 1000 series lightweight access points on the periphery of a building and disable the Side B internal antennas. This configuration can be used to supply service to the building interior without extending coverage to the parking lot, at the cost of eliminating the internal antenna diversity function.

Refer to Appendix E: Internal Antenna Patterns for information on the radiation patterns of internal antennas in 1000 series lightweight access points.

Cisco 1000 Series Lightweight Access Point LEDs

Each Cisco 1000 series lightweight access point is equipped with four LEDs across the top of the case. They can be viewed from nearly any angle. The LEDs indicate power and fault status, 2.4 GHz (802.11b/g) Cisco Radio activity, and 5 GHz (802.11a) Cisco Radio activity.

This LED display allows the wireless LAN manager to quickly monitor the Cisco 1000 series lightweight access point status. For more detailed troubleshooting instructions, refer to the Error Messages and Access Point LEDs appendix.

Cisco 1000 Series Lightweight Access Point Connectors

The AP1020 and AP1030 Cisco 1000 series lightweight access points have the following external connectors:

- One RJ-45 Ethernet jack, used for connecting the Cisco 1000 series lightweight access point to the network.
- One 48 VDC power input jack, used to plug in an optional factory-supplied external power adapter.
- Three male reverse-polarity TNC antenna jacks, used to plug optional external antennas into the Cisco 1000 series lightweight access point: two for an 802.11b/g radio, and one for an 802.11a radio.



Note The AP1010 Cisco 1000 Series lightweight access points are designed to be used exclusively with the internal high-gain antennas, and have no jacks for external antennas.

The Cisco 1000 series lightweight access point communicates with a Cisco Wireless LAN Controller using standard CAT-5 (Category 5) or higher 10/100 Mbps twisted pair cable with RJ-45 connectors. Plug the CAT-5 cable into the RJ-45 jack on the side of the Cisco 1000 series lightweight access point.

Note that the Cisco 1000 series lightweight access point can receive power over the CAT-5 cable from network equipment. Refer to Power over Ethernet for more information about this option.

The Cisco 1000 series lightweight access point can be powered from an optional factory-supplied external AC-to-48 VDC power adapter. If you are powering the Cisco 1000 series lightweight access point using an external adapter, plug the adapter into the 48 VDC power jack on the side of the Cisco 1000 series lightweight access point.

The Cisco 1000 series lightweight access point includes two 802.11a and two 802.11b/g high-gain internal antennas, which provide omnidirectional coverage. However, some Cisco 1000 series lightweight access points can also use optional factory-supplied external high-gain and/or directional antennas. When you are using external antennas, plug them into the male reverse-polarity TNC jacks on the side of the AP1020 and AP1030 Cisco 1000 series lightweight access points.



Note Cisco 1000 Series lightweight access points must use the factory-supplied internal or external antennas to avoid violating FCC requirements and voiding the user's authority to operate the equipment.

Cisco 1000 Series Lightweight Access Point Power Requirements

Each Cisco 1000 series lightweight access point requires a 48 VDC nominal (between 38 and 57 VDC) power source capable of providing 7 Watts. The polarity of the DC source does not matter because the Cisco 1000 series lightweight access point can use either a +48 VDC or a -48 VDC nominal source.

Cisco 1000 series lightweight access points can receive power from the external power supply (which draws power from a 110-220 VAC electrical outlet) plugged into the side of the access point case, or from Power over Ethernet.

Cisco 1000 Series Lightweight Access Point External Power Supply

The Cisco 1000 series lightweight access point can receive power from an external 110-220 VAC-to-48 VDC power supply or from Power over Ethernet equipment.

The external power supply (AIR-PWR-1000) plugs into a secure 110 through 220 VAC electrical outlet. The converter produces the required 48 VDC output for the Cisco 1000 series lightweight access point. The converter output feeds into the side of the Cisco 1000 series lightweight access point through a 48 VDC jack.

Note that the AIR-PWR-1000 external power supply can be ordered with country-specific electrical outlet power cords. Contact Cisco when ordering to receive the correct power cord.

Cisco 1000 Series Lightweight Access Point Mounting Options

Refer to the *Internal-Antenna AP1010 Cisco 1000 Series IEEE 802.11a/b/g Lightweight Access Point Quick Start Guide* or the *External-Antenna AP1020 and AP1030 Cisco 1000 Series IEEE 802.11a/b/g Lightweight Access Point Quick Start Guide* for the Cisco 1000 series lightweight access point mounting options.

Cisco 1000 Series Lightweight Access Point Physical Security

The side of the Cisco 1000 series lightweight access point housing includes a slot for a Kensington MicroSaver Security Cable. Refer to the Kensington website for more information about their security products, or to the *Internal-Antenna AP1010 Cisco 1000 Series IEEE 802.11a/b/g Lightweight Access Point Quick Start Guide* or *External-Antenna AP1020 and AP1030 Cisco 1000 Series IEEE 802.11a/b/g Lightweight Access Point Quick Start Guide* for installation instructions.

Cisco 1000 Series Lightweight Access Point Monitor Mode

The Cisco 1000 series lightweight access points and Cisco Wireless LAN Controllers can perform rogue access point detection and containment while providing regular service. The rogue access point detection is performed across all 801.11 channels, regardless of the Country Code selected.

However, if the administrator would prefer to dedicate specific Cisco 1000 series lightweight access points to rogue access point detection and containment, the Monitor mode should be enabled for individual Cisco 1000 series lightweight access points.

The Monitor function is set for all 802.11 Cisco Radios on a per-access point basis using any of the Cisco Wireless LAN Controller user interfaces.

Using the DNS for Controller Discovery

In Cisco Wireless LAN Solution software releases 3.0 and later, access points can discover controllers through your domain name server (DNS). To use this feature you configure your DNS to return controller IP addresses in response to `CISCO-LWAPP-CONTROLLER.localdomain`. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve `CISCO-LWAPP-CONTROLLER.localdomain`. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Dynamic Frequency Selection

The Cisco Wireless LAN solution complies with regulations in Europe and Singapore that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them.

When a lightweight access point with a 5-GHz radio operates on one of the 15 channels listed in [Table 7-1](#), the controller to which the access point is associated automatically uses DFS to set the operating frequency.

When you manually select a channel for DFS-enabled 5-GHz radios, the controller checks for radar activity on the channel for 60 seconds. If there is no radar activity, the access point operates on the channel you selected. If there is radar activity on the channel you selected the controller automatically selects a different channel, and after 30 minutes, the access point re-tries the channel you selected.


Note

The Rogue Location Detection Protocol (RLDP) is not supported on the channels listed in [Table 7-1](#).


Note

The maximum legal transmit power is greater for some 5-GHz channels than for others. When it randomly selects a 5-GHz channel on which power is restricted, the controller automatically reduces transmit power to comply with power limits for that channel.

Table 7-1 5-GHz Channels on Which DFS is Automatically Enabled

| | | |
|----------------|----------------|----------------|
| 52 (5260 MHz) | 104 (5520 MHz) | 124 (5620 MHz) |
| 56 (5280 MHz) | 108 (5540 MHz) | 128 (5640 MHz) |
| 60 (5300 MHz) | 112 (5560 MHz) | 132 (5660 MHz) |
| 64 (5320 MHz) | 116 (5580 MHz) | 136 (5680 MHz) |
| 100 (5500 MHz) | 120 (5600 MHz) | 140 (5700 MHz) |

Using DFS, the controller monitors operating frequencies for radar signals. If it detects radar signals on a channel, the controller takes these steps:

- It changes the access point channel to a channel that has not shown radar activity. The controller selects the channel at random.
- If the channel selected is one of the channels in [Table 7-1](#), it scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the controller accepts client associations.
- It records the channel that showed radar activity as a radar channel and prevents activity on that channel for 30 minutes.
- It generates a trap to alert the network manager.

Autonomous Access Points Converted to Lightweight Mode

You can use an upgrade conversion tool to convert autonomous Cisco Aironet 1130AG, 1200, and 1240AG Series Access Points to lightweight mode. When you upgrade one of these access points to lightweight mode, the access point communicates with a wireless LAN controller and receives a configuration and software image from the controller.

Refer to these documents for complete instructions on upgrading an autonomous access point to lightweight mode:

- *Release Notes for Cisco Aironet 1130AG, 1200, and 1240AG Series Access Points for Cisco IOS Release 12.3(7)JX*
- *Application Note: Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*

Guidelines for Using Access Points Converted to Lightweight Mode

Keep these guidelines in mind when you use autonomous access points that have been converted to lightweight mode:

- Converted access points support 2006, 4400, and WiSM controllers only. When you convert an autonomous access point to lightweight mode, the access point can communicate with Cisco 2006 series wireless LAN controllers, 4400 series controllers, or the controllers on a Wireless Services Module (WiSM) only. Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series controllers are not supported because lack the memory required to support access points running Cisco IOS software.
- Access points converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- Access points converted to LWAPP mode support 8 BSSIDs per radio and a total of 8 wireless LANs per access point. (Cisco 1000 series access points support 16 BSSIDs per radio and 16 wireless LANs per access point.) When a converted access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- Access points converted to lightweight mode do not support Layer 2 LWAPP. Access Points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.

Reverting from Lightweight Mode to Autonomous Mode

After you use the upgrade tool to convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS release 12.3(7)JA or earlier). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Using a Controller to Return to a Previous Release

Follow these steps to revert from lightweight mode to autonomous mode using a wireless LAN controller:

-
- Step 1** Log into the CLI on the controller to which the access point is associated.
 - Step 2** Enter this command:
config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*
 - Step 3** Wait until the access point reboots and reconfigure the access point using the CLI or GUI.
-

Using the MODE Button and a TFTP Server to Return to a Previous Release

Follow these steps to revert from lightweight mode to autonomous mode by using the access point MODE (reset) button to load a Cisco IOS release from a TFTP server:

-
- Step 1** The PC on which your TFTP server software runs must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.
 - Step 2** Make sure that the PC contains the access point image file (such as *c1200-k9w7-tar.123-7.JA.tar* for a 1200 series access point) in the TFTP server folder and that the TFTP server is activated.
 - Step 3** Rename the access point image file in the TFTP server folder to **c1200-k9w7-tar.default** for a 1200 series access point.
 - Step 4** Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.
 - Step 5** Disconnect power from the access point.
 - Step 6** Press and hold the **MODE** button while you reconnect power to the access point.



Note The MODE button on the access point must be enabled. Follow the steps in the [“Disabling the Reset Button on Access Points Converted to Lightweight Mode”](#) section on page 7-13 to check the status of the access point MODE button.

- Step 7** Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.
 - Step 8** Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.
 - Step 9** After the access point reboots, reconfigure the access point using the GUI or the CLI.
-

Controllers Accept SSCs from Access Points Converted to Lightweight Mode

The lightweight access point protocol (LWAPP) secures the control communication between the access point and controller by means of a secure key distribution requiring X.509 certificates on both the access point and controller. LWAPP relies on a priori provisioning of the X.509 certificates. Factory installed certificates are referenced by the term *MIC*, which is an acronym for manufacturing-installed certificate. Cisco Aironet access points shipped before July 18, 2005 do not have a MIC, so these access points create a self-signed certificate (SSC) when upgraded to operate in lightweight mode. Controllers are programmed to accept SSCs for authentication of specific access points.

Using DHCP Option 43

Cisco 1000 series access points use a string format for DHCP option 43, whereas Cisco Aironet access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). [Table 7-2](#) lists the VCI strings for Cisco access points capable of operating in lightweight mode.

Table 7-2 VCI Strings For Lightweight Access Points

| Access Point | VCI String |
|---------------------------|----------------|
| Cisco 1000 Series | Airespace 1200 |
| Cisco Aironet 1130 Series | Cisco AP c1130 |
| Cisco Aironet 1200 Series | Cisco AP c1200 |
| Cisco Aironet 1240 Series | Cisco AP c1240 |

This is the format of the TLV block:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of the IP addresses of controller management interfaces

Refer to the product documentation for your DHCP server for instructions on configuring DHCP Option 43. The *Application Note: Upgrading Autonomous Cisco Aironet Access Points To Lightweight Mode* contains example steps for configuring option 43 on a DHCP server.

Using a Controller to Send Debug Commands to Access Points Converted to Lightweight Mode

Enter this command to enable the controller to send debug commands to an access point converted to lightweight mode:

```
config ap remote-debug [enable | disable | exc_command] access-point-name
```

When this feature is enabled, the controller sends debug commands to the converted access point as character strings. You can send any debug command supported by Cisco Aironet access points that run Cisco IOS software in lightweight mode.

Converted Access Points Send Crash Information to Controller

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of crash. After the unit reboots, it sends the reason for the reboot to the controller. If the unit rebooted because of a crash, the controller pulls up the crash file using existing LWAPP messages and stores it in the controller flash memory. The crash info copy is removed from the access point flash memory when the controller pulls it from the access point.

Converted Access Points Send Radio Core Dumps to Controller

When a radio module in a converted access point generates a core dump, the access point stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the controller indicating which radio generated a core dump file. The controller sends a trap alerting the network administrator, and the administrator can retrieve the radio core file from the access point.

On the controller CLI, enter this command to pull the core file from the access point:

```
config ap get-radio-core-dump slot ap-name
```

For *slot*, enter the radio interface number on the access point.

The retrieved core file is stored in the controller flash and can subsequently be uploaded through TFTP to an external server for analysis. The core file is removed from the access point flash memory when the controller pulls it from the access point.

Enabling Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the controller. To enable this feature, enter this command:

```
config ap core-dump enable tftp-server-ip-address filename {compress | uncompress} {ap-name | all}
```

- For *tftp-server-ip-address*, enter the IP address of the TFTP server to which the access point sends core files. The access point must be able to reach the TFTP server.
- For *filename*, enter a filename that the access points uses to label the core file.
- Enter **compress** to configure the access point to send compressed core files. Enter **uncompress** to configure the access point to send uncompressed core files.
- For *ap-name*, enter the name of a specific access point, or enter **all** to enable memory core dumps from all access points converted to lightweight mode.

Display of MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the controller lists converted access points by radio MAC address.

Disabling the Reset Button on Access Points Converted to Lightweight Mode

You can disable the reset button on access points converted to lightweight mode. The reset button is labeled MODE on the outside of the access point.

Use this command to disable or enable the reset button on one or all converted access points associated to a controller:

```
config ap reset-button {enable | disable} {ap-name | all}
```

The reset button on converted access points is enabled by default.

Configuring a Static IP Address on an Access Point Converted to Lightweight Mode

After an access point converted to lightweight mode associates to a controller, enter this command to configure a static IP address on the access point:

```
config ap static-ip enable ap-name ip-address mask gateway
```

