CHAPTER 7

Troubleshooting Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the 1200 series lightweight access point (models: AIR-LAP1231G and AIR-LAP1232AG). For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Sections in this chapter include:

Guidelines for Using 1200 Series Lightweight Access Points

Keep these guidelines in mind when you use a 1200 series lightweight access point:

- The access points can only communicate with 2006 series or 4400 series controllers.

Note Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series controllers are not supported because they lack the memory required to support access points running Cisco IOS software.

- The access points do not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support eight Basic Service Set Identifiers (BSSIDs) per radio and a total of eight wireless LANs per access point. When a lightweight access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- The access points do not support Layer 2 LWAPP. They must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes (all configuration commands are disabled when associated with a controller).

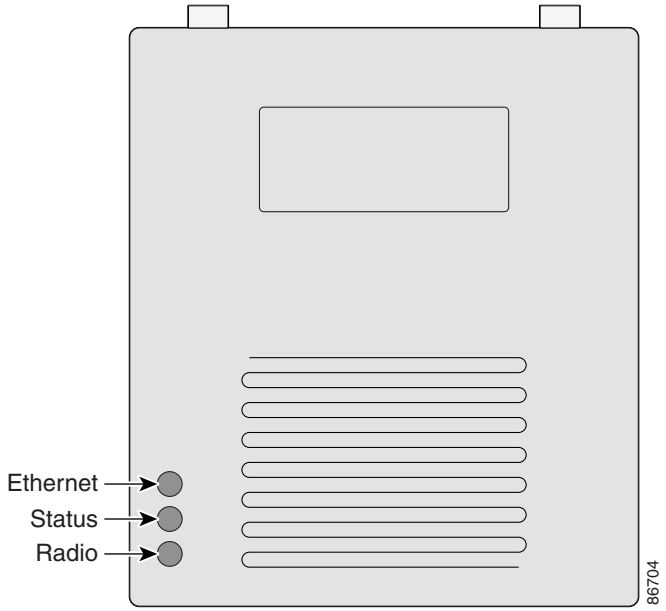
Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. For additional information, refer to the Appendix G, "Configuring DHCP Option 43 for Lightweight Access Points."

Checking the Top Panel LEDs

If your access point is not communicating, check the three LEDs on the top panel. You can use them to quickly assess the unit's status. Figure 7-1 shows the LEDs.

Figure 7-1 Access Point LEDs



The LEDs signals have the following meanings (for additional details refer to Table 7-1):

- The Ethernet LED signals traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

Table 7-1 Top Panel LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	-	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failure	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
Firmware Upgrade	–	Red	–	Loading new firmware image.
Controller status	Alternating green, red , and amber[1]			Connecting to the wireless LAN controller. **Note** If the access point remains in this mode for more than five minutes, the access point is unable to find the controller. Ensure a DHCP server is available or that controller information is configured on the access point.

1. This status indication has the highest priority and overrides other status indications.

Manually Configuring Controller Information Using the Access Point CLI

In a new installation, when your access point is unable to reach a DHCP server, you can manually configure needed controller information using the access point CLI. For information on how to connect to the console port, see the "Connecting to the Access Point Locally" section on page 7-9.

Note The CLI commands in this section can be used only on an access point that is not associated to a controller.

The static information configured with the CLI commands are used by the access point to connect with a controller. After connecting with the controller, the controller reconfigures the access point with new controller settings, but the static IP addresses for the access point and the default gateway are not changed.

Configuring Controller Information

To manually configure controller information on a new (out-of -the-box) access point using the access point CLI interface, you can use these EXEC mode CLI commands:

```
AP# lwapp ap ip address <IP address> <subnet mask>
AP# lwapp ip default-gateway IP-address
AP# lwapp controller ip address IP-address
AP# lwapp ap hostname name
    Where name is the access point name on the controller.
```

Note The default (out-of-box) Enable password is *Cisco*.

Clearing Manually Entered Controller Information

When you move your access point to a different location in your network, you must clear the manually entered controller information to allow your access point to associate with a different controller.

Note This command requires the controller configured Enable password to enter the CLI EXEC mode.

To clear or remove the manually entered controller information, you can use these EXEC mode CLI commands:

```
clear lwapp ap ip address
clear lwapp ip default-gateway
clear lwapp controller ip address
clear lwapp ap hostname
```

Manually Resetting the Access Point to Defaults

You can manually reset your access point to default settings using this EXEC mode CLI command:

Note This command requires the controller configured Enable password to enter the CLI EXEC mode.

```
clear lwapp private-config
```

Returning the Access Point to Autonomous Mode

You can return a lightweight access point to autonomous mode by loading a Cisco IOS release that supports autonomous mode (such as Cisco IOS Release 12.3(8)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.

Using a Controller to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using a controller:

Step 1 Log into the CLI on the controller to which the access point is associated and enter this command:

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*
(where:
a) *tftp-server-ip-address* is the IP address of the TFTP server
b) *filename* is the full path and filename of the access point image file, such as D:/Images/*c1200-k9w7-tar.123-8.JA.tar*
c) *access-point-name* is the name that identifies the access point on the gondolier.)

Step 2 Wait until the access point completes the reboot, as indicated by the Status LED turning green to indicate a client is associated or blinking green to indicate a client is not associated.

Step 3 After the access point reboots, reconfigure it using the access point GUI or the CLI.

Using the MODE Button to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using the access point MODE button and a TFTP server:

Note The access point MODE button is enabled by default, but you need to verify that the MODE button is enabled (see the "MODE Button Setting" section on page 7-7).

Step 1 Set the static IP address of the PC on which your TFTP server software runs to an address between 10.0.0.2 and 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1200-k9w7-tar.123-8.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.**

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.

Step 7 Hold the **MODE** button until the Radio LED turns red (approximately 20 to 30 seconds) and then release.

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 it using the access point GUI or the CLI.

MODE Button Setting

The access point MODE button is configured from your controller. Use these controller CLI commands to view and configure the MODE button:

```
1) config ap rst-button enable <access-point-name>/all
2) config ap rst-button disable <access-point-name>/all
3) show ap config general <access-point-name>
   (Where access-point-name is the name that identifies the access point on the
   oontroller.)
```

Obtaining the Autonomous Access Point Image File

The autonomous access point image file can be obtained from the Cisco.com software center using these steps:

Note To download software from the Cisco.com software center, you must be a registered user. You can register from the main Cisco.com web page at this URL: http://cisco.com.

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless

Step 2 Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1200 Series > Cisco Aironet 1200 Access Point**. The Enter Password window appears.

Step 3 Enter your username and password in the respective fields and click **OK**. The **Select a Software Type** page appears.

Step 4 Click **IOS** and the Select a Release page appears.

Step 5 Click on the IOS release for the desired access point image file, such as *12.3(8)JA*.

Step 6 Click **Wireless LAN** and the Enter Password window appears.

Step 7 Enter your username and password in the respective fields and click **OK**.

Step 8 If you receive a *Do you want to display the nonsecure items?* message, click **Yes**.

Step 9 On the Encryption Software Export Distribution Authorization Form, read the information and click the appropriate box.

Step 10 Click **Submit**.

Step 11 If you indicated that the software is not for you or your company, follow these steps:

a. If you receive a *Do you want to display the nonsecure items?* message, click **Yes**. The Encryption Software Export Distribution Authorization window appears.

b. Carefully read the information and enter the Cisco.com user profile or detailed data describing the end user of this software image in the provided fields.

c. Click **Submit**.

Step 12 If you receive a *Do you wish to continue?* security alert message, click **Yes** to continue.

Step 13 Click **Download**.

Step 14 Carefully read the Software Download Rules and click **Agree** to download the image file. An Enter Password window appears.

Step 15 Enter your username and password in the respective fields and click **OK**.

Step 16 Download and save the image file to your hard drive and then exit the Internet browser.

Obtaining the TFTP Server Software

You can download TFTP server software from several web sites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

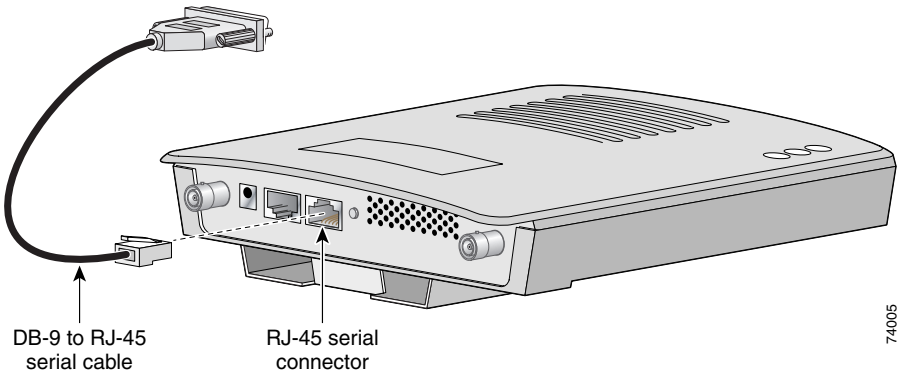
Follow the instructions on the website for installing and using the utility.

Connecting to the Access Point Locally

The console port is enabled during power up for diagnostic and monitoring purposes, which might be helpful if the access point is unable to associate to a controller. You can connect a PC to the console port using a DB-9 to RJ-45 serial cable.

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer. Figure 7-2 shows the serial port connection.

Figure 7-2 Connecting the Serial Cable



Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to http://www.cisco.com/go/marketplace to order a serial cable.

Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Note When your monitoring and diagnostic activities are completed, you must remove the serial cable from the access point.

Step 3 At the prompts, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.