Troubleshooting 1240AG Series Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the 1240AG series lightweight access point (AIR-LAP1242AG or AIR-LAP1242G). 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/cisco/web/psa/default.html

Sections in this chapter include:

Guidelines for Using Cisco Aironet Lightweight Access Points

Keep these guidelines in mind when you use a 1240 series lightweight access point:

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

> **Note** Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series wireless LAN 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 an 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 connected to 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 "Configuring DHCP Option 43 for Lightweight Access Points" section on page G-1.

Checking the Lightweight Access Point LEDs

If your lightweight access point is not working properly, check the Status, Ethernet, and Radio LEDs on the 2.4 GHz end of the unit. You can use the LED indications to quickly assess the unit's status. Figure 4-1 shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

Figure 4-1   Access Point LEDs
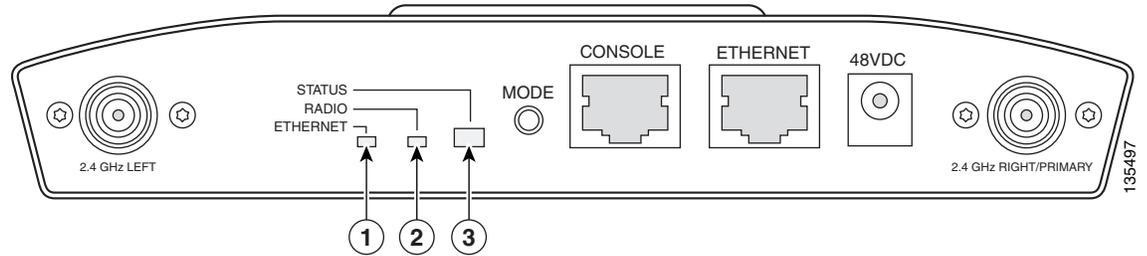
1	Ethernet LED	**3**	Status LED
2	Radio LED		

The LED signals are listed in Table 4-1.

Table 4-1   LED Signals

Message type	Ethernet LED	Radio LED	Status LED	Meaning
Boot loader status	Green	Green	Green	DRAM memory test ok.
	Off	Blinking green	Blue-green	Initialize Flash file system.
	Off	Green	Pink	Flash memory test ok.
	Green	Off	Dark blue	Ethernet test ok.
	Green	Green	Green	Starting Cisco IOS.
Association status	—	—	Light green	Normal operating condition, but no wireless client devices are associated with the unit.
	—	—	Blue	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	—	—	Ethernet link is operational.
	Blinking green	—	—	Transmitting or receiving Ethernet packets.
	—	Blinking green	—	Transmitting or receiving radio packets.
	—	—	Blinking dark blue	Software upgrade in progress
	Slow blinking green	—	—	Hybrid-REAP standalone mode

Table 4-1   LED Signals (continued)

Message type	Ethernet LED	Radio LED	Status LED	Meaning
Boot loader warnings	Off	Off	Yellow	Ethernet link not operational.
	Red	Off	Yellow	Ethernet failure.
	Amber	Off	Yellow	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Pink	Image recovery (Mode button pressed for 20 to 30 seconds)
	Blinking green	Blinking red	Blinking pink	Image recovery in progress and Mode button is released.
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Red	Blinking red and blue	Flash file system failure.
	Off	Amber	Blinking red and blue-green	Environment variable (ENVAR) failure.
	Amber	Off	Blinking red and yellow	Bad MAC address.
	Red	Off	Blinking red and off	Ethernet failure during image recovery.
	Amber	Amber	Blinking red and off	Boot environment error.
	Red	Amber	Blinking red and off	No Cisco IOS image file.
	Amber	Amber	Blinking red and off	Boot failure.
Cisco IOS errors	Blinking amber	—	—	Transmit or receive Ethernet errors.
	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio.
	Red	Red	Amber	Software failure; try disconnecting and reconnecting unit power.
	—	—	Amber	General warning, insufficient inline power (see the Low Power Condition for Lightweight Access Points section).
Controller status	Alternating green, red , and amber[1]			Connecting to the 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.
	Green	Green	Blinking dark blue	Loading the access point image file.

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

Low Power Condition for Lightweight Access Points

Warning   **This product must be connected to a Power over Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.** Statement 353

The access point can be powered from the 48-VDC power module or from an in-line power source. The access point supports the IEEE 802.3af power standard, Cisco Pre-Standard PoE protocol, and Cisco Intelligent Power Management for in-line power sources.

For full operation, the access point (powered device) requires 12.95 W (up to 15.4 W with 100 m CAT 5 Ethernet cable). When the access point is being used in a PoE configuration, the power drawn from the power sourcing equipment (PSE), such as a switch or power injector, is higher by an amount dependent on the length of the interconnecting cable.

The power module and Cisco Aironet power injectors are capable of supplying the required power for full operation, but some inline power sources are not capable of supplying sufficient power. Also, some high-power inline power sources, might not be able to provide up to 15.4 W of power to all ports at the same time.

Note   An 802.3af compliant switch (Cisco or non-Cisco) is capable of supplying sufficient power for full operation.

Note   If your access point is connected to in-line power, do not connect the power module to the access point. Using two power sources on the access point might cause the access point to shut down to protect internal components and might cause the switch to shut down the port to which the access point is connected. If your access point shuts down, you must remove all power and reconnect only a single power source.

On power up, the access point is placed into low power mode (both radios are disabled), Cisco IOS software loads and runs, and power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on; otherwise, the access point remains in low power mode with the radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication (see the "Checking the Lightweight Access Point LEDs" section on page 4-3).

Intelligent Power Management

The access point requires 12.95 W of power (up to 15.4 W with 100 m CAT 5 Ethernet cable) for full power operation with both radios, but only needs 6.3 W of power when operating in low power mode with both radios disabled. To help avoid an over-current condition with low power sources and to optimize power usage on Cisco switches, Cisco developed Intelligent Power Management, which uses Cisco Discovery Protocol (CDP) to allow powered devices (such as your access point) to negotiate with a Cisco switch for sufficient power.

The access point supports Intelligent Power Management and as a result of the power negotiations, the access point will either enter full power mode or remain in low power mode with the radios disabled.

> **Note** Independent of the power negotiations, the access point hardware also uses the 802.3af classification scheme to indicate the power required from the power source. However, the power source cannot report the power available to the access point unless the power source also supports Intelligent Power Management.

Some Cisco switches that are capable of supplying sufficient power require a software upgrade to support Intelligent Power Management. If the software upgrade is not desired, you can configure the access point to operate in pre-standard compatibility mode and the access point automatically enters full power mode if these Cisco switches are detected in the received CDP ID field.

When the access point determines that sufficient power is not available for full-power operation, the readios are deactivated and the Status LED turns amber to indicate low power mode (see Table 4-1).

If your Cisco switch is capable of supplying sufficient power for full operation but the access point remains in low-power mode, your access point or your switch (or both) might be misconfigured (see Table 4-2.

If your inline power source is not able to supply sufficient power for full operation, you should consider these options (see Table 4-2):

- Upgrade to a higher-powered switch
- Use a Cisco Aironet power injector on the switch port
- Use the 48-VDC power module to locally power the access point

Configuring Power Using Controller CLI Commands

Intelligent Power Management support is dependent on the version of software resident in the Cisco switch that is providing power to the access point. Each Cisco switch should be upgraded to support Intelligent Power Management. Until the software is upgraded, you can use your controller to configure the access point to operate with older switch software using these controller CLI commands:

```
1) config ap power pre-standard enable <ap>
     where <ap> is the access point name on the controller

2) config ap power injector enable <ap> <switch port MAC address>
     (where <ap> is the access point name on the controller
         and <switch port MAC address> is the MAC address of the switch port to which the
         access point is connected)
```

> **Note** Refer to your controller documentation for instructions on using these commands.

You can use these controller CLI commands to inform the access point of the following:

- The Cisco switch does not support Intelligent Power Management but should be able to supply sufficient power.

- A power injector is being used to supply sufficient power and the Cisco switch does not support Intelligent Power Management.

Refer to Table 4-2 for information on when to use these special CLI controller commands and the corresponding Cisco switch power command.

⚠

Caution   If the access point receives power through PoE, the output current of the power sourcing equipment (PSE) cannot exceed 400 mA per port. The power source must comply with IEEE 802.3af or IEC60950 for limited power sources.

Table 4-2   Using CLI Power Commands

Power Source	CLI Commands	
	Cisco Wireless LAN Controller	**Cisco Switch**
AC power module	None required	**power inline never**
Cisco switch that supports Intelligent Power Management[1]	None required	**power inline auto**
Cisco switch that does not support Intelligent Power Management[1]	**config ap power pre-standard enable**	**power inline auto**
Power injector[2] used with a Cisco switch that supports Intelligent Power Management[1]	None required	**power inline never[3]**
Power injector[2] used with a Cisco switch that does not support Intelligent Power Management[1]	**config ap power injector enable**	**power inline never**
Power injector used with a non-Cisco switch	None required	–
802.3af compliant non-Cisco switches	None required	–

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.

2. Power injector must be AIR-PWRINJ3 or AIR-PWRINJ-FIB.

3. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.

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 4-11.

✎

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 Lightweight 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(7)JA or earlier). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release (refer to your controller documentation). 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/c1240-k9w7-tar.123-7.JA.tar
        c) access-point-name is the name that identifies the access point on the
        ocntroller.)
```

Step 2   Wait until the access point reboots, as indicated by all LEDs turning green followed by the Status LED blinking green.

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 4-10).

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 *c1240-k9w7-tar.123-7.JA.ta*r for a 1240 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 **c1240-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 lightweight access point MODE button is configured from your Cisco Wireless LAN 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 ocntroller.)

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://www.cisco.com.

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

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

Step 2   Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1240AG Series > Cisco Aironet 1240AG 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.

Connecting to the Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable.

⚠

Caution   Be careful when handling the access point, the bottom plate might be hot.

✎

Note   After completing your configuration changes, you must remove the serial cable from the access point.

Follow these steps to open the CLI by connecting to the access point console port:

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

Figure 4-2 shows the console port location.

Figure 4-2   Console Port Location
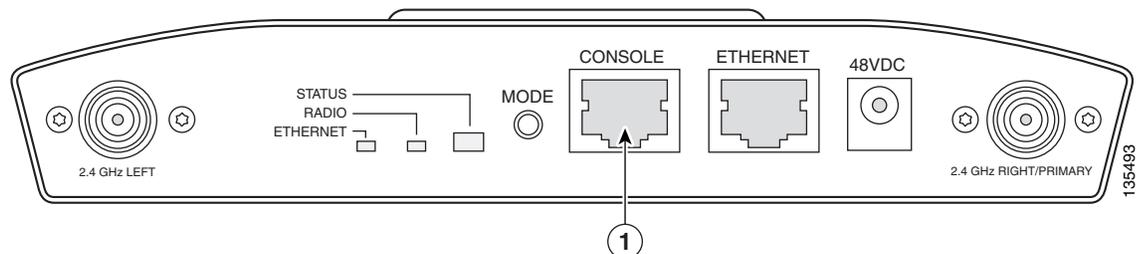
1	Console port	

✎

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 on your PC 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.

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.

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.