



Troubleshooting Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the lightweight access point (model: LAP1310G). 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

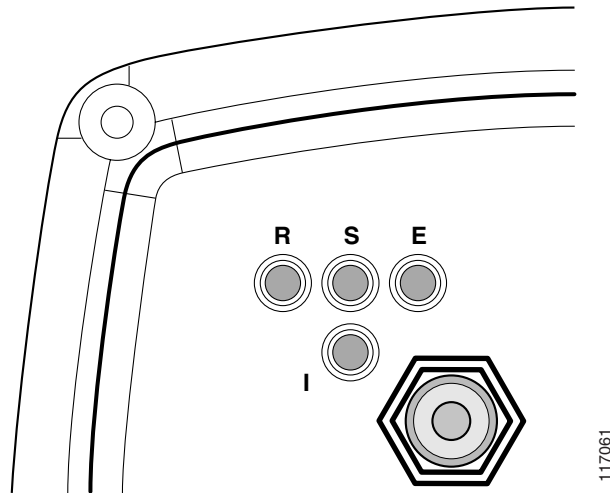
Sections in this chapter include:

- [Checking the LEDs on Lightweight Access Points, page 5-2](#)
- [Power Injector, page 5-4](#)
- [Checking Power, page 5-5](#)
- [Using DHCP Option 43, page 5-5](#)
- [Manually Configuring Controller Information Using the Access Point CLI, page 5-6](#)
- [Returning the Access Point to Autonomous Mode, page 5-8](#)
- [Obtaining the Autonomous Access Point Image File, page 5-9](#)

Checking the LEDs on Lightweight Access Points

If your lightweight access point is not operating properly, check the LEDs on the back panel. You can use them to quickly assess the unit's status. [Figure 5-1](#) shows the access point LEDs.

Figure 5-1 LEDs



R	Radio LED	E	Ethernet LED
S	Status LED	I	Install LED



Note

The Install LED is not used on the 1300 series lightweight access points.

LED Indications

During access point operation the LEDs provide status information as shown in [Table 5-1](#).

Table 5-1 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.

Table 5-1 LED Signals (continued)

Message type	Ethernet LED	Status LED	Radio LED	Meaning
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.
Message type	Ethernet LED	Status LED	Radio LED	Meaning

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

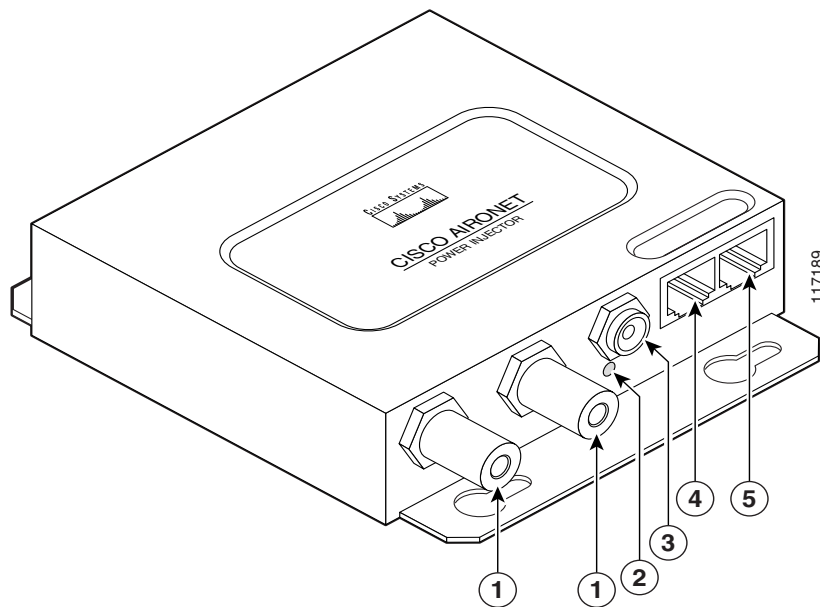
Power Injector

When the power injector is powered up, it applies 48-VDC to the dual-coax cables to the access point.

When power is applied to the access point, the unit activates the bootloader and begins the POST operations. The access point begins to load the Cisco IOS image when the POST operations are successfully completed. Upon successfully loading the image, the unit initializes and tests the radio.

The power injector LED is shown in [Figure 5-2](#).

Figure 5-2 Power Injector



1	Dual-coax Ethernet ports (F-Type connectors)	4	Ethernet LAN port (RJ-45 connector)
2	Power LED	5	Console serial port (RJ-45 connector)
3	Power jack		

The power injector is available in two models:

- Cisco Aironet Power Injector LR2—standard version (included with the access point)
 - 48-VDC input power
 - Uses the 48-VDC power module (included with the access point)
- Cisco Aironet Power Injector LR2T—optional transportation version
 - 12- to 40-VDC input power

Checking Power

You can verify the availability of power to the lightweight access point by checking the power injector LED (see [Figure 5-2](#)):

- Power LED
 - Green color indicates input power is being supplied to the access point.
 - Red color indicates an overcurrent or overvoltage error condition—disconnect input power from the power injector, check all coax cable connections for a possible short, wait approximately 1 minute, and reconnect input power to the power injector. If the LED turns red again, contact technical support for assistance.



Note The power injector requires approximately 50 seconds to recover from an overcurrent or overvoltage condition.

- Off indicates input power is not available—verify that the power module is connected to the power injector and that AC power is available or that 12- to 40-VDC input power is connected to the power injector.

Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the lightweight access points, enabling the access point to find and associate with a controller. For additional information, refer to the “[Configuring DHCP Option 43 for Lightweight Access Points](#)” section on page G-1.

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 lightweight access point CLI.



Note

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

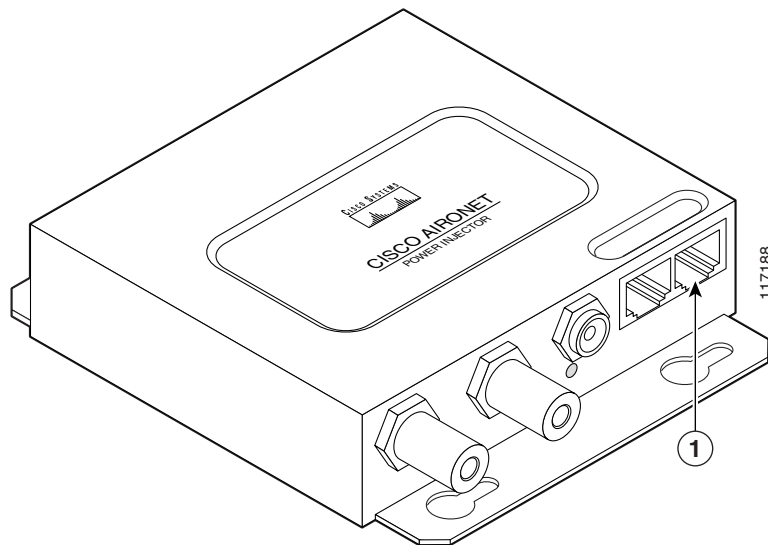
The static information configured with the CLI commands are used by the lightweight access point to connect with a controller. After connecting with the controller, the controller reconfigures the access point with new controller settings, but the static IP addresses for the access point and the default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

Connecting to the Console Serial Port

If you need to configure the access point locally (without connecting to a wired LAN), you can connect a PC to the power injector console serial port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the console serial port:

- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the power injector and to the COM port on your PC. [Figure 5-3](#) shows the power injector's console serial port connector.

Figure 5-3 Console Serial Port Connector



- | | |
|----------|---|
| 1 | Console serial port connector (RJ-45 connector) |
|----------|---|

**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.
- Step 3** When the terminal emulator is activated, press **Enter**.
- Step 4** Enter your username in the User Name field. The default username is *Cisco*.
- Step 5** Enter the access point/bridge password in the Password field and press **Enter**. The default password is *Cisco*.

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:

lwapp ap ip address *<IP address> <subnet mask>*

lwapp ip default-gateway *IP-address*

lwapp controller ip address *IP-address*

lwapp ap hostname *name*

Where *name* is the access point name that displays on the controller.

**Note**

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

Clearing Manually Entered Controller Information

When you need to 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:

```
clear lwapp private-config
```



Note

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

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). When the access point is associated to a controller, you can use the controller to load the Cisco IOS release.

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/c1310-k9w7-tar.123-8.JA.tar*
- c) *access-point-name* is the name that identifies the access point on the controller.)

Step 2 Wait until the access point completes the reboot.

Step 3 After the access point reboots, reconfigure it using the access point GUI or the CLI. For additional information refer to the *Cisco Aironet 1300 Series Outdoor Access Point Hardware Installation Guide* available at this URL:

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

To browse to the 1300 series access point documentation, click **Cisco Aironet 1300 Series** listed under “Wireless LAN Access.”

Obtaining the Autonomous Access Point Image File

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

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>



Note To download software from the Cisco.com software center, you must be a registered user. You can register from the web page.

Step 2 Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1300 Series** .

Step 3 Click **Cisco Aironet 1310 Access Point/Bridge**.

Step 4 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 5 Click **IOS**.

Step 6 Choose the Cisco IOS release desired, such as 12.3.11.JA.

Step 7 Click **WIRELESS LAN** for an access point image file, such as c1310-k9w7-tar.123-11.JA.tar.

Step 8 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 9 On the Security Information window, click **Yes** to display non-secure items.

Step 10 On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.

Step 11 If you checked No, enter the requested information and click **Submit**.

Step 12 Click **Yes** to continue.

Step 13 Click **DOWNLOAD**.

Step 14 Read and accept the terms and conditions of the Software Download Rules.

Step 15 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 16 Click **Save** to download your image file to your hard disk.

Step 17 Select the desired download location on your hard disk and click **Save**.

■ Obtaining the Autonomous Access Point Image File