CHAPTER 22

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the wireless device. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Top Issues** and then select **Wireless Technologies**):

http://www.cisco.com/tac

Sections in this chapter include:

Checking the Top Panel Indicators

Note The LED indicator setup is not the same across all Cisco Aironet series access points. Depending on the series, your access point may have a single Status LED indicator, or three indicators – Ethernet LED, Status LED, and Radio LED. The LED indicator setup information in the following sections is limited. Refer to your access point's *Getting Started Guide* or the *Hardware Installation Guide* (for Outdoor Access Points) for complete information on its LED indicator setup.

If your wireless device is not communicating, check the three LED indicators on the top panel to quickly assess the device's status. Figure 22-1 shows the indicators on the 1200 series access point. Figure 22-2 shows the indicators on the 1100 series access point. Figure 22-3 and Figure 22-4 show the indicators on the 350 series access point.

Note The 1130 series access point has a status LED on the top of the unit and two LEDs inside the protective cover. See the "Indicators on 1130 Series Access Points" section on page 22-6 for information on 1130 series access point indicators.

Figure 22-1 Indicators on the 1200 Series Access Point

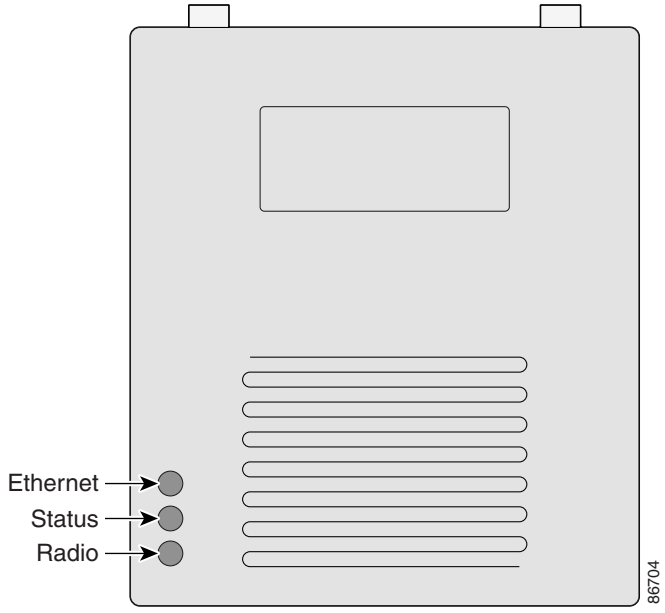


Figure 22-2 Indicators on the 1100 Series Access Point

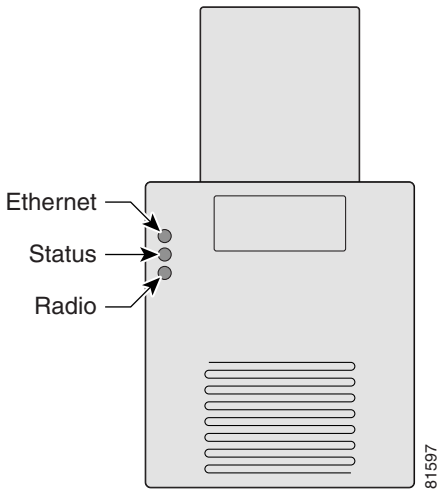


Figure 22-3 Indicators on the 350 Series Access Point (Plastic Case)

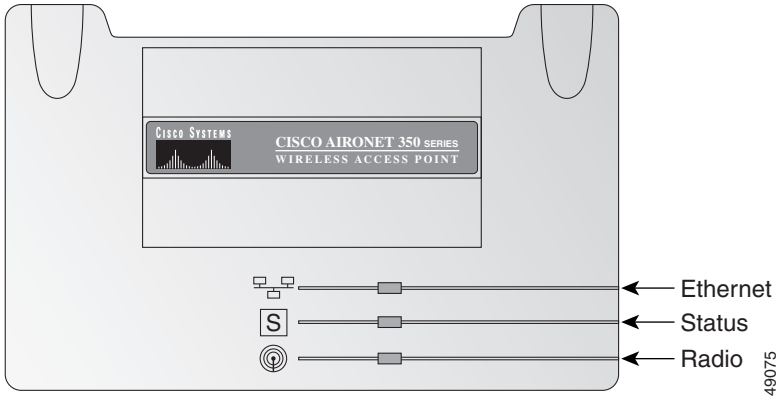
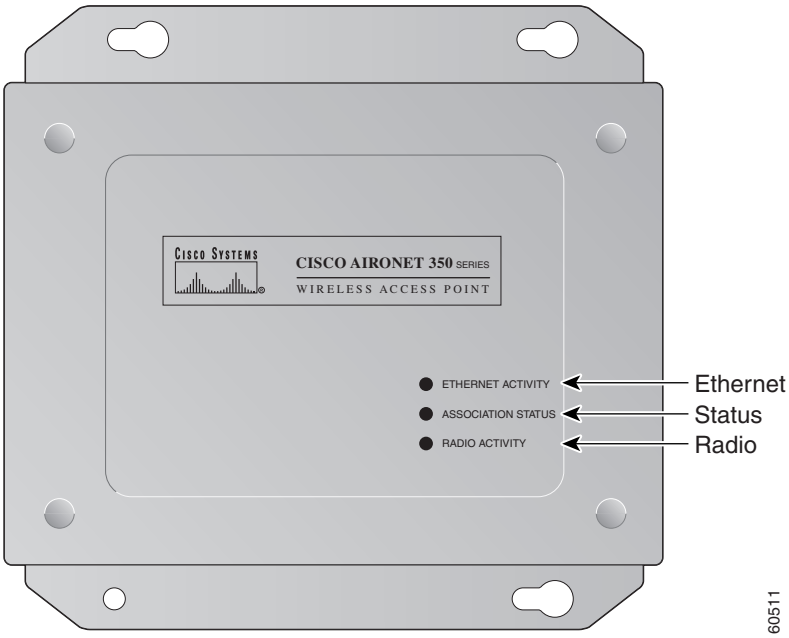


Figure 22-4 Indicators on the 350 Series Access Point (Metal Case)



The indicator signals on the wireless device have the following meanings (for additional details refer to Table 22-1):

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

Table 22-1 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	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 software.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the wireless device's SSID and WEP settings.

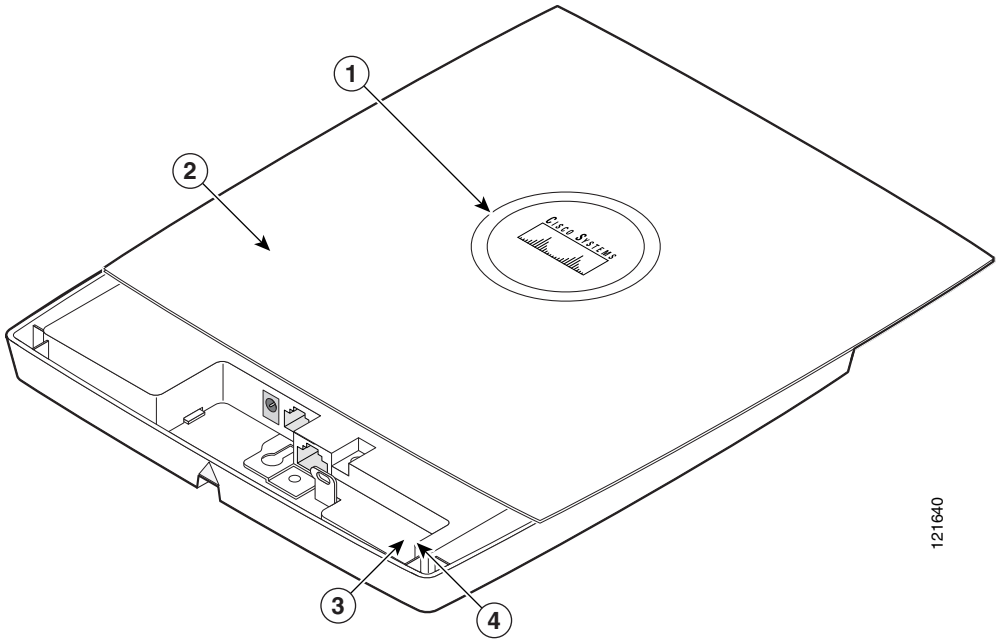
Table 22-1 Top Panel Indicator Signals (continued)

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
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.
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
	Blinking red	–	–	Hardware failure. The wireless device must be replaced.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Indicators on 1130 Series Access Points

If your access point is not working properly, check the LED ring on the top panel or the Ethernet and Radio LEDs in the cable bay area. You can use the LED indications to quickly assess the unit's status. Figure 22-1 shows the access point LEDs.

Figure 22-5 1130 Series Access Point LEDs



1	Status LED	**3**	Ethernet LED
2	Access point cover	**4**	Radio LED

Note To view the Ethernet and Radio LEDs you must open the access point cover.

The LED signals are listed in Table 22-2.

Table 22-2 LED Signals

	Cable Bay Area		Top of Unit	
Message type	**Ethernet LED**	**Radio LED**	**Status LED**	**Meaning**
Boot loader status	Green	Green	Green	DRAM memory test ok.
	Off	Blinking green	Light blue	Initialize Flash file system.
	Off	Green	Pink	Flash memory test ok.
	Green	Off	Blue	Ethernet test ok.
	Green	Green	Green	Starting Cisco IOS.
Association status	n/a	n/a	Light green	Normal operating condition, but no wireless client devices are associated with the unit.
	n/a	n/a	Light blue	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	n/a	n/a	Ethernet link is operational.
	Blinking green	n/a	n/a	Transmitting or receiving Ethernet packets.
	n/a	Blinking green	n/a	Transmitting or receiving radio packets.
	n/a	n/a	Blinking dark blue	Software upgrade in progress
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	Red	Blinking pink and off	Image recovery in progress and Mode button is released.

Table 22-2 LED Signals (continued)

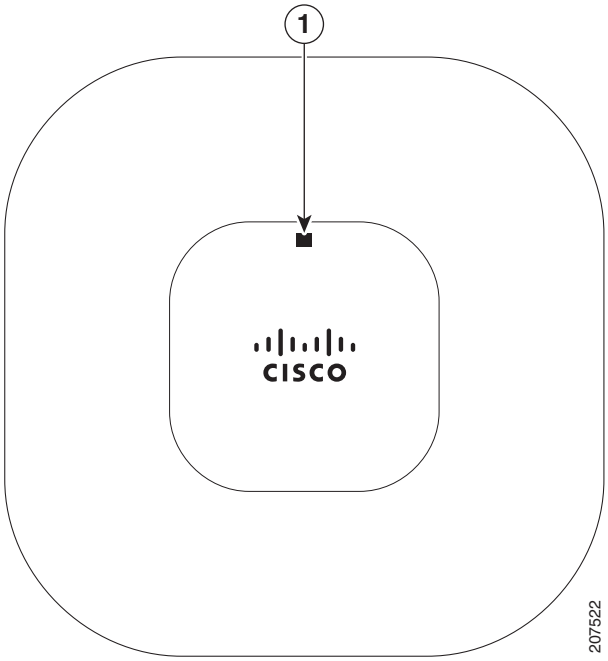
Message type	Cable Bay Area		Top of Unit	Meaning
	Ethernet LED	Radio LED	Status LED	
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Red	Blinking red and blue	Flash file system failure.
	Off	Amber	Blinking red and light blue	Environment variable (ENVAR) failure.
	Amber	Off	Blinking red 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	n/a	n/a	Transmit or receive Ethernet errors.
	n/a	Blinking amber	n/a	Maximum retries or buffer full occurred on the radio.
	Red	Red	Orange	Software failure; try disconnecting and reconnecting unit power.
	n/a	n/a	Orange	General warning, insufficient inline power.
	Blinking green	Blinking green	Blinking green	User activation of location indicator.

Indicators on 1140 Series Access Point

If your access point is not working properly, check the Ethernet and Status LEDs of the unit. You can use the LED indications to quickly assess the unit's status.Table 22-3 shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

Figure 22-6 shows the 1140 series access point LEDs.

Figure 22-6 1140 Series Access Point LEDs



1	Status LED		

Table 22-3 1140 Series Access Point LED Signals

Message Type	Status LED	Message Meaning
Boot loader status sequence	Blinking green	DRAM memory test in progress
		DRAM memory test OK
		Board initialization in progress
		Initializing FLASH file system
		FLASH memory test OK
		Initializing Ethernet
		Ethernet OK
		Starting Cisco IOS
		Initialization successful

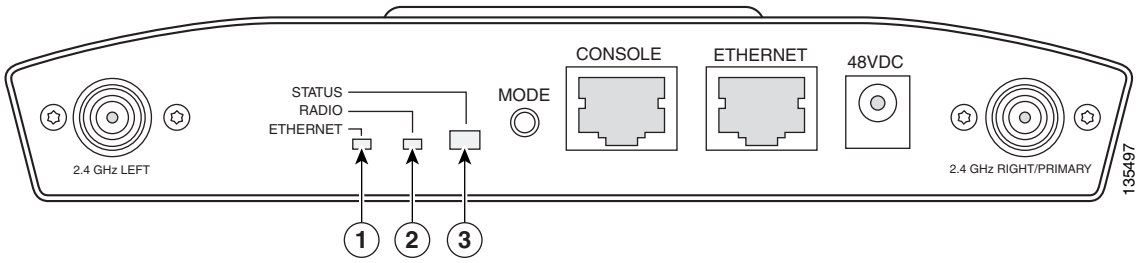
Table 22-3 1140 Series Access Point LED Signals (continued)

Message Type	Status LED	Message Meaning
Association status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association
Operating status	Blinking blue	Software upgrade in progress
	Cycling through green, red, and amber	Discovery/join process in progress
	Rapidly cycling through blue, green, and red	Access point location command invoked
	Blinking red	Ethernet link not operational
Boot loader warnings	Blinking blue	Configuration recovery in progress (MODE button pushed for 2 to 3 seconds)
	Red	Ethernet failure or image recovery (MODE button pushed for 20 to 30 seconds)
	Blinking green	Image recovery in progress (MODE button released)
Boot loader errors	Red	DRAM memory test failure
	Blinking red and blue	FLASH file system failure
	Blinking red and off	Environment variable failure
		Bad MAC address
		Ethernet failure during image recovery
		Boot environment failure
		No Cisco image file
		Boot failure
Cisco IOS errors	Red	Software failure; try disconnecting and reconnecting unit power
	Cycling through blue, green, red, and off	General warning; insufficient inline power

Indicators on 1240 Series Access Points

If your 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 22-1 shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

Figure 22-7 1240 Series Access Point LEDs



1	Ethernet LED	**3**	Radio LED
2	Radio LED		

The 1240 series access point LED signals are listed in Table 22-5.

Table 22-4 1240 Series Access Point 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

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	Red	Blinking pink and off	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 section).

Indicators on 1250 Access Points

If your access point is not working properly, check the Ethernet, Status, 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.Table 22-5 shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

Figure 22-8 shows the 1250 series access point LEDs.

Figure 22-8 1250 Series Access Point LEDs

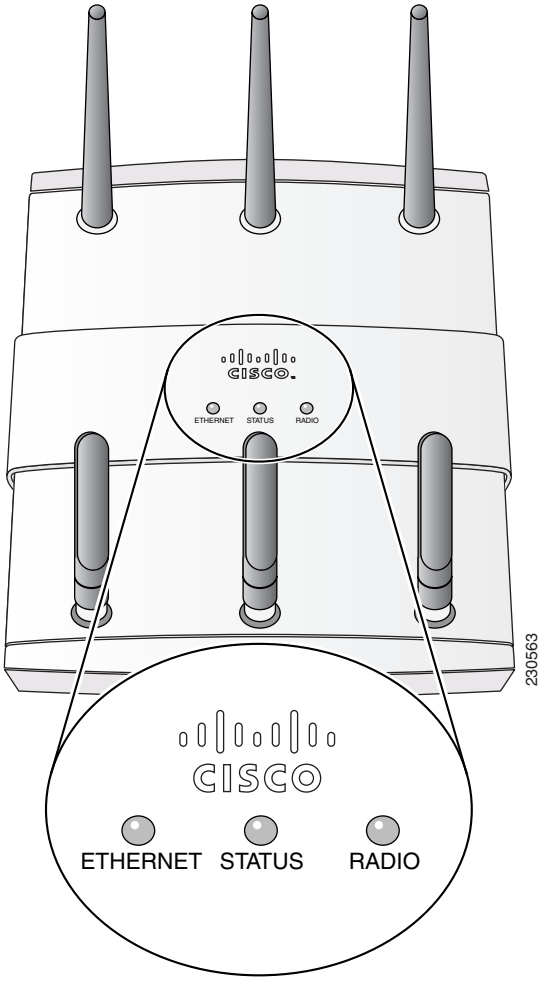


Table 22-5 1250 Series Access Point LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	Off	Amber	DRAM test in progress.
	Green	Green	Green	DRAM memory test ok.
	Off	Off	Red	Board initialization in progress.
	Off	Blinking green	Blinking green	Initialize Flash file system.
	Off	Green	Green	Flash memory test ok.
	Amber	White	Off	Initialize Ethernet.
	Green	Blinking blue	Off	Ethernet test ok.
	Green	Blinking green	Green	Starting Cisco IOS.
	Off	Off	Off	Initialization ok.
Association status	—	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 blue	—	Software upgrade in progress.
	Blinking green	Blinking green	Blinking green	Access point location command.
Boot loader warnings	Off	Blinking red	Off	Ethernet link not operational.
	Red	Red	Off	Ethernet failure.
	Amber	Blinking blue	Off	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Red	Image recovery (Mode button pressed for 20 to 30 seconds).
	Blinking green	Blinking green	Red	Image recovery in progress and Mode button is released.

Table 22-5 1250 Series Access Point LED Signals (continued) (continued)

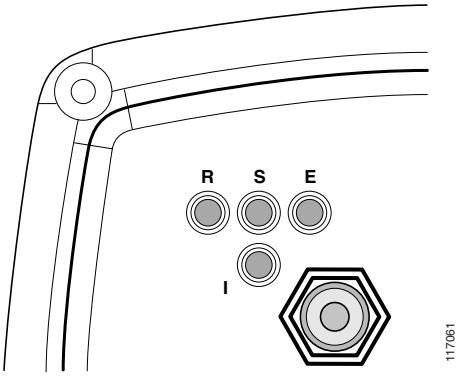
Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Blinking red and blue	Red	Flash file system failure.
	Off	Alternating red and green	Amber	Environment variable (ENVAR) failure.
	Amber	Rapid blinking red	Off	Bad MAC address.
	Red	Blinking red and off	Off	Ethernet failure during image recovery.
	Amber	Blinking red and off	Amber	Boot environment error.
	Red	Blinking red and off	Amber	No Cisco IOS image file.
	Amber	Blinking red and off	Amber	Boot failure.
Cisco IOS errors	Blinking amber	—	—	Transmit or receive Ethernet errors.
	—	—	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Red	Off	Red	Software failure; try disconnecting and reconnecting unit power.
	—	Cycle through blue, green, red, and off	—	General warning, insufficient inline power

Indicators on 1300 Outdoor Access Point/Bridges

If your access point/bridge is not associating with a remote bridge or access point, check the four LEDs on the back panel. You can use them to quickly assess the unit's status. For information on using the LEDs during the installation and alignment of the access point/bridge antenna, refer to the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Mounting Instructions* that shipped with your access point/bridge.

Figure 22-1 shows the access point/bridge LEDs.

Figure 22-9 LEDs



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

Normal Mode LED Indications

During access point/bridge operation the LEDs provide status information as shown in Table 22-6.

Table 22-6 1300 Series Access Point/Bridge LED Indications

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
Off	—	—	—	Ethernet link is down or disabled.
Blinking green	—	—	—	Transmitting and receiving Ethernet packets.
Blinking amber	—	—	—	Transmitting and receiving Ethernet errors.
amber	—	—	—	Firmware error—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.

Table 22-6 1300 Series Access Point/Bridge LED Indications (continued)

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
—	Blinking green	—	—	Root bridge mode—no remote bridges are associated. Non-root bridge mode—not associated to the root bridge. If all bridges are powered up, this could be caused by incorrect SSID and security settings or improper antenna alignment. You should check the SSID and security settings of all bridges and verify antenna alignment. If the problem continues, contact technical support for assistance.
—	Green	—	—	Root mode—associated to at least one remote bridge. Non-root mode—associated to the root bridge. This is normal operation.
—	Blinking amber	—	—	General warning—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	Amber	—	—	Loading firmware.
Red	Amber	Red	—	Loading Firmware error—disconnect and reconnect the power injector power. If the problem continues, contact technical support for assistance.
—	—	Off	—	Normal operation.
—	—	Blinking green	—	Transmitting and receiving radio packets—normal operation.
—	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio interface—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	—	Amber	—	Radio firmware error—disconnect and reconnect power injector power.If the problem continues, contact technical support for assistance.
—	—	—	Amber blinking	Not associated (non-root mode). The access point/bridge attempts to associate with a root bridge for 60 seconds[1].
—	—	—	Amber	Associated (non-root mode).
—	—	—	Green blinking	Not associated (root mode). The access point/bridge attempts to associate with a non-root bridge indefinitely.
—	—	—	Green	Associated (root mode).
—	—	—	Red	Overcurrent or overvoltage error—disconnect power to the power injector, check all coax cable connections, wait approximately 1 minute, and reconnect power. If error continues, contact technical support.

1. Preconfigured bridges search indefinitely.

The access point/bridge uses a blinking code to identify various error conditions. The code sequence uses a two-digit diagnostic code that starts with a long pause to delimit the code, followed by the LED flashing red to count out the first digit, then a short pause, followed by the LED flashing red to count out the second digit.

The LED blinking error codes are described in Table 22-7.

Table 22-7 LED Blinking Error Codes

LED	Blinking Codes		Description
	First Digit	Second Digit	
Ethernet	2	1	Ethernet cable problem—verify that the cable is properly connected and not defective. This error might also indicate a problem with the Ethernet link. If the cable is connected properly and not defective, contact technical support for assistance.
Radio	1	2	Radio not detected—contact technical support for assistance.
	1	3	Radio not ready—contact technical support for assistance.
	1	4	Radio did not start—contact technical support for assistance.
	1	5	Radio failure—contact technical support for assistance.
	1	6	Radio did not flash its firmware—contact technical support for assistance.

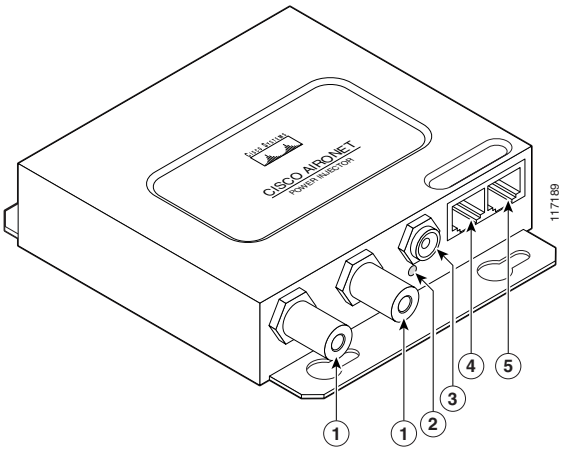
Power Injector

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

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

The power injector LED is shown in Figure 22-10.

Figure 22-10 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 bridge)
  - 48-VDC input power
  - Uses the 48-VDC power module (included with the bridge)
- Cisco Aironet Power Injector LR2T—optional transportation version
  - 12- to 40-VDC input power
  - Uses 12 to 40 VDC from a vehicle battery

Checking Power

You can verify the availability of power to the access point/bridge by checking the power injector LED (see Figure 22-10):

- Power LED
  - Green color indicates input power is being supplied to the bridge.
  - 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.

Low Power Condition

Access points can be powered from the 48-VDC power module or from an in-line power source. The 1130 and 1240 access points support 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 1130 and 1240 series access points require 12.95 W of power. 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 12.95 W. Also, some high-power inline power sources, might not be able to provide 12.95 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.

On power up, the 1130 and 1240 series access points are 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, displays a low power message on the browser and serial interfaces, and creates an event log entry.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the wireless device does not communicate with client devices, check the areas described in this section.

SSID

Wireless clients attempting to associate with the wireless device must use the same SSID as the wireless device. If a client device's SSID does not match the SSID of an wireless device in radio range, the client device will not associate.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on the wireless device and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must set WEP Key 3 on the wireless device to exactly the same value. The wireless device does not need to use Key 3 as its transmit key, however.

Refer to Chapter 10, "Configuring Cipher Suites and WEP," for instructions on setting the wireless device's WEP keys.

Security Settings

Wireless clients attempting to authenticate with the wireless device must support the same security options configured in the wireless device, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If your radio clients are using EAP-FAST authentication, you must configure open authentication with EAP. If you do not configure open authentication with EAP, a warning message appears. If you are using the CLI. the following warning appears:

SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

If you are using the GUI, this warning message appears:

WARNING:
"Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured."

If a wireless client is unable to authenticate with the wireless device, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the wireless device settings.

Note The wireless device MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the wireless device radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Resetting to the Default Configuration

If you forget the password that allows you to configure the wireless device, you may need to completely reset the configuration. On 1100 and 1200 series access points, you can use the MODE button on the access point or the web-browser interface. On 350 series access points, you can use the web-browser or CLI interfaces.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. The default username and password are both **Cisco**, which is case-sensitive.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the MODE button.

Note You cannot use the mode button to reset the configuration to defaults on 350 series access points. To reset the configuration on 350 series access points, follow the instructions in the "Using the Web Browser Interface" section on page 22-22, or in the "Using the CLI" section on page 22-22.

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the **MODE** button while you reconnect power to the access point.

Step 3 Hold the **MODE** button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button.

Step 4 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). The default username and password are **Cisco**, which is case-sensitive.

Using the Web Browser Interface

Follow these steps to delete the current configuration and return all wireless device settings to the factory defaults using the web browser interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** or **Reset to Defaults (Except IP)** button.

Note Select **Reset to Defaults (Except IP)** if you want to retain a static IP address.

Step 8 Click **Restart**. The system reboots.

Step 9 After the wireless device reboots, you must reconfigure the wireless device by using the Web-browser interface or the CLI. The default username and password are **Cisco**, which is case-sensitive.

Using the CLI

Follow the steps below to delete the current configuration and return all wireless device settings to the factory defaults using the CLI.

Step 1 Open the CLI using a Telnet session or a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until the command prompt appears and the wireless device begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

Step 4 At the ap: prompt, enter the **flash_init** command to initialize the Flash.

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
```

```
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

Step 5 Use the **dir flash:** command to display the contents of Flash and find the config.txt configuration file.

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

Step 6 Use the **rename** command to change the name of the config.txt file to config.old.

```
ap: rename flash:config.txt flash:config.old
```

Step 7 Use the **reload** command to reboot the wireless device.

```
ap: reload
System configuration has been modified. Save (y/n)?y
Building configuration.
[OK]
Proceed with reload? [confirm]
Connection with host lost.
```

Step 8 When the access point has finished reloading the software, Establish a new Telnet session to the access point.

Note The wireless device is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default username and password (**Cisco**).

Step 9 When IOS software is loaded, you can use the **del** privileged EXEC command to delete the config.old file from Flash.

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

Reloading the Access Point Image

If the wireless device has a firmware failure, you must reload the image file using the Web browser interface or on 1100 and 1200 series access points, by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the wireless device firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image. On 350 series access points, you cannot use the MODE button to reload the image file, but you can use the CLI through a Telnet or console port connection.

Using the MODE button

You can use the MODE button on 1100 and 1200 series access points to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

Note You cannot use the mode button to reload the image file on 350 series access points. To reload the image file on 350 series access points, follow the instructions in the "Using the CLI" section on page 22-26.

If the wireless device experiences a firmware failure or a corrupt firmware image, indicated by three red LED indicators, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the wireless device IP address, and SSIDs.

Follow these steps to reload the access point image file:

Step 1 The PC you intend to use 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 *c1100-k9w7-tar.123-8.JA.tar* for an 1100 series access point or *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. For additional information, refer to the "Obtaining the Access Point Image File" and "Obtaining TFTP Server Software" sections.

Step 3 Rename the access point image file in the TFTP server folder. For example, if the image file is **c1100-k9w7-tar.123-8.JA.tar** for an 1100 series access point, rename the file to **c1100-k9w7-tar.default**.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power (the power jack for external power or the Ethernet cable for in-line 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 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, you must reconfigure the access point by using the Web-browser interface or the CLI.

Using the Web Browser Interface

You can also use the Web browser interface to reload the wireless device image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your wireless device configuration does not change when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the wireless device image file on your PC and download the image to the wireless device. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click **Browse** to find the image file on your PC.

Step 7 Click **Upload**.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the wireless device image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click **Upload**.

For additional information click the **Help** icon on the Software Upgrade screen.

Using the CLI

Follow the steps below to reload the wireless device image using the CLI. When the wireless device begins to boot, you interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the wireless device.

Note Your wireless device configuration is not changed when using the CLI to reload the image file.

Step 1 Open the CLI using a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

Step 4 When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the wireless device.

Note You must use upper-case characters when you enter the **IP-ADDR**, **NETMASK**, and **DEFAULT_ROUTER** options with the **set** command.

Your entries might look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

Step 5 Enter the **tftp_init** command to prepare the wireless device for TFTP.

```
ap: tftp_init
```

Step 6 Enter the **tar** command to load and inflate the new image from your TFTP server. The command must include this information:

- the **-xtract** option, which inflates the image when it is loaded
- the IP address of your TFTP server
- the directory on the TFTP server that contains the image
- the name of the image
- the destination for the image (the wireless device Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c350-k9w7-tar.122-13.JA1.tar flash:
```

Step 7 When the display becomes full, the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
```

```
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
 -- MORE --
```

Note If you do not press the spacebar to continue, the process eventually times out and the wireless device stops inflating the image.

Step 8 Enter the **set BOOT** command to designate the new image as the image that the wireless device uses when it reboots. The wireless device creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:

```
ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

Step 10 Enter the **boot** command to reboot the wireless device. When the wireless device reboots, it loads the new image.

```
ap: boot
```

Obtaining the Access Point Image File

You can obtain the wireless device image file from the Cisco.com by following these steps:

Step 1 Use your Internet browser to access the Tools and Resources Downloads page at the following URL:

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

Step 2 Expand the Wireless LAN Access folder.

Step 3 Expand the appropriate access point folder.

Step 4 Select the appropriate access point.

Step 5 Enter your CCO login and password. The Select Software page appears.

Step 6 Click **IOS**. A list of available Cisco IOS versions appears.

Step 7 Choose the version you wish to download. The download page for the version you chose appears.

Step 8 Click **WIRELESS LAN**.

Step 9 If prompted, enter your login and password. The Encryption Software Export Distribution Authorization page appears.

Step 10 Answer the questions on the page and click **Submit**. The Download page appears.

Step 11 Click **DOWNLOAD**. The Software Download Rules page appears.

Step 12 Read the Software Download Rules carefully and click **Agree**.

Step 13 If prompted, enter your login and password. A File Download window appears.

Step 14 Save the file to a director on your hard drive.

Obtaining TFTP Server Software

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

http://tftpd32.jounin.net

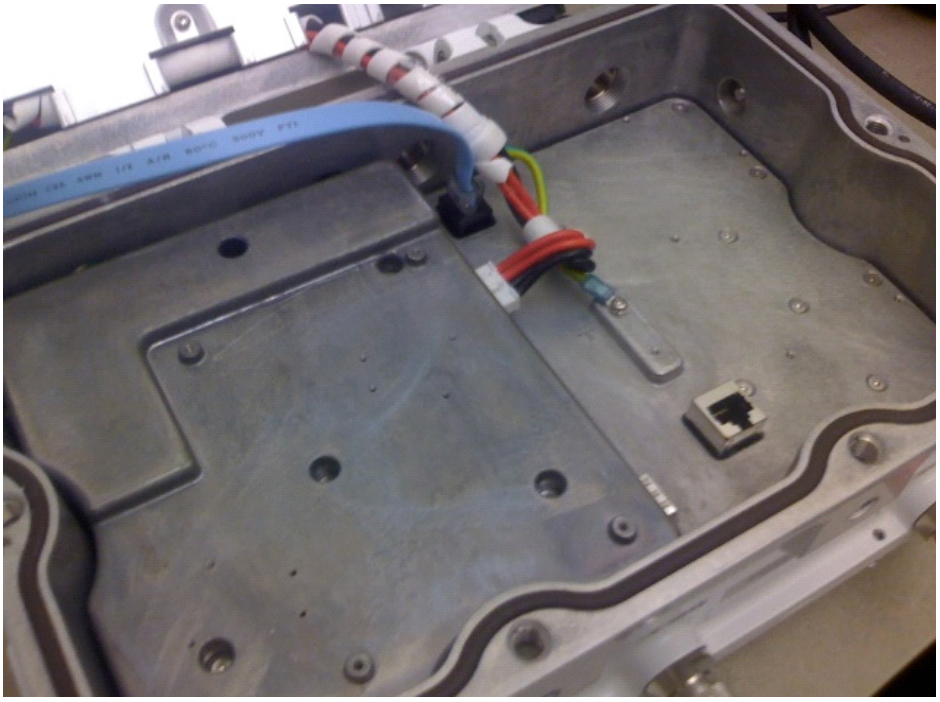
Follow the instructions on the website for installing and using the utility.

Image recovery on the 1520 Access Point

To perform image recovery on the 1520 access point, follow these steps:

Step 1 With the access point powered off, connect an RJ45 console cable to the console port (). The console port is the black plastic RJ45 jack inside the unit.

Figure 22-11 Connecting an RJ45 Console Cable to the Console Port



Step 2 Configure the terminal emulator for 8 databits, no parity, no flow control, 9600 bps.

Step 3 Apply power to the access point.

Step 4 When the bootloader displays “Base Ethernet MAC Address”, hit the <esc> key to break to the **ap:** prompt:

```
IOS Bootloader - Starting system.
Xmodem file system is available.
flashfs[0]: 13 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31868928
flashfs[0]: Bytes used: 9721344
flashfs[0]: Bytes available: 22147584
flashfs[0]: flashfs fsck took 20 seconds.
Reading cookie from flash parameter block...done.
Base Ethernet MAC address: 00:1f:27:75:db:00

The system boot has been aborted.  The following
commands will finish loading the operating system
software:
    ether_init
    tftp_init
    boot
```

```
ap:
```

Note If the **ENABLE_BREAK=no environmental** variable is set, you will not be able to escape to the bootloader.

Step 5 Cable the 1520 access point's LAN port ("PoE In") to a TFTP server. For example, a Windows PC with tftpd32 installed.

Step 6 Install a good copy of the **c1520 k9w8** IOS image on the TFTP server.

Step 7 Configure the TFTP server's LAN interface with a static IP address. For example, 10.1.1.1.

Step 8 On the access point enter:

```
ap: dir flash:
```

Verify there is enough free space on flash to hold the new code (or if the flash file system is corrupt), then enter:

```
ap: format flash:
```

Step 9 Copy the image using TFTP to the 1520 access point's flash:

```
ap: set IP_ADDR 10.1.1.2

ap: set NETMASK 255.255.255.0

ap: ether_init
Initializing ethernet port 0...

ap: tftp_init
tftp_init success: You can now use tftp file system!

ap: tar -xtract tftp://10.1.1.1/c1520-k9w8-tar.124-21a.JA2 flash:

extracting info (293 bytes)
c1520-k9w8-mx.124-21a.JA2/ (directory) 0 (bytes)
extracting c1520-k9w8-mx.124-21a.JA2/c1520-k9w8-mx.124-21a.JA2 (5197365 bytes)..
.........................................
extracting c1520-k9w8-mx.124-21a.JA2/8001.img (97896 bytes).....................
extracting c1520-k9w8-mx.124-21a.JA2/c1520_avr_1.img (10368 bytes)..
extracting c1520-k9w8-mx.124-21a.JA2/c1520_avr_2.img (10624 bytes)..
extracting c1520-k9w8-mx.124-21a.JA2/c1520_avr_3.img (14720 bytes)...
extracting c1520-k9w8-mx.124-21a.JA2/info (293 bytes)
extracting info.ver (293 bytes)
ap: set
49_RADIO_CARRIER_SET=0x0024
49_RADIO_MAX_TX_POWER=400
58_RADIO_CARRIER_SET=0x0027
58_RADIO_MAX_TX_POWER=640
5G_RADIO_ANTENNA_DIVERSITY=0x01
5G_RADIO_CARRIER_SET=0x000B
5G_RADIO_ENCRYPTION_CONFIG=0x0002
5G_RADIO_MAX_TX_POWER=250
BOOT=flash:/c1520-k9w8-mx.124-18a.JA1/c1520-k9w8-mx.124-18a.JA1
CRASH_LOG=yes
DEFAULT_ROUTER=10.0.0.1
DOT11G_RADIO_MODE=0xFF
DOT11_DEVICE_TYPE=4C
DOT11_ENCRYPTION_CONFIG=0x0002
DOT11_MAX_ASSOCIATION_NUM=2007
ENABLE_BREAK=yes
FAB_PART_NUM=1c 1f 44 03
```

```
IP_ADDR=10.1.1.2
MAC_ADDR=00:1F:27:75:DB:00
MAC_ADDR_BLOCK_SIZE=01 00
NETMASK=255.255.255.0
NEW_IMAGE=yes
PCA_ASSY_NUM_800=03 20 00 70 ed 03
PCA_PART_NUM_73=49 2a a6 03
PCA_REVISION_NUM=B0
PCA_REVISION_NUM_800=B0
PCB_SERIAL_NUM=FOC1213496Z
PEP_PRODUCT_ID=AIR-LAP1524PS-A-K9
PEP_VERSION_ID=V01
PRODUCT_MODEL_NUM=AIR-LAP1524PS-A-K9
RADIO_ANTENNA_DIVERSITY=0x01
RADIO_CARRIER_SET=0x0000
RADIO_MAX_TX_POWER=640
RELOAD_REASON=23
SYSTEM_REVISION_NUM_800=A0
TERMLINES=0
TOP_ASSY_NUM_800=03 20 00 77 2e 01
TOP_ASSY_SERIAL_NUM=FTX1218P080

ap:

ap: dir flash:
Directory of flash:/

2    -rwx  63        <date>              mesh_cfg.txt
3    -rwx  4515840   <date>              c1520-img-tar
4    -rwx  213       <date>              mesh_port_cfg.txt
9    drwx  384       <date>              c1520-k9w8-mx.124-18a.JA1
5    -rwx  1008      <date>              env_vars
6    -rwx  293       <date>              info
7    -rwx  9240      <date>              private-multiple-fs
8    -rwx  90439     <date>              event.log
15   drwx  384       <date>              c1520-k9w8-mx.124-21a.JA2
10   -rwx  3564      <date>              private-config
24   -rwx  293       <date>              info.ver

16813056 bytes available (15055872 bytes used)

ap: set BOOT flash:/c1520-k9w8-mx.124-21a.JA2/c1520-k9w8-mx.124-21a.JA2

ap: boot
Loading "flash:/c1520-k9w8-mx.124-21a.JA2/c1520-k9w8-mx.124-21a.JA2"...#########
###################################################################
[ ... ]
*Mar  1 00:00:14.047: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Version 12.4(21a)JA2, RELEASE SOFTWARE
(fc1)
```