



Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point/bridge. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Hardware Support > Wireless Devices**):

<http://www.cisco.com/cisco/web/support/index.html>

Sections in this chapter include:

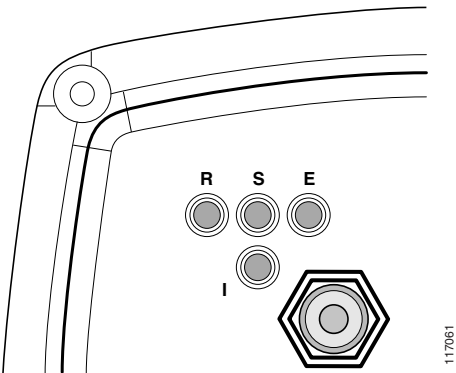
- [Checking the LEDs, page 21-2](#)
- [Power Injector, page 21-4](#)
- [Checking Power, page 21-5](#)
- [Checking Basic Configuration Settings, page 21-5](#)
- [Antenna Alignment, page 21-6](#)
- [Resetting the Access Point/Bridge to the Default Configuration, page 21-6](#)
- [Reloading the Access Point/Bridge Image, page 21-9](#)

Checking the LEDs

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 21-1 shows the access point/bridge LEDs.

Figure 21-1 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 21-1.

Table 21-1 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 21-1 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 21-2](#).

Table 21-2 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.

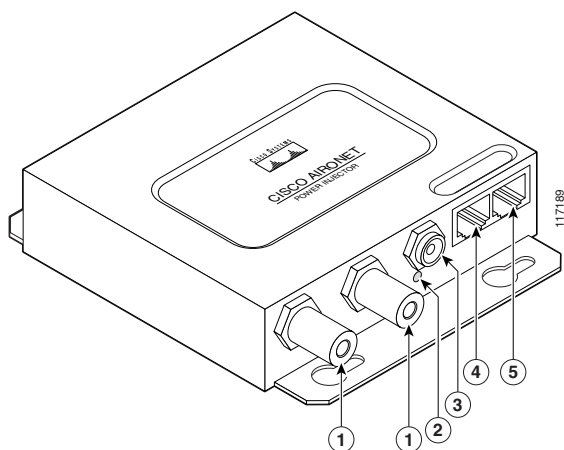
Power Injector

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 21-2](#).

Figure 21-2 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 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 21-2](#)):

- 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.

Checking Basic Configuration Settings

Mismatched basic settings are the most common causes of lost wireless connectivity. If the access point/bridge does not associate with a remote bridge, access point, or client device, check the following areas.

SSID

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



Note

Access points and bridges are not designed to associate together. However, a workgroup bridge can associate to either a Cisco Aironet access point or a Cisco Aironet bridge.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on the access point/bridge 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 access point/bridge to exactly the same value. The access point/bridge does not need to use Key 3 as its transmit key, however.

Refer to [Chapter 9, “Configuring Cipher Suites and WEP,”](#) for instructions on setting the wireless device’s WEP keys.

Security Settings

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

If a wireless client is unable to authenticate with the access point/bridge, 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 access point/bridge settings.

**Note**

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

Antenna Alignment

If your non-root bridges or non-root access points are unable to associate to your root bridge or root access point, you should verify the basic configuration settings on all bridges or access points before attempting to verify antenna alignment ([Chapter 2, “Configuring the Access Point/Bridge for the First Time.”](#)) If your basic configuration settings are correct, you can verify antenna alignment by using the Install mode RSSI LED indications. For additional information, refer to the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Mounting Instructions* that shipped with your access point/bridge.

**Note**

To meet regulatory restrictions, the external antenna access point/bridge unit and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Resetting the Access Point/Bridge to the Default Configuration

You can use the web-browser interface or the CLI to reset the access point/bridge to a factory default configuration.

**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 Web-Browser Interface

Follow the steps below to delete the current configuration and return all access point/bridge settings to the factory defaults using the Web-browser interface.

-
- Step 1** Open your Internet browser.
- Step 2** Enter the bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Enter your username (default *Cisco*) in the User Name field.
- Step 4** Enter the access point/bridge password (default *Cisco*) 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 one of the following:
- a. **Reset to Defaults**. This option deletes a static IP address and resets the Configuration Server Protocol setting to DHCP.
 - b. **Reset to Defaults (Except IP)**. This option does not reset the IP address.
- Step 8** After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).
-

Using the CLI

From the privileged EXEC mode, you can reset the access point/bridge configuration to factory default values using the CLI by following these steps:

-
- Step 1** Enter **erase nvram:** to erase all NVRAM files including the startup configuration.
- Step 2** Enter **Y** when the following CLI message displays: *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]*.
- Step 3** Enter **reload** when the following CLI message displays: *Erase of nvram: complete*. This command reloads the operating system.
- Step 4** Enter **Y** when the following CLI message displays: *Proceed with reload? [confirm]*.

**Caution**

Do not interrupt the boot process to avoid damaging the configuration file. Wait until the access point/bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished: *Line protocol on Interface Dot11Radio0, changed state to up.*

Step 5

After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).

The access point/bridge is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the unit's new IP address, you can use the *show interface bvi1* CLI command. If the unit does not receive an IP address from a DHCP server, the access point/bridge IP address is 10.0.0.1.

Corrupt IOS Configuration or Lost Password Procedure

This section describes the procedure for resetting the access point/bridge to its default settings in the unlikely event that the operating system is corrupt or if you have misplaced the configuration login and password. Because the access point/bridge does not have a mode switch, you must use the console port to perform this operation. Follow these steps to reset the unit to its default settings:

Step 1 Open the CLI using a Telnet session or a connection to the access point/bridge's console port.

Step 2 Reboot the access point/bridge by removing power and reapplying power.

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

**Note**

Depending on the terminal emulation software you are using, you may have to press **Esc** twice to access the boot loader.

```
Loading "flash:/c1310-k9kw-7mx.v122_15_ja.200040314-k9w7-mx.v122_15_ja.20040314"
...#####
#####
#####
```

Messages similar to those below appear:

```
Error loading "flash:/c1310-k9kw-7mx.v122_15_ja.200040314-k9w7-mx.v122_15_ja.20040314"
```

```
Interrupt within 5 seconds to abort boot process.
Boot process terminated.
```

```
The system is unable to boot automatically. The BOOT environment variable needs to be set
to a bootable image.
```

```
C1310 Boot Loader (C1310-BOOT-M), Version 12.2 [BLD-v122_15_ja_throttle.20040314 100]
```

```
ap:
```

Step 4 At the prompt, enter the following command to show a directory of the flash file system similar to the directory shown below:


```

ap: dir flash:
Directory of flash:/

 2  -rwx   0      <date>    env_vars
 5  drwx  384    <date>    C1310-k9w7-mx.v133_15_JA.20040314
 3  -rwx  1128   <date>    config.txt
 4  -rwx   5     <date>    private-config

3693568 bytes available (4047872 bytes used)

```

ap:

Step 5 Reboot the bridge.



Note

The access point/bridge is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default case-sensitive user name and password (**Cisco**).



Note

If your access point/bridge does not use a DHCP server to obtain an IP address, it continues to request a DHCP address. To assign an IP address, you must access the CLI using the console. See [“Obtaining and Assigning an IP Address” section on page 2-2](#) for information.

Reloading the Access Point/Bridge Image

If your access point/bridge has a firmware failure, you must reload the complete image file using the Web-browser interface or by using the console serial port. You can use the browser interface if the access point/bridge firmware is operational. However, you can use the console serial port when the access point/bridge has a corrupt image.

Web-Browser Interface

You can also use the Web-browser interface to reload the access point/bridge image file. The Web-browser interface supports loading the image file using HTTP or TFTP interfaces.



Note

Your access point/bridge configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the access point/bridge image file on your PC and download the image to the unit. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser.

Step 2 Enter the access point/bridge’s IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.

- Step 3** Enter your username in the User Name field.
 - Step 4** Enter the access point/bridge 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 locate the image file on your PC.
 - Step 7** Click **Upgrade**.
 - Step 8** After the access point/bridge reboots, you can reconfigure the unit by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).
For additional information, click the **Help** icon on the Software Upgrade screen.
-

Browser TFTP Interface

The TFTP interface enables you to use a TFTP server on a network device to load the access point/bridge image file. Follow the instructions below to use a TFTP server:

-
- Step 1** Open your Internet browser.
 - Step 2** Enter the access point/bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
 - Step 3** Enter your username in the User Name field.
 - Step 4** Enter the access point/bridge password in the Password field and press **Enter**. The Summary Status page appears.
 - Step 5** Click **System Software** and then click **Software Upgrade**. The HTTP Upgrade screen appears.
 - Step 6** Click **TFTP Upgrade**. The TFTP Upgrade screen appears.
 - Step 7** Enter the IP address for the TFTP file server in the TFTP File Server field.
 - Step 8** Enter the filename for the access point/bridge image file (*c1310-k9w7-tar.122-15.JA.tar*) 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 in the TFTP root directory, enter only the filename.
 - Step 9** Click **Upgrade**.
 - Step 10** After the access point/bridge reboots, you can reconfigure the access point/bridge by using the Web-browser interface or the CLI (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* or to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).
For additional information click the **Help** icon on the Software Upgrade screen.
-

Using the CLI

Follow the steps below to reload the access point image using the CLI. When the access point 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 access point.



Note Your access point configuration is not changed when using the CLI to reload the image file.

- Step 1** Open the CLI using a Telnet session or a connection to the access point console port.
- Step 2** Reboot the access point by removing power and reapplying power.
- Step 3** Let the access point boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c1310-k9w7-mx.v122_13_ja.20031010/c1310-k9w7-mx.v122_13_ja.20031010"
...#####
#####
#####
#####
#####
```



Note Depending on the terminal emulation software you are using, you may have to press **Esc** twice to access the boot loader.

- Step 4** When the bridge: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the access point.



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 access point 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 access point Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c1310-k9w7-tar.122_15.JA1 flash:
```

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

```
extracting info (229 bytes)
c1310-k9w7-mx.122-15.JA1/ (directory) 0 (bytes)
c1310-k9w7-mx.122-15.JA1/html/ (directory) 0 (bytes)
c1310-k9w7-mx.122-15.JA1/html/level1/ (directory) 0 (bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/appsui.js (558 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/back.htm (205 bytes)
```

```

extracting c1310-k9w7-mx.122-15.JA1/html/level1/cookies.js (5027 bytes).
extracting c1310-k9w7-mx.122-15.JA1/html/level1/forms.js (15704 bytes)...
extracting c1310-k9w7-mx.122-15.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c1310-k9w7-mx.122-15.JA1/html/level1/config.js (2554 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/stylesheets.css (3215 bytes)
c1310-k9w7-mx.122-15.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c1310-k9w7-mx.122-15.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869
bytes)
-- MORE --

```

If you do not press the spacebar to continue, the process eventually times out and the access point stops inflating the image.

- Step 8** Enter the **set BOOT** command to designate the new image as the image that the access point uses when it reboots. The access point 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:/c1310-k9w7-mx.122-15.JA1/c1310-k9w7-mx.122-15.JA1
```

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

```

ap: set
BOOT=flash:/c1310-k9w7-mx.122-15.JA1/c1310-k9w7-mx.122-15.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 access point. When the access point reboots, it loads the new image.

```
ap: boot
```

## Obtaining the Access Point/Bridge Image File

You can obtain the access point/bridge image file from the Cisco.com software center by following these steps:

- Step 1** Use your Web-browser to go to the Cisco Software Center at the following URL:  
<http://www.cisco.com/cisco/software/navigator.html>
- Step 2** Select **Option #1: Aironet Wireless Software Display Tables**. The Wireless Software page appears.
- Step 3** Scroll down to the Cisco Aironet Wireless Bridge Firmware and Utilities section and click **Cisco Aironet 1300 Series**. The Software Download page for the Cisco Aironet 1300 Series Wireless Bridge Firmware and Utilities appears.
- Step 4** Select the release you desire to download and click **Submit**. The Encryption Authorization Form appears.

- Step 5** On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply. Click **Submit**.
  - Step 6** Read and accept the terms and conditions of the Software License Agreement.
  - Step 7** Select the access point/bridge image file again to download it.
  - Step 8** Save the file to a directory on 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.

