Troubleshooting Autonomous Access Points and Bridges

This chapter provides troubleshooting procedures for basic problems with the autonomous access point/bridge (model: AIR-BR1310G). 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/support/index.html

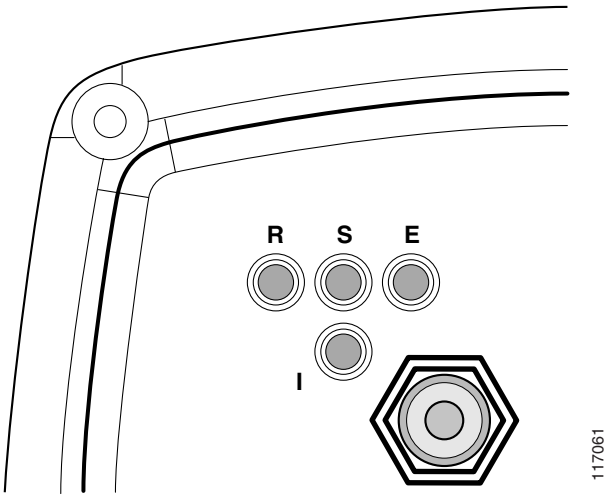
Sections in this chapter include:

Checking the LEDs on an Autonomous Access Point/Bridge

If your autonomous access point/bridge is not associating with a remote bridge or a wireless client, 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 antenna, refer to the "LEDs" section on page 3-5.

Figure 4-1 shows the access point/bridge LEDs.

Figure 4-1 LEDs



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

Normal Mode LED Indications for an Autonomous Access Point/Bridge

During normal operation of your autonomous access point/bridge the LEDs provide status information as shown in Table 4-1.

Table 4-1 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 4-1 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 autonomous 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 4-2.

Table 4-2 LED Blinking Error Codes on an Autonomous Access Point/Bridge

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.

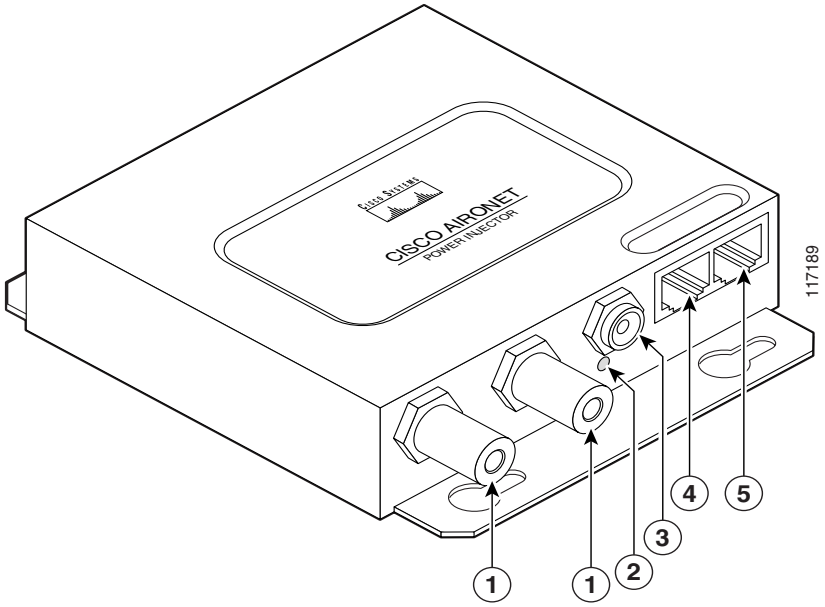
Power Injector

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 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 4-2.

Figure 4-2 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 4-2):

- 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. Check the following areas.

Default IP Address Behavior

When you connect an autonomous access point/bridge running Cisco IOS Release 12.3(2)JA or later software with a default configuration to your LAN, the access point/bridge requests an IP address from your DHCP server and, if it does not receive an IP address, continues to send requests indefinitely. To eliminate this behavior, you must access the access point/bridge through its console port and assign a static IP address.

When you connect an autonomous access point/bridge running Cisco IOS Release 12.2(15)JA2 or earlier software with a default configuration to your LAN, the access point/bridge requests an IP address from your DHCP server and, if it does not receive an IP address, it assigns a default IP address of 10.0.0.1

Default SSID and Radio Behavior

In Cisco IOS Release 12.3(2)JA2 and earlier, on initial power up the access point/bridge defaults to the Install-Mode role with the radio enabled and supports these SSIDs:

- SSID is *autoinstall* for the Install-Mode role.
- SSID is *tsunami* for Root AP and Workgroup Bridge roles.

In Cisco IOS Release 12.3(4)JA or later, on initial power up the access point/bridge defaults to the Root AP role with the radio disabled and no default SSID configured.

Note In Cisco IOS Release 12.3(4)JA or later, you must create an SSID and enable the radio before the access point/bridge allows wireless associations from other devices. These changes to the default configuration improve the security of a newly installed access point/bridge. Refer to the *Cisco IOS Software Configuration Guide for Access Points* for instructions on configuring the SSID and to the "Enabling the Radio Interface" section on page 4-7 for instructions on enabling the radio interface.

Enabling the Radio Interface

To enable the radio interface, follow these instructions:

Step 1 Open your web browser and enter the access point/bridge's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 When the Summary Status page displays, click **Network Interfaces > Radio0-802.11g** and the radio status page displays.

Step 4 Click **Settings** and the radio settings page displays.

Step 5 Click **Enable** in the Enable Radio field.

Step 6 Click **Apply**.

Step 7 Close your web-browser.

SSID

To associate, all bridges, access points, workgroup bridges, or client devices must use the same SSID. The bridge installation mode SSID is *autoinstall* and the normal mode default SSID is *tsunami*. You should verify that the SSID value shown on the Express Setup page is the same for all bridges, access points, workgroup bridges, or client devices. You should also verify that the bridges or access points are configured for the proper network role; only one bridge can be configured as the root bridge and only one access point can be configured as a root access point.

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

Note In Cisco IOS Release 12.3(4)JA or later, there is no default SSID. You must configure an SSID and enable the radio interface to communicate with other wireless devices.

Security Settings

Remote Cisco Aironet bridges or client devices attempting to authenticate to your access point/bridge must support the same security options configured in the access point/bridge, such as WEP, EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a Cisco Aironet non-root bridge or a non-root access point is unable to authenticate to your root bridge or root access point, verify that the security settings are the same as your access point/bridge settings. For additional information, refer to the *Cisco IOS Software Configuration Guide for Access Points*.

Antenna Alignment

If your autonomous non-root bridges are unable to associate to your root bridge, you should verify the basic configuration settings on all bridges before attempting to verify antenna alignment (refer to *Cisco IOS Software Configuration Guide for Access Points*). 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 "Aligning the Autonomous Bridge Antenna Using RSSI LED Indications" section on page 3-6.

For detailed alignment instructions, refer to the *Cisco Aironet 1300 Series Outdoor 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.

Running the Carrier Busy Test

You can use the carrier busy test to determine the least congested channel for the radio interface (802.11g). You should typically run the test several times to obtain the best results and to avoid temporary activity spikes.

Note The carrier busy test is primarily used for single access points or bridge environments. For sites with multiple access points, a site survey is typically performed to determine the best operating locations and operating frequencies for the access points.

Note All associated clients on the selected radio will be disassociated during the 6 to 8 seconds needed for the carrier busy test.

Follow these steps to activate the carrier busy test:

Step 1 Open your web browser and enter the access point/bridge's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 Click **Network Interfaces** and the Network Interface Summary page appears.

Step 4 Choose the radio interface by clicking **Radio0-802.11G**. The radio status page appears.

Step 5 Click the **Carrier Busy Test** tab and the Carrier Busy Test page appears.

Step 6 Click **Start** to begin the carrier busy test.

When the test completes, the results are displayed on the bottom of the page. For each of the channel center frequencies, the test produces a value indicating the percentage of time that the channel is busy.

Running the Ping or Link Test

You can use the ping or link test to evaluate the communication link with an associated wireless device. The ping or link test provides two modes of operation:

- Uses a specified number of packets and then displays the test results.
- Continuously operates until you stop the test and then displays the test results.

Follow these steps to activate the ping or link test:

Step 1 Open your web browser and enter the access point/bridge's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 Click **Association** and the main association page appears.

Step 4 Click the MAC address of an associated wireless device and the Statistics page for that device appears.

Step 5 Click the **Ping/Link Test** tab and the Ping/Link Test page appears.

Step 6 If you want to specify the number of packets to use in the test, follow these steps:

a. Enter the desired number of packets in the Number of Packets field.

b. Enter the desired packet size in the Packet Size field.

c. Click **Start**. The test automatically stops when all packets are used.

Step 7 If you want to use a continuous test, follow these steps:

a. Enter the desired packet size in the Packet Size field.

b. Click **Start** to activate the test.

c. When desired, click **Stop** to stop the test.

When the test stops, the test results are displayed at the bottom of the page. You should check for lost packets that might indicate a possible problem with the wireless link. For best results, you should perform this test several times.

Resetting the Autonomous Access Point/Bridge to the Default Configuration

You can use the web-browser interface or the CLI to reset the autonomous 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.

For additional information on access point/bridge default behavior, see the "Default IP Address Behavior" section on page 4-6 and the "Default SSID and Radio Behavior" section on page 4-6.

Using the Web-Browser Interface

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

Step 1 Open your web-browser and enter the access point/bridge's IP address in the browser address or location line. Press **Enter**.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 3 Click **System Software** and the System Software page appears.

Step 4 Click **System Configuration** and the System Configuration page appears.

Step 5 Click **Default**.

Note If the access point/bridge is configured with a static IP address, the IP address does not change.

Step 6 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 Access Points)*.

Using the CLI on an Autonomous Access Point/Bridge

From privileged EXEC mode, you can reset the autonomous 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 Interrupting the boot process will damage 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 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.

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 autonomous access point/bridge configuration is not changed when you use 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 The PC you intend to use must be configured with a static IP address in the same subnet as the access point.

Step 2 Open your web-browser and enter the access point/bridge's IP address in the browser address or location line. Press **Enter**. An Enter Network Password window appears.

Step 3 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 4 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade page appears.

Step 5 Click **Browse** to locate the image file on your PC.

Step 6 Click **Upload**.

Step 7 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 Access Points*).

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

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 The PC you intend to use must be configured with a static IP address in the same subnet as the access point.

Step 2 Open your web-browser and enter the access point/bridge's IP address in the browser address or location line. Press **Enter**. An Enter Network Password window appears.

Step 3 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.The Summary Status page appears.

Step 4 Click **System Software** and then click **Software Upgrade**. The HTTP Upgrade page appears.

Step 5 Click **TFTP Upgrade**.

Step 6 Enter the IP address for the TFTP server in the TFTP Server field.

Step 7 Enter a filename for the access point/bridge image file (such as c1310-k9w7-tar.123-8.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 8 Click **Upload**.

Step 9 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 Access Points*).

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

Obtaining the Autonomous Access Point/Bridge 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://www.cisco.com/cisco/software/navigator.html

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**.

Step 3 Choose **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1300 Series** .

Step 4 Click **Cisco Aironet 1310 Access Point/Bridge**.

Step 5 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 6 Click **IOS**.

Step 7 Choose the Cisco IOS release desired, such as 12.3.11.JA.

Step 8 Click **WIRELESS LAN** for an access point image file, such as c1310-k9w7-tar.123-11.JA.tar.

Step 9 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 10 On the Security Information window, click **Yes** to display non-secure items.

Step 11 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 12 If you checked No, enter the requested information and click **Submit**.

Step 13 Click **Yes** to continue.

Step 14 Click **DOWNLOAD**.

Step 15 Read and accept the terms and conditions of the Software Download Rules.

Step 16 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 17 Click **Save** to download your image file to your hard disk.

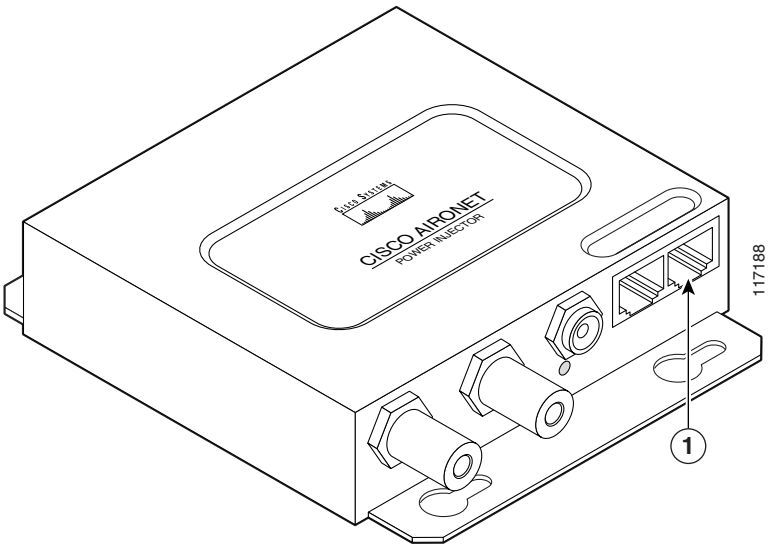
Step 18 Select the desired download location on your hard disk and click **Save**.

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. 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 console port on the power injector and to the COM port on your PC. Figure 4-3 shows the power injector's console serial port connector.

Figure 4-3 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/pcgi-bin/marketplace/welcome.pl 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 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.