



CHAPTER 6

Troubleshooting Autonomous Access Points

This chapter provides troubleshooting procedures for basic problems with the 1200 series autonomous access point (models: AIR-AP1200, AIR-AP1210, AIR-AP1220B, AIR-AP1230B, AIR-AP1220A, AIR-AP-1230A, AIR-AP1231G, and AIR-AP1232AG) . For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

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

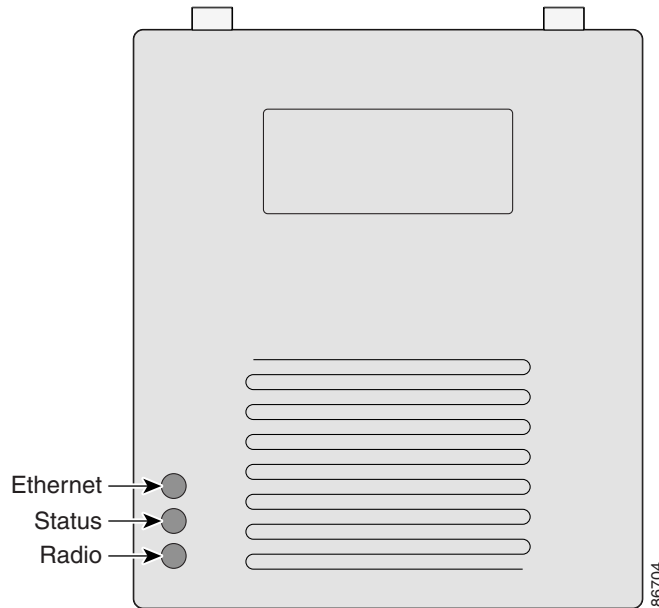
Sections in this chapter include:

- [Checking the Top Panel LEDs, page 6-2](#)
- [Checking Basic Settings, page 6-4](#)
- [Resetting to the Default Configuration, page 6-7](#)
- [Reloading the Access Point Image, page 6-8](#)
- [Obtaining the Access Point Image File, page 6-11](#)
- [Obtaining the TFTP Server Software, page 6-12](#)

Checking the Top Panel LEDs

If your access point is not communicating, check the three LEDs on the top panel. You can use them to quickly assess the unit's status. [Figure 6-1](#) shows the LEDs.

Figure 6-1 Access Point LEDs



The LEDs signals have the following meanings (for additional details refer to [Table 6-1](#)):

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

Table 6-1 Top Panel LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failure	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following areas.

Default IP Address Behavior

When you connect a 1200 series access point running Cisco IOS Release 12.3(2)JA or later software with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an IP address, continues to send requests indefinitely.

When you connect a 1200 series access point running Cisco IOS Release 12.2(15)JA or earlier software with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an IP address, the access point assigns a default IP address of 10.0.0.1

Default SSID and Radio Behavior

In Cisco IOS Release 12.3(2)JA and earlier, the access point radio is enabled by default and the default SSID is *tsunami*.

In Cisco IOS Release 12.3(4)JA and later, the access point radio is disabled by default for security reasons, and there is no default SSID. You must create an SSID and enable the radio before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on configuring the SSID and the “[Enabling the Radio Interfaces](#)” section on page 6-4 for instructions on enabling the radio interface.

Enabling the Radio Interfaces

In Cisco IOS Release 12.3(4)JA and later, the access point radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radios before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on configuring the SSID.

To enable the radio interfaces, follow these instructions:

-
- Step 1** Use your internet browser to access your access point.
 - Step 2** At the prompt, 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 > Radio0-802.11b** or **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 and click **Apply**.
 - Step 6** Click **Radio1-802.11A** and the radio status page displays.
 - Step 7** Repeat Steps 3 and 4.

Step 8 Close your internet browser.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device's SSID does not match the SSID of an access point in radio range, the client device will not associate. In Cisco IOS Release 12.3(2)JA2 and earlier, the access point default SSID is *tsunami*.



Note

In Cisco IOS Release 12.3(4)JA and later, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

WEP Keys

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

Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting the access point's WEP keys.

Security Settings

Wireless clients attempting to authenticate with your access point must support the same security options configured in the access point, 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 your access point, 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 settings.



Note

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

Running the Carrier Busy Test

You can use the carrier busy test to find the least congested channel for a radio interface (802.11b/g or 802.11a). 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 a single access point or a bridge environment. 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.

Perform these steps to activate the carrier busy test:

Step 1 Use your web browser to open the access point interface.

**Note**

The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

Step 2 At the prompt, 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 experiencing problems by clicking **Radio0-802.11B** or **Radio0-802.11G** or **Radio1-802.11A**. The respective radio status page appears.

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

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

When the test completes, the results are displayed on the bottom of the screen. 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. With the ping or link test you can:

- a. Perform a test using a specified number of packets and then display the test results.
- b. Perform a test that continuously operates until you stop it and then display the test results.

Perform these steps to activate the ping or link test:

Step 1 Use your web browser to open the access point interface.

**Note**

The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

- Step 2** At the prompt, 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:
- Enter a number of packets in the Number of Packets field
 - Enter a packet size in the Packet Size field.
 - Click **Start**. The test automatically stops when all packets are utilized.
- Step 7** If you want to use a continuous test, follow these steps:
- Enter a packet size in the Packet Size field.
 - Click **Start** to activate the test.
 - 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 problem with the wireless link. For best results, you should perform this test several times.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you may need to completely reset the configuration. You can use the MODE button on the access point or the web-browser interface.



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 default behavior, refer to the [“Default IP Address Behavior” section on page 6-4](#) and the [“Default SSID and Radio Behavior” section on page 6-4](#).

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:

- 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 2 to 3 seconds), and release the button.

- Step 4** After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.



Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP).

Using the Web Browser Interface

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

- Step 1** Open your Internet browser.



Note The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

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

- Step 3** At the prompt, 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 the System Software screen appears.

- Step 5** Click **System Configuration** and the System Configuration screen appears.

- Step 6** Click the **Reset to Defaults** button.



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

- Step 7** After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.

Reloading the Access Point Image

If your access point has a firmware failure, you must reload the complete access point image file using the Web browser interface or by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the access point 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.

**Caution**

Your access point must be running specific Cisco IOS software releases before you upgrade its radios; otherwise, your access point might not be able to complete the boot sequence until the radio is removed (see [Table 6-3](#)). For additional information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Table 6-2 Required Cisco IOS Software Release

Radio Upgrade	Required Cisco IOS Software Release
IEEE 802.11g	12.2(13)JA or later
RM21A or RM22A	12.3(2)JA or later

Using the MODE button

You can use the MODE button on the access point 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**

If your access point experiences a firmware failure or a corrupt firmware image, indicated by three red LEDs, 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 access point IP address, and SSIDs.

Follow the steps below 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 same subnet as the access point.
- Step 2** Place a copy of the access point image file (such as *c1200-k9w7-tar.123-8.JA.tar*) into the TFTP server folder on your PC. For additional information, refer to the “[Obtaining the Access Point Image File](#)” and “[Obtaining the TFTP Server Software](#)” sections.
- Step 3** Rename the access point image file in the TFTP server folder to **c1200-k9w7-tar.default**.
- Step 4** Activate the TFTP server.
- Step 5** Connect the PC to the access point power injector using a Category 5 (CAT5) Ethernet cable.
- Step 6** Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.
- Step 7** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 8** Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the **MODE** button.
- Step 9** Wait until the access point reboots as indicated by all LEDs turning green followed by the status LED blinking green.

- Step 10** After the access point reboots, you must reconfigure the access point by using the Web interface, the Telnet interface, or Cisco IOS commands.
-

Web Browser Interface

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



Note Your access point 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 image file on your PC and download the image to the access point. Follow the instructions below to use the HTTP interface:

- Step 1** Open your Internet browser.



Note The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

- Step 2** Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.
- Step 3** At the prompt, 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 screen appears.
- Step 5** Click the **Browse** button to locate the access point image file (such as *c1200-k9w7-tar.123-8.JA.tar*) on your PC.
- Step 6** Click the **Upload** button.

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 access point image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser.



Note The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

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

Step 3 At the prompt, 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 screen appears.

Step 5 Click the **TFTP Upgrade** tab.

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

Step 7 Enter the file name for the access point image file (such as *c1200-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 located in the TFTP root directory, enter only the filename.

Step 8 Click the **Upload** button.

Step 9 When a message appears that indicates the upgrade is complete, click **OK**.
For additional information click the **Help** icon on the Software Upgrade screen.

Obtaining the Access Point Image File



Caution

Your access point must be running specific Cisco IOS software releases before you upgrade its radios; otherwise your access point might not be able to complete the boot sequence until the radio is removed (see [Table 6-3](#)). For additional information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Table 6-3 Required Cisco IOS Software Release

Radio Upgrade	Required Cisco IOS Software Release
IEEE 802.11g	12.2(13)JA or later
RM21A or RM22A	12.3(2)JA or later

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

**Note**

To download software from the Cisco.com software center, you must be a registered user. You can register from the main Cisco.com web page at this URL: <http://cisco.com>.

-
- Step 1** Use your Internet browser to access the Cisco Software Center at the following URL:
<http://www.cisco.com/kobayashi/sw-center/index.shtml>
- Step 2** Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1200 Series > Cisco Aironet 1200 Access Point**. The Enter Password window appears.
- Step 3** Enter your username and password in the respective fields and click **OK**. The **Select a Software Type** page appears.
- Step 4** Click **IOS** and the Select a Release page appears.
- Step 5** Click on the IOS release for the desired access point image file, such as *12.3(8)JA*.
- Step 6** Click **Wireless LAN** and the Enter Password window appears.
- Step 7** Enter your username and password in the respective fields and click **OK**.
- Step 8** If you receive a *Do you want to display the nonsecure items?* message, click **Yes**.
- Step 9** On the Encryption Software Export Distribution Authorization Form, read the information and click the appropriate box.
- Step 10** Click **Submit**.
- Step 11** If you indicated that the software is not for you or your company, follow these steps:
- a. If you receive a *Do you want to display the nonsecure items?* message, click **Yes**. The Encryption Software Export Distribution Authorization window appears.
 - b. Carefully read the information and enter the Cisco.com user profile or detailed data describing the end user of this software image in the provided fields.
 - c. Click **Submit**.
- Step 12** If you receive a *Do you wish to continue?* security alert message, click **Yes** to continue.
- Step 13** Click **Download**.
- Step 14** Carefully read the Software Download Rules and click **Agree** to download the image file. An Enter Password window appears.
- Step 15** Enter your username and password in the respective fields and click **OK**.
- Step 16** Download and save the image file to your hard drive and then exit the Internet browser.
-

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>

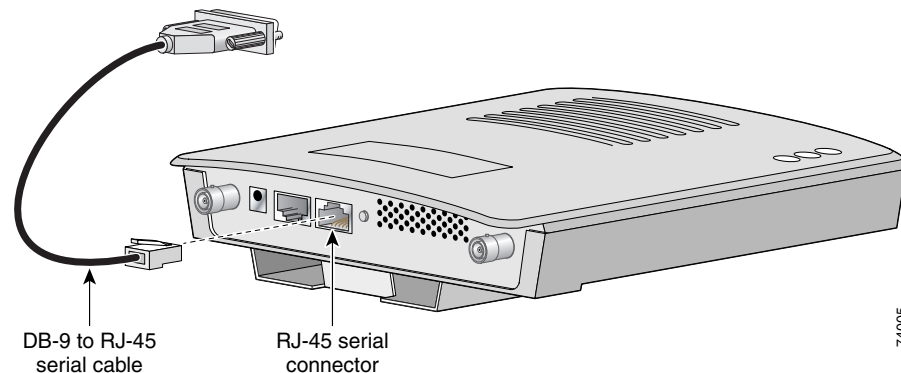
Follow the instructions on the website for installing and using the utility.

Connecting to the Access Point Locally

The console port is enabled during power up for diagnostic and monitoring purposes, which might be helpful if the access point is unable to associate to a controller. You can connect a PC to the console port using a DB-9 to RJ-45 serial cable.

- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer. [Figure 6-2](#) shows the serial port connection.

Figure 6-2 Connecting the Serial Cable



Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/go/marketplace> to order a serial cable.

- Step 2** Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.



Note When your monitoring and diagnostic activities are completed, you must remove the serial cable from the access point.

- Step 3** At the prompts, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

