



Troubleshooting Autonomous Access Points

This chapter provides troubleshooting procedures for basic problems with the 1100 series autonomous access point. 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

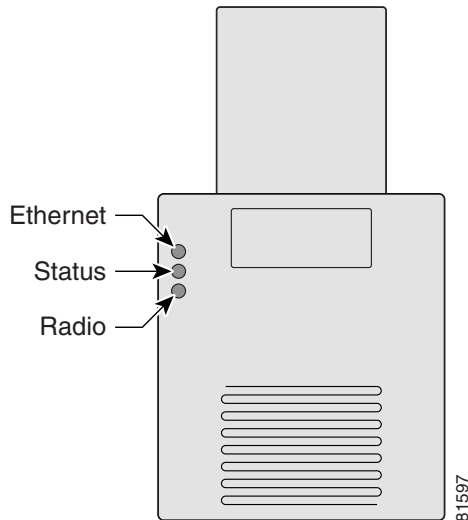
Sections in this chapter include:

- [Checking the Autonomous Access Point LEDs, page 5-2](#)
- [Checking Basic Settings, page 5-4](#)
- [Running the Carrier Busy Test, page 5-6](#)
- [Running the Ping or Link Test, page 5-7](#)
- [Resetting to the Default Configuration, page 5-7](#)
- [Reloading the Access Point Image, page 5-9](#)
- [Obtaining the Access Point Image File, page 5-11](#)
- [Obtaining the TFTP Server Software, page 5-11](#)

Checking the Autonomous Access Point LEDs

If your autonomous 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 5-1](#) shows the LEDs.

Figure 5-1 Access Points



The LEDs signals have the following meanings (for additional details refer to [Table 5-1](#)):

- 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 5-1 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 an 1100 series access point running Cisco IOS Release 12.3(2)JA or later with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes and does not become a mini-DHCP server. During this five-minute window, you can browse to the default IP address and configure a static address. If after five minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

When you connect an 1100 series access point running Cisco IOS Release 12.2(15)JA or earlier with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 and becomes a mini-DHCP server. In that capacity, the access point provides up to twenty IP addresses between 10.0.0.11 and 10.0.0.30 to the following devices:

- An Ethernet-capable PC connected to its Ethernet port
- Wireless client devices configured to use either no SSID or tsunami as the SSID, and with all security settings disabled

The mini-DHCP server feature is disabled automatically when you assign a static IP address to the access point.

**Caution**

When the access point is connected to your LAN, the access point mini-DHCP server provides an IP address to any DHCP requests it receives.

Default SSID and Radio Behavior

In Cisco IOS Release 12.3(2)JA2 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, 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 5-5](#) for instructions on enabling the radio interface.

Enabling the Radio Interfaces

To enable the radio interface, follow these instructions:

-
- Step 1** Open your web browser and enter the access point'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 > Radio0-802.11B** or **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**.
-

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. The access point default SSID is *tsunami*.

**Note**

In Cisco IOS Release 12.3(4)JA, 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 *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 the radio interface (802.11b). 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.

Follow these steps to activate the carrier busy test:

- Step 1** Open your web browser and enter the access point'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 displays.
- Step 4** Choose the radio interface experiencing problems by clicking **Radio0-802.11B**. The radio status page displays.
- Step 5** Click the **Carrier Busy Test** tab and the Carrier Busy Test page displays.
- 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 access point. 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.

Follow these steps to activate the ping or link test:

-
- Step 1** Open your web browser and enter the access point'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 displays.
 - Step 4** Click the MAC address of an associated access point, and the Statistics page for that device displays.
 - Step 5** Click the **Ping/Link Test** tab and the Ping/Link Test page displays.
 - Step 6** If you want to specify the number of packets to use in the test, follow these steps:
 - a. Enter a number of packets in the Number of Packets field
 - b. Enter a packet size (1 to 1400 bytes) in the Packet Size field.
 - c. Click **Start**. The test automatically stops when all packets are utilized.
 - Step 7** If you want to use a continuous test, follow these steps:
 - a. Enter a packet size in the Packet Size field.
 - b. Click **Start** to activate the test.
 - c. 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 5-4 and the [“Default SSID and Radio Behavior”](#) section on page 5-4.

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 web browser and enter the access point'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. The Summary Status page appears.
 - Step 3** Click **System Software** and the System Software screen appears.
 - Step 4** Click **System Configuration** and the System Configuration screen appears.
 - Step 5** Click **Default**.



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

- Step 6** 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 about 20 to 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.

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 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 same subnet as the access point.
 - Step 2** Place a copy of the desired access point image file (such as `c1100-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 **`c1100-k9w7-tar.default`**.
 - Step 4** Activate the TFTP server.
 - Step 5** Connect the PC to the access point 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 these instructions to use the HTTP interface:

-
- Step 1** Open your web browser and enter the access point'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** 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 c1100-k9w7-tar.123-8.JA.tar) on your PC.
 - Step 6** Click **Upload**.
 - Step 7** When a message appears that indicates the upgrade is complete, click **OK**.
- 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 these instructions to use a TFTP server:

-
- Step 1** Open your web browser and enter the access point'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. The Summary Status page appears.
 - Step 3** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
 - Step 4** Click the **TFTP Upgrade** tab.
 - Step 5** Enter the IP address for the TFTP server in the TFTP Server field.
 - Step 6** Enter the file name for the access point image file (such as c1100-k9w7-tar.123-7.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 7** Click **Upload**.

- Step 8** 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

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

- Step 1** Use your Internet browser to access the Cisco Software Center at the following URL:
<http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>
- Step 2** Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1100 Series**.
- Step 3** Click **Cisco Aironet 1100 Access Point**.
- Step 4** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
- Step 5** Click **IOS**.
- Step 6** Choose the Cisco IOS release desired, such as 12.3.11.JA.
- Step 7** Click **WIRELESS LAN** for an access point image file, such as c1100-k9w7-tar.123-11.JA.tar.
- Step 8** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
- Step 9** On the Security Information window, click **Yes** to display non-secure items.
- Step 10** On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.
- Step 11** If you checked No, enter the requested information and click **Submit**.
- Step 12** Click **Yes** to continue.
- Step 13** Click **DOWNLOAD**.
- Step 14** Read and accept the terms and conditions of the Software Download Rules.
- Step 15** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
- Step 16** Click **Save** to download your image file to your hard disk.
- Step 17** Select the desired download location on your hard disk and click **Save**.
-

Obtaining the 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.

