Read This First

This guide is designed to help you prepare your Cisco Aironet 1250 Series Access Point (hereafter referred to as the *access point*) for use on your wireless network. This section contains important information on what you you need to know so that you can successfully prepare and deploy your access point.

Login and Password

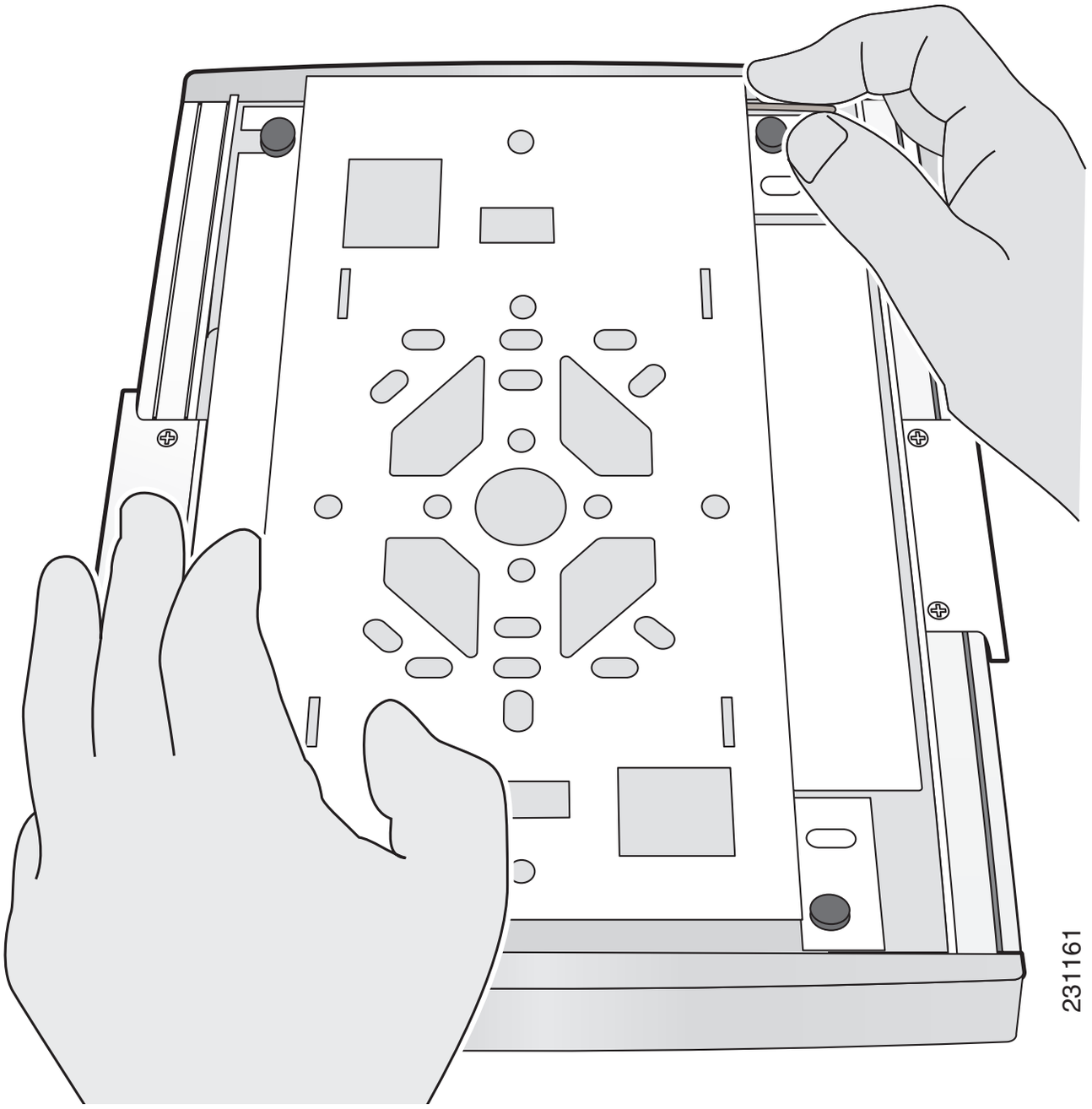
The default login and password used to access the access point GUI or CLI is *Cisco*. The password and login is case sensitive.

Removing the Mounting Plate

The access point ships with the mounting plate attached. You must remove the plate before you can connect the power and Ethernet cables and access the console port.

After unpacking the access point, follow these steps to remove the mounting plate.

Step 1 Grasp the access point with both hands as shown in the illustration below.



Step 2 With your right thumb or forefinger, pull the security hasp toward you to release it from the mounting plate.

Step 3 Maintain pressure on the security hasp, use your thumb or forefinger to push the mounting plate to the right, and slide it off the mounting plate pins.

Step 4 Remove the mounting plate from the access point.

Radio and IP Address Configuration

The access point ships with its radios disabled and no assigned IP address or service set identifier (SSID). You must enable the radios when you configure the access point for the first time. Also, the access point no longer is assigned a default IP address. It is configured to obtain an IP address using a DHCP server. If your network does not use a DHCP server, you must connect to the access point's console port and assign a static IP address. See the "Obtaining and Assigning an IP Address" section on page 18.

Bridging Feature Not Tested

The 1250 series access point has not been tested for bridging purposes, even though the commands for configuring the unit as a bridge are available.

Before You Start

Because the configuration process varies depending on how you intend to use your access point, detailed configuration instructions are not discussed in this guide.

Configuration instructions specific to your intended use are covered in the "Configuring the Access Point for the First Time" chapter of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.*

We also recommend that you have the following documents available:

- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*—provides detailed information for advanced configurations.
- *Cisco Aironet Command Reference for Cisco Aironet Access Points and Bridges*—lists all Cisco IOS commands with descriptions and syntax instructions.
- *Cisco Aironet 1250 Series Access Point Hardware Installation Guide*—provides mounting instructions, compliance information, and technical specifications.
- *Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.4(3g)JA* (or later)—provides system requirements, new feature descriptions, important notes, limitations, and last-minute updates.

These documents are also available on cisco.com. Follow this link:

http://www.cisco.com/en/US/products/ps6973/tsd_products_support_series_home.html

Make sure that you are using a computer connected to the same network as the access point, and obtain the following information from your network administrator:

- A host name for the access point.
- The case-sensitive SSID for your 802.11 radio network.
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use).
- The Media Access Control (MAC) address from the label on the bottom of the access point (such as 0016462584c), if you plan to use the Cisco IP Setup Utility to find an access point IP address.
- If you are not connected to a DHCP server, you can assign an IP address to the access point using the CLI. In this situation, obtain a unique IP address for your access point, a default gateway, and subnet mask from your network system administrator.

Safety Information

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991.

Proper installation of this radio according to the instructions found in this manual will result in user exposure that is substantially below the FCC recommended limits.

- Do not hold any component containing a radio so that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.

Warnings

Translated versions of the following safety warnings are provided in the *Safety Warnings for Cisco Aironet 1250 Series Access Points* document that ships with the access point.

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
20A Statement 1005

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.** Statement 332

Unpacking the Access Point

Package Contents

Each access point package contains the following items:

- Cisco Aironet 1250 series autonomous access point
- Mounting hardware kit
  - – One mounting plate, two 4 x 40 x 3/16 in screws, and a mounting plate latch (all attached to the access point)
  - – Two suspended ceiling T-rail clips, spacers (accommodates standard and recessed T-rails), and nuts
  - – Four 8 x 18 x 3/4 in pan head Phillips sheet metal screws
  - – Four #8 plastic wall anchors
  - – One 10 x 24 nut (for ground stud on the mounting plate)
  - – Two cable tie wraps
- Product quick start guide
- Product translated safety warning document
- Cisco product registration card

Follow these steps to unpack the access point:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in the Package Contents section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized Cisco sales representative.

Note The access point has two radio module slots: Slot 0 and Slot 1. Slot 0 can only be used with the 2.4-GHz radio module and slot 1 can only be used with the 5-GHz radio module. New radio configuration changes are associated with the specific module slot where the radio module is located. Once the default radio settings are changed, the radio modules should not be moved to a different slot. If you move the radio to a different slot, the radio configuration must be deleted and then remade.

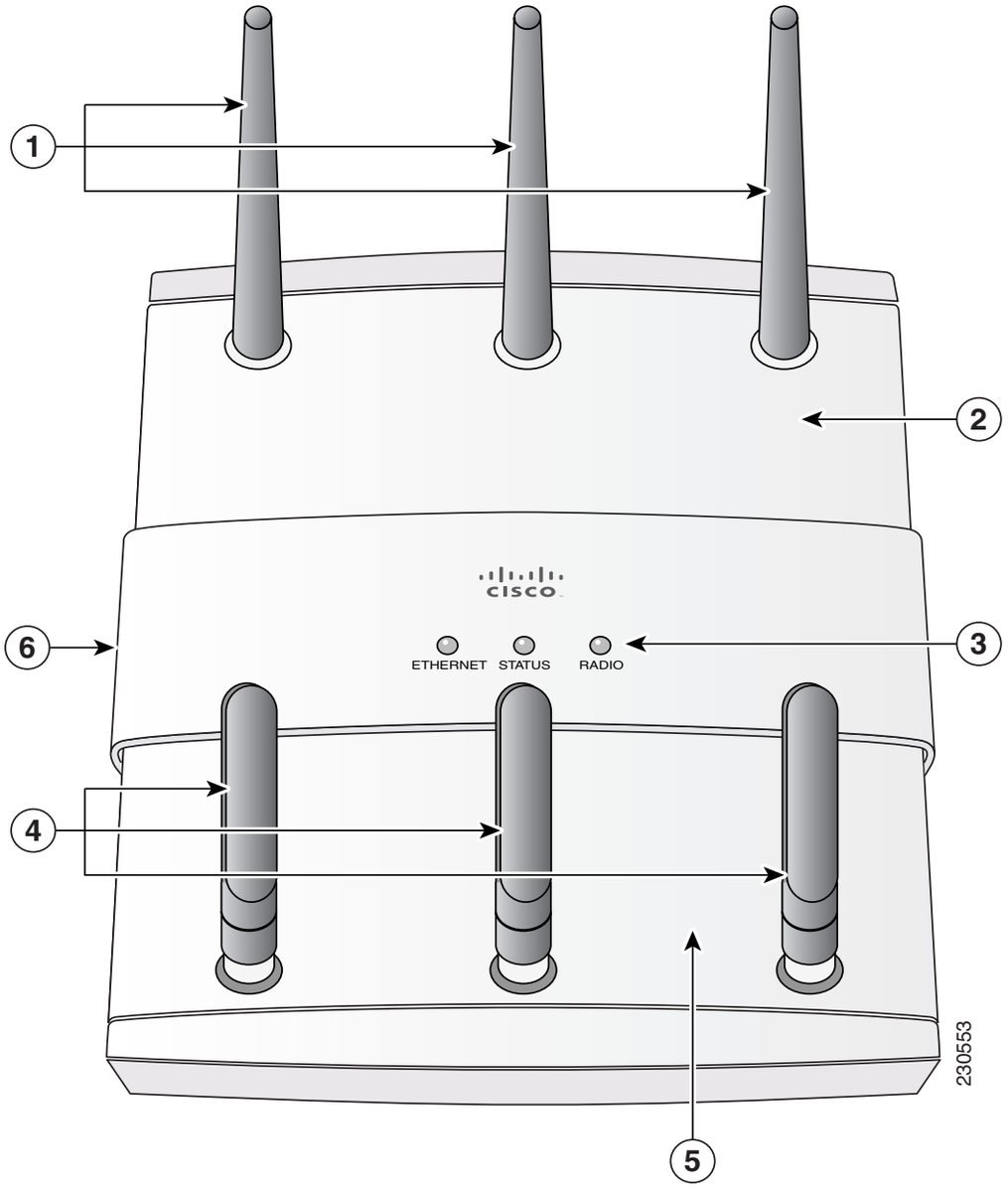
Before Beginning the Installation

Before you begin the installation, refer to the illustrations on the following pages to become familiar with the access point and the mounting hardware

Caution Be careful when handling the access point; the bottom plate might be hot.

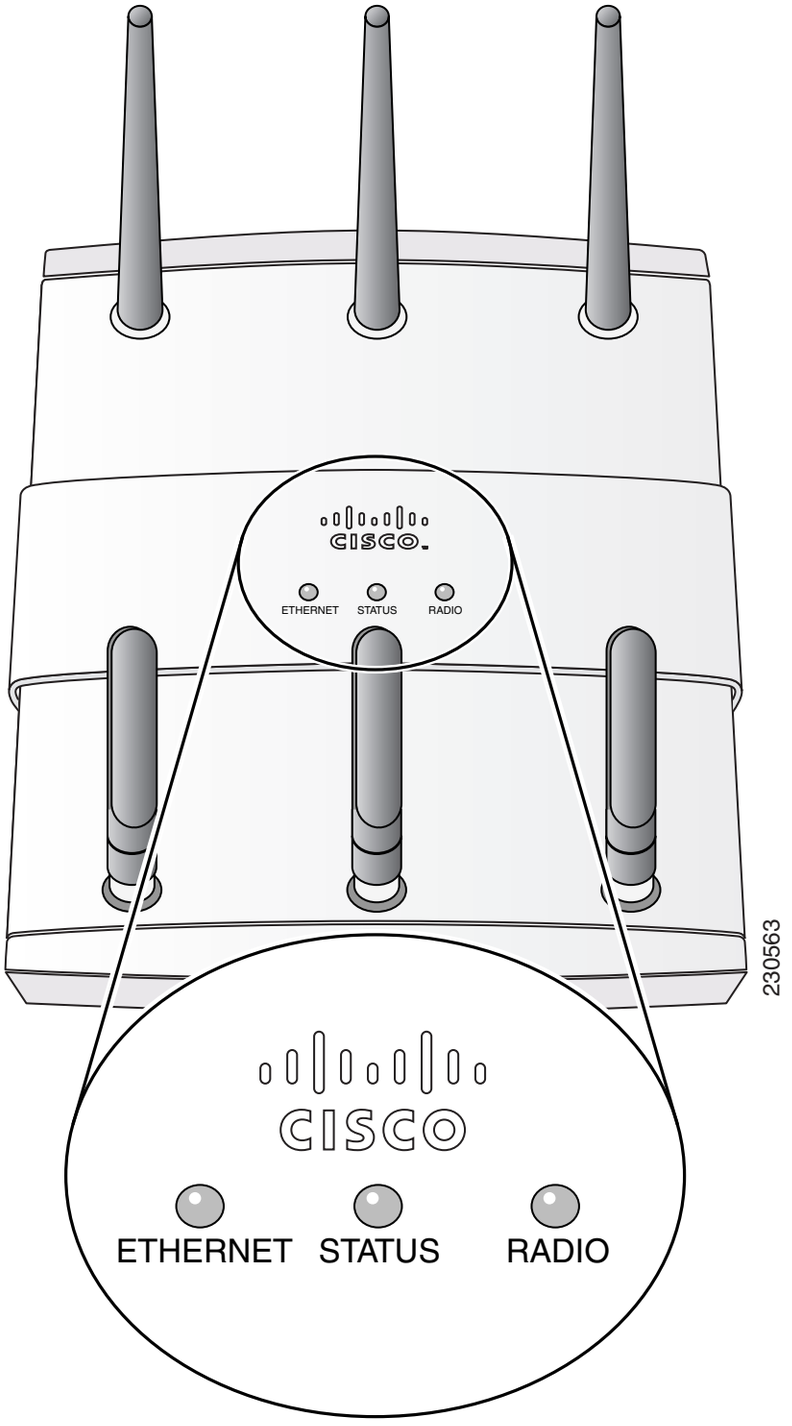
Caution The access point must be located indoors within the same building, including the associated LAN connections.

The following illustrations show the access point and identify its features.

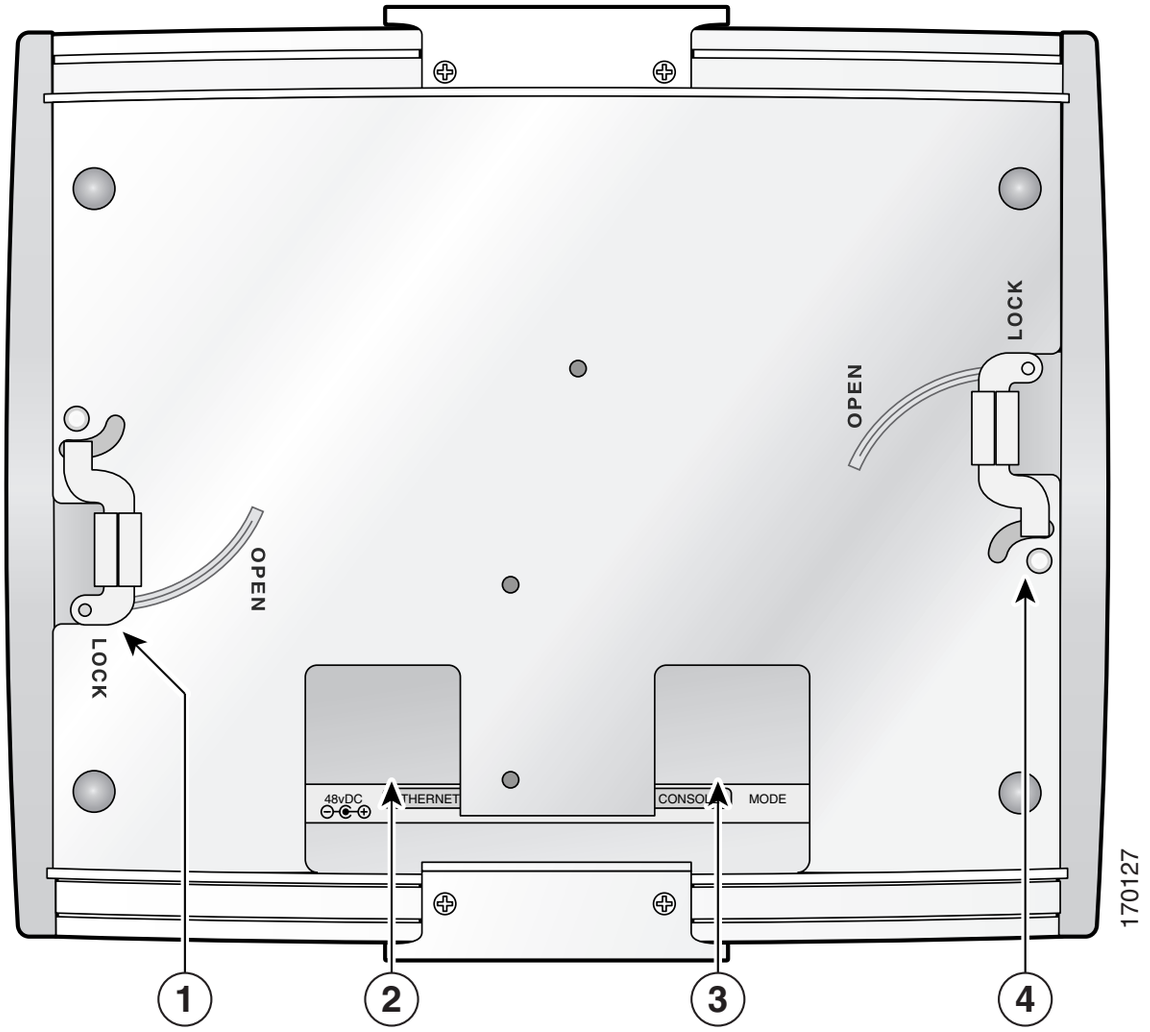


1	2.4-GHz radio antennas	**4**	5-GHz radio antennas
2	2.4-GHz radio module	**5**	5-GHz radio module
3	LEDs	**6**	Security lock slot (hidden)

This illustration shows LED placement.

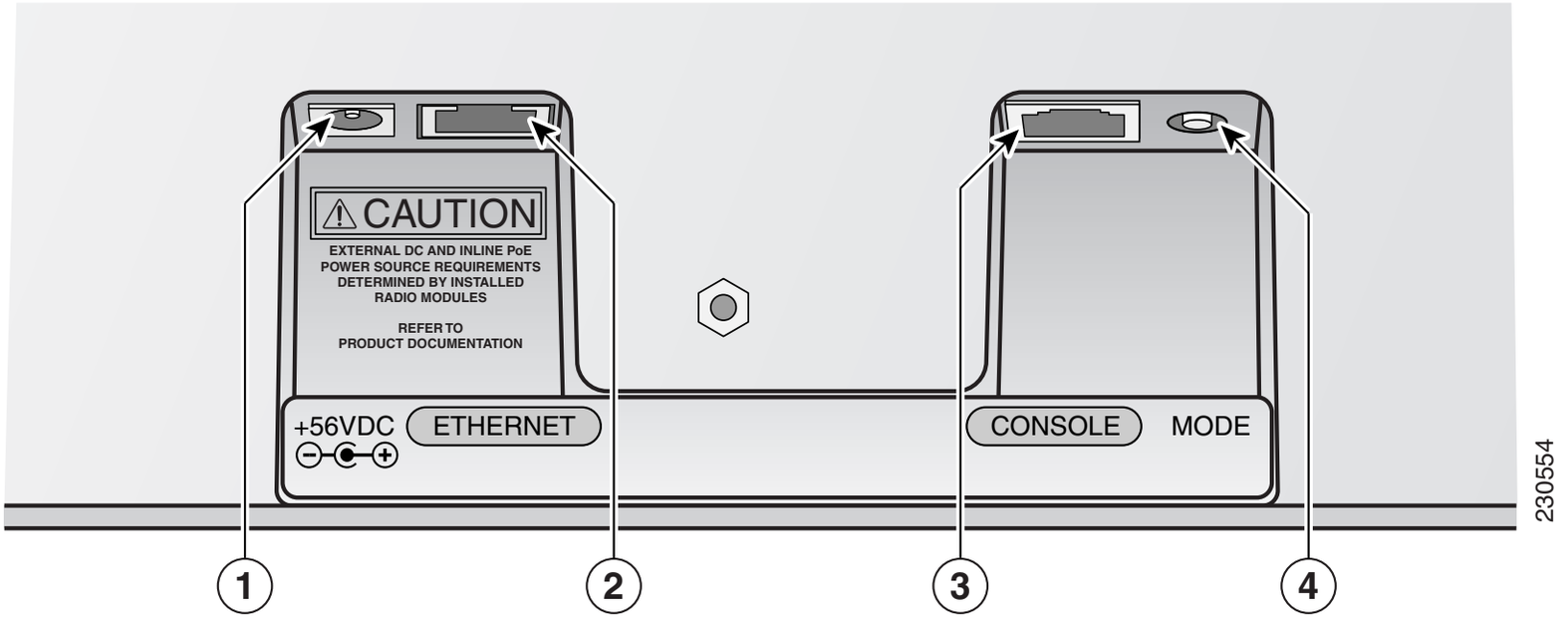


This illustration shows the bottom of the access point with the mounting plate removed.



1	Radio module latch	**3**	Console port cable bay
2	Ethernet cable bay	**4**	Radio module latch

This illustration shows the connections inside the Ethernet and console port bays.



1	DC power receptacle	**3**	Console port (RJ-45)
2	Ethernet port (RJ-45)	**4**	Mode button

Installation Summary

Installing the access point involves these operations:

- Mounting the Access Point
- Connecting Power
- Obtaining and Assigning an IP Address
- Configuring Power
- Configuring Security Settings

Mounting the Access Point

Detailed mounting instructions are in the *Cisco Aironet 1250 Series Access Point Hardware Configuration Guide.* This document is available on Cisco.com.

UL 2043 Compliance

The access point has adequate fire resistance and low smoke-producing characteristics. The device is suitable for operation in a building's environmental air space, such as above suspended ceilings. The access point complies with with Section 300-22(c) of the NEC and with Sections 2-128, 12-010(3), and 12-100 of the *Canadian Electrical Code,* Part 1, C22.1.

Note The 1250 series power injector, 1250 series DC power module, and antennas are not tested to UL 2043 and should not be placed in a building's environmental air space.

Connecting Power

The access point can be powered locally by the 1250 DC power module or an IEEE 802.3af compliant Power-over-Ethernet (PoE) power source. However, if the access point is powered by an 802.3af source, only one radio is supported because the two radio operation requires 18.5 watts. Two radio operation is supported only by the 1250 series power injector and an 802.at compliant PoE switch.

IEC60950 and IEEE 802.3af devices include:

- A 1250 DC power module connected to the access point's power connector
  - The 1250 DC power module should be plugged into a 100-240 VAC source
- The following devices provide PoE:
  - An IEEE 802.af compliant power source

- An IEEE 802.3af compliant Cisco inline power switch
- A Cisco 1250 series power injector (AIR-PWRINJ4)

Note Some older switches and patch panels might not provide enough power to operate the access point. At power-up, if the access point is unable to detect sufficient power, the access point deactivates both radios to prevent an over-current condition, and the Status LED displays a low power error (cycles blue, green, red, and off).

When power is applied to the access point, it begins a routine power-up sequence that you can monitor by observing the three LEDs on top of the access point. When all three LEDs turn green to indicate the starting of the IOS operating system, the Status LED blinks green signifying that IOS is operational. When in an operational status, the Ethernet LED is continuously green when no traffic is being passed and dark when traffic is being passed. The sequence takes about 1 minute to complete. Refer to the "Checking the Access Point LEDs" section on page 28 for LED descriptions.

When the sequence is complete, you can obtain the access point's IP address and perform an initial configuration. Refer to the "Obtaining and Assigning an IP Address" section on page 18 for instructions on assigning basic settings to the access point.

Note If your access point is connected to in-line power, do not connect the power module to the access point. Using two power sources on the access point might cause the access point to shut down to protect internal components and might cause the switch to shut down the port to which the access point is connected. If your access point shuts down, you must remove all power and reconnect only a single power source.

Obtaining and Assigning an IP Address

To browse to the access point Express Setup page, you must either obtain or assign the access point IP address using these methods:

- Assign a static IP address by connecting to its console port and opening the access point CLI.
- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address by using one of the following methods:
  - Connect to the access point console port and use a Cisco IOS command such as **show interface bvi1** to display the IP address.

- Provide your organization's network administrator with your access point MAC address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The MAC address is on a label attached to the bottom of the access point.
- Use the CLI and serial port to identify the assigned IP address.

Connecting to the Access Point Locally

If you need to configure the access point locally (without connecting it to a wired LAN), you can connect a PC to its console port by using a DB-9 to RJ-45 serial cable.

Follow these steps to open the CLI by connecting to the access point console port.

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 console port on the access point and to the COM port on the PC.

Step 2 Set up a terminal emulator on your PC 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.

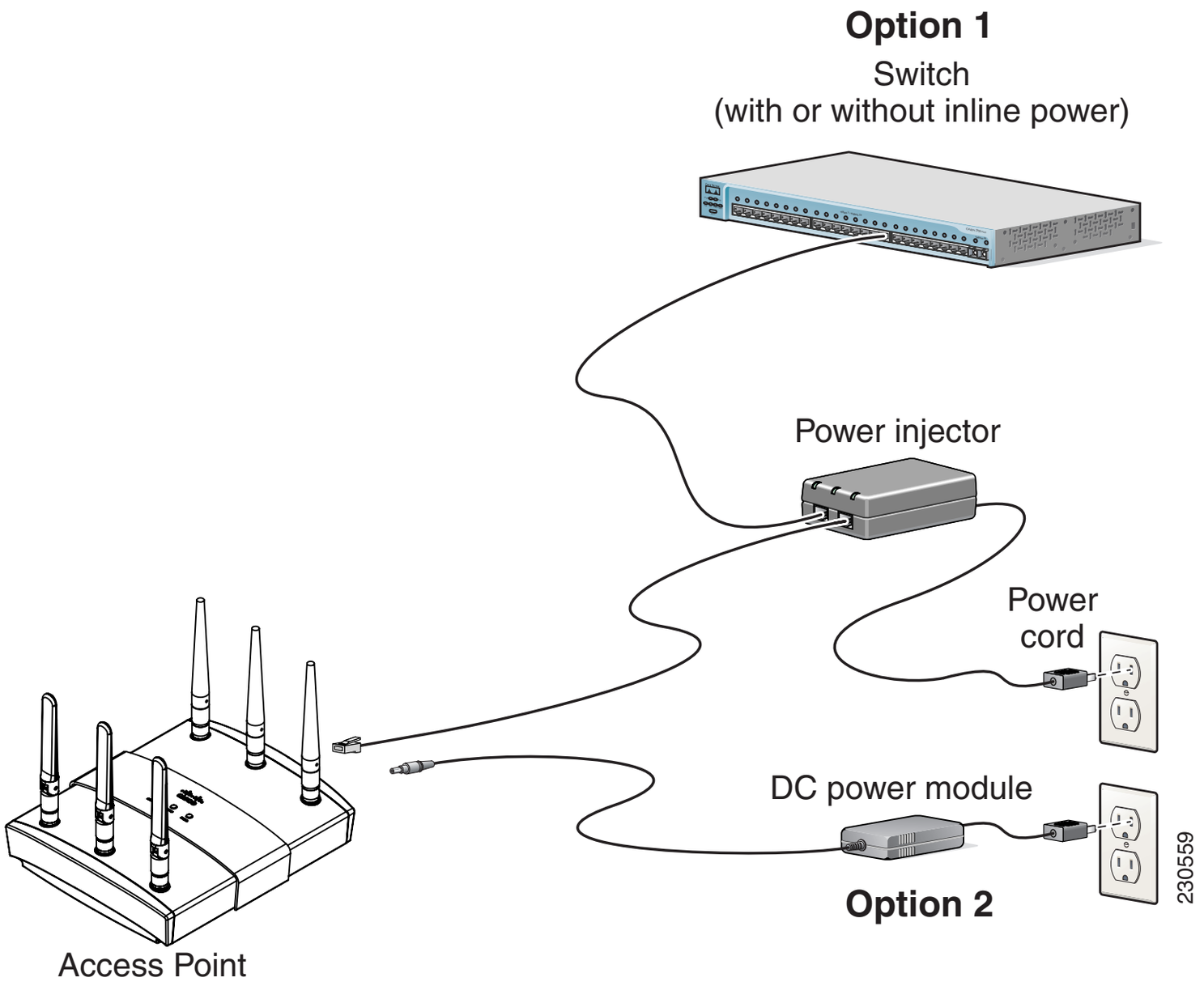
Assigning an IP Address Using the CLI

When you assign an IP address to the access point using the CLI, you must assign the address to the BVI. Beginning in a privileged EXEC mode, follow these steps to assign an IP address to the access point BVI using the console port:

	Command	Purpose
Step 1	**enable**	Enter privileged EXEC mode.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**Interface bvi1**	Enters interface configuration mode for the BVI.
Step 4	**ip address** *address mask*	Assigns an IP address and subnet mask address to the BVI.
Step 5	**end**	Return to privileged EXEC mode.

Configuring Power

The access point receives power through the Ethernet cable or an external power module. The following illustration shows the power options for the access point.



Warning **This product must be connected to a Power over Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source. Statement 353**

The access point power options:

- Option 1—Switches with sufficient inline power (single radio only):
  - An inline power capable switch, such as the Cisco Catalyst 3550 PWR XL, 3560-48PS, 4500 with 802.3af PoE module, or the 6500 with 802.3af PoE module
  - Other inline power switches supporting the IEEE 802.3af inline power standard
- Option 2—Switches without sufficient inline power can use the power injector (two radio operation):
  - – 1250 series power injector (AIR-PWRINJ4)
- Option 3—Local power using the 1250 series DC power module (AIR-PWRSPLY1)
- Option 4—An 802.at compliant PoE switch

Note Some older switches and patch panels might not provide enough power to operate the access point. At power-up, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point Status LED turns amber and an error log entry is created

Connecting to an Ethernet Network with an Inline Power Source

Caution Be careful when handling the access point; the bottom plate might be hot.

Note If your access point is connected to in-line power, do not connect the power module to the access point. Using two power sources on the access point might cause the access point to shut down to protect internal components and might cause the switch to shut down the port to which the access point is connected. If your access point shuts down, you must remove all power and reconnect only a single power source.

Follow these steps to connect the access point to the Ethernet LAN when you have an inline power source:

Step 1 Connect a Category 5E (or higher) Ethernet cable to the RJ-45 Ethernet connector labeled Ethernet on the access point.

Step 2 Step 2 Connect the other end of the Ethernet cable to one of the following:

- A switch with inline power.
- The Ethernet connector on the 1250 series power injector labeled *To AP*.

Step 3 When using the power injector, connect a Category 5E (or higher) Ethernet cable from your your inline power switch to the power injector connector labeled *To Switch*.

Step 4 When using the power injector, connect an AC power cord to the power injector and the AC wall socket.

Connecting to an Ethernet Network with Local Power

Note If your access point is connected to in-line power, do not connect the DC power module to the access point. Using two power sources on the access point might cause the access point to shut down to protect internal components and might cause the switch to shut down the port to which the access point is connected. If your access point shuts down, you must remove all power and reconnect only a single power source.

Follow these steps to connect the access point to an Ethernet LAN when you are using a local power source:

Step 1	Connect a Category 5E (or higher) Ethernet cable to the RJ-45 Ethernet connector labeled Ethernet on the access point.
Step 2	Connect the 1250 series DC power module's output connector to the access point's DC-IN power connector.
Step 3	Plug the other end of the Ethernet cable into an unpowered Ethernet port on your LAN network.
Step 4	Plug the 1250 series DC power module's AC power cord into an approved 100- to 240-VAC outlet.

Configuring the Access Point

How you configure your access point depends on how you intend to use it in your wireless network. This guide provides a brief synopsis of the configuration process. For detailed information, refer to the "Configuring the Access Point for the First Time" chapter of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for the Cisco IOS release you are using.

The following basic settings must be configured on your access point.

- Host Name
- Configuration Server Protocol
- IP Address
- IP Subnet Mask
- Default Gateway
- SNMP Community

The following radio settings must be applied separately to each radio.

- Role in Radio Network
- Optimize Radio Network For
- Aironet Extensions

Configuring Security Settings

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your work site.

Basic security settings are explained in the “Configuring the Access Point for the First Time” chapter of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for the Cisco IOS release you are using.

The following security settings are available on the Express Security Setup page.

- No Security
- Static WEP Key
- EAP Authentication
- WPA and WPA2

Advanced security settings are described in appropriate chapters of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for the Cisco IOS release you are using.

Note The 802.11n radio only supports no encryption, WPA2 Enterprise, and WPA-2 Personal. WPA-2 Enterprise and WPA-2 Personal requires AES encryption.

In Case of Difficulty

If you followed the instructions in previous sections of this guide, you should have had no trouble getting your access point installed and running. If you do experience difficulty, the following sections provide basic troubleshooting information.

Before contacting Cisco, look for a solution to your problem in this guide or the "Troubleshooting" chapter of the *Cisco Aironet 1250 Series Access Point Hardware Installation Guide.*

Follow this link to access the Technical Assistance Center (TAC) on Cisco.com:

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

Checking the Access Point LEDs

If your access point is not working properly, check the Status, Ethernet, and Radio LEDs on the top panel. You can use the LED colors to assess the unit status.

The LED meanings are in the following table.

Note Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect.

Ethernet LED	Radio LED	Status LED	Meaning
–	–	Green	Normal operation; no wireless clients associated.
–	–	Blue	Normal operation; at least one wireless client associated.
Green	–	–	Ethernet link is operational.
–	Blinking green	–	Transmitting or receiving radio packets
–	–	Blinking blue	Software upgrade in progress.
Blinking green	Blinking green	Blinking green	Access location command.
–	–	Blinking red	Ethernet link not operational.
Red	–	Red	Ethernet failure

Ethernet LED	Radio LED	Status LED	Meaning
Amber	–	Blinking blue	Configuration recovery in progress (Mode button pressed for 2–3 seconds).
Blinking green	Red	Blinking green	Image recovery in progress (Mode button pressed for 20–30 seconds).
Blinking amber	–	–	Ethernet transmit or receive errors.
–	Blinking amber	–	Maximum retries or buffer full failure on radio.
Red	Red	–	Software failure.
–	–	Cycling blue, green, red, off	General warning; insufficient inline power.

For more details on these LED status codes, see the “Troubleshooting” chapter of the *Cisco Aironet 1250 Series Access Point Hardware Installation Guide*.

Resetting to Default Configuration

Note These steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

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 your web browser to reset the configuration.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults:

Step 1 If the access point is mounted using its mounting plate, remove it to gain access to the MODE button.

Step 2 Disconnect power from the access point (the power jack for external power or the Ethernet cable for in-line power).

Step 3 Press and hold the MODE button while you reconnect power to the access point.

Step 4 Continue holding the MODE button until the Ethernet LED turns amber (approximately 2 to 3 seconds), then release the button.

Step 5 After the access point reboots, you must reconfigure it using the web browser interface, the Telnet interface, or connecting to the access point console port.

Using the Web Browser Interface

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

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

Step 2 Enter the access point IP address in the browser address line, and press **Enter**. An Enter Network Password window appears.

Step 3 Enter your username in the User Name field.

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

Step 5 Click **System Software**. The System Software page appears.

Step 6 Click **System Configuration**. The System Configuration page appears.

Step 7 Click the **Reset to Defaults** or **Reset to Defaults (Except IP)** button (depending on your configuration).

Step 8 After the access point reboots, reconfigure it.

Compliance Information

This equipment has been tested and found to comply with the European Telecommunications Standard ETS 300.328. This standard covers Wideband Data Transmission Systems referred to in CEPT recommendation T/R 10.01.

This type-accepted equipment is designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed in accordance with the instruction manual, may cause harmful interference to radio communications.

The Declarations of Compliance for this product relevant to the European Union and other countries following EU Directive 1999/5/EC (R&TTE Directive) can be found in the *Cisco Aironet 1250 Series Access Point Hardware Installation Guide.* This guide is available on Cisco.com.

Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranties and license agreements applicable to Cisco software, is available on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/en/US/products/prod_warranties_listing.html

   The Warranties and License Agreements page appears.

2. To read the *Cisco Information Packet*, follow these steps:

   a. Click the **Information Packet Number** field, and make sure that the part number 78-5235-03B0 is highlighted.

   b. Select the language in which you would like to read the document.

   c. Click **Go**.

      The Cisco Limited Warranty and Software License page from the Information Packet appears.

d. Read the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website: http://www.adobe.com

3. To read translated and localized warranty information about your product, follow these steps:

   a. Enter this part number in the Warranty Document Number field:

      78-5236-01C0

   b. Select the language in which you would like to read the document.

   c. Click **Go**.

      The Cisco warranty page appears.

   d. Review the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

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

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	