Installing the Access Point

This chapter describes the setup of the access point and includes the following sections:

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the access point.

FCC Safety Compliance Statement

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.

General Safety Guidelines

- Do not touch or move antenna(s) while the unit is transmitting or receiving.
- 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 local codes, the national codes, and the safety directors of such environments.

Warnings

Translated versions of all safety warnings are available in the safety warning document that shipped with your access point or on Cisco.com. To browse to the document on Cisco.com, refer to Appendix A, "Translated Safety Warnings" for instructions.

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

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

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: 20 A..** Statement 1005

Unpacking the Access Point

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.

Package Contents

Each access point package contains the following items:

- Access point with power module
- Wall or ceiling mounting bracket
- Security hasp adapter
- Cubical partition mounting bracket assembly
- Horizontal surface mounting holster
- Mounting hardware kit
- Product quick start quide
- Product safety warnings document
- Cisco product registration and Cisco documentation feedback cards

Basic Installation Guidelines

Because the access point is a radio device, it is susceptible to interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

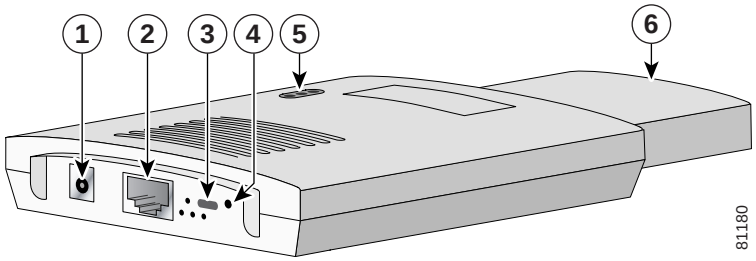
- Ensure a site survey has been performed to determine the optimum placement of access points.
- For lightweight access points, check the latest release notes to ensure that your controller software version supports the access points to be installed. You can find the controller release notes by selecting your controller under **Wireless LAN Controllers** at this URL:

  http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html
- Ensure that access points are not mounted closer than 20 cm (7.9 in) from the body of all persons.
- Do not mount the access point within 3 feet of metal obstructions.
- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.
- Do not mount the access point outside of buildings.
- Do not mount the access points on building perimeter walls unless outside coverage is desired.

Access Point Layout and Connectors

Figure 2-1 shows the access point layout and connectors.

Figure 2-1 Access Point Layout and Connectors



1	48-VDC power port	**4**	Mode button
2	Ethernet port (RJ-45)	**5**	Status LEDs
3	Cable lock slot	**6**	Antenna

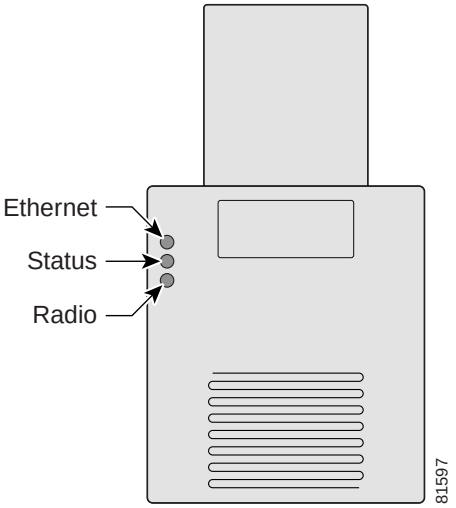
LEDs

The three LEDs on the top of the access point report Ethernet activity, association status, and radio activity.

- The Ethernet LED signals Ethernet traffic on the wired LAN.
- The status LED signals operational status.
- The radio LED signals wireless traffic over the radio interface.

Figure 2-2 shows the three status LEDs.

Figure 2-2 Access Point LEDs



Controller Discovery Process for Lightweight Access Points

The lightweight access point supports these controller discovery processes:

- DHCP server discovery—Uses DHCP Option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option. For additional information, refer to the "Configuring DHCP Option 43 for Lightweight Access Points" section on page F-1.
- DNS server discovery—The access point uses the name *CISCO-LWAPP-CONTROLLER.<local domain>* to discover the controller IP addresses from a DNS server. Where *<local domain>* is the access point domain name.
- Locally stored controller IP addresses—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point non-volatile memory. The process of storing controller IP addresses in access points for later deployment is called priming the access point. For additional information, refer to the "Priming Lightweight Access Points Prior to Deployment" section on page E-1.

For lightweight access points, Cisco recommends that you configure a DHCP server with Option 43 to provide the controller IP addresses to your access points. Cisco switches provide a DHCP server option that is typically used for this purpose.

Deploying the Access Points on the Wireless Network

Prior to beginning the actual access point deployment, perform these tasks:

- Ensure that a site survey has been preformed.
- Ensure that your network infrastructure devices are operational and properly configured.
- For lightweight access points, perform these tasks:
  - Ensure that your controllers are connected to switch trunk ports.
  - Ensure that your switch is configured with untagged access ports for connecting your access points.
  - Ensure that a DHCP server with Option 43 configured is reachable by your access points.

To deploy your access points, follow these steps:

Step 1 Obtain the access point location map created during your building site survey.

Step 2 Review the access point locations and identify the specific mounting methods required for each access point location.

Step 3 For each access point perform these steps:

a. For lightweight access points, record the access point MAC address on the access point location map. When you have completed the access point deployment, return the access point MAC addresses and the access point locations on the access point location maps or floor plans to your network planner or manager. The network operators can use the MAC address and location information to create maps for precise wireless system management.

b. Mount the access point at the indicated destination using the specified mounting method. For specific instructions, see these sections:

- Horizontal or vertical surface, such as a ceiling or wall (refer to the Mounting on a Horizontal or Vertical Surface, page 3-3).
- Below a suspended ceiling (refer to the "Mounting on a Suspended Ceiling" section on page 3-4).
- Above a suspended ceiling (refer to the "Mounting Above a Suspended Ceiling" section on page 3-6).
- On a cubicle wall (refer to the "Mounting on a Cubical Wall Partition" section on page 3-8).
- On a desktop (see the "Using the Desktop Holster" section on page 3-9).

c. Optionally secure the access point using a padlock or security cable (refer to the "Using the Security Hasp Adapter" section on page 3-7 and the "Using the Cable Lock Feature" section on page 3-11).

d. Connect the access point cables (Ethernet, optional power, optional antennas). For instructions see the "Connecting the Ethernet and Power Cables" section on page 2-7.

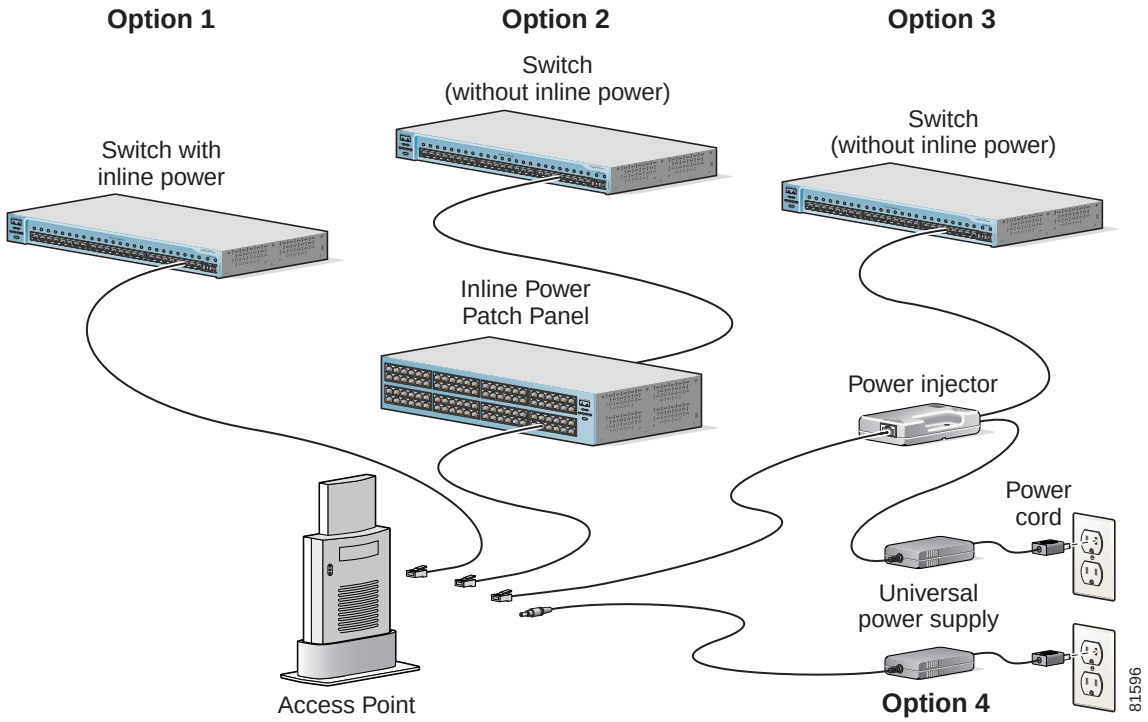
e. On power up, verify that the access point is operating normally by checking the LEDs. For additional information, refer to the "Checking the Autonomous Access Point LEDs" section on page 5-2 or the "Checking the Lightweight Access Point LEDs" section on page 6-3.

Step 4 For lightweight access points, after your access points are deployed, ensure that your controller is not configured as a master controller. A master controller should only be used for configuring access points and not in a working network.

Connecting the Ethernet and Power Cables

The access point receives power through the Ethernet cable or an external power module. Figure 2-3 shows the power options for the access point.

Figure 2-3 Access Point Power Options



The access point power options are listed below:

- A switch with inline power, such as a Cisco Catalyst 3500XL, 3550, 4000, or 6500 switch
- An inline power patch panel, such as a Cisco Catalyst Inline Power Patch Panel
- A power injector (Cisco AIR-PWRINJ3= or Cisco AIR-PWRINJ-FIB=)
- A power module (Universal power supply)

Note If you use in-line power from a switch or patch panel, do not connect the power module to the access point. Using two power sources on the access point might cause the switch or patch panel to shut down the port to which the access point is connected.

Connecting to an Ethernet Network with an Inline Power Source

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

Step 1 Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point.

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

- A switch with inline power, such as a Cisco Catalyst 3500XL, 3550, 4000, or 6500 switch.
- An inline power switch panel, such as a Cisco Catalyst Inline Power Patch Panel.
- The end of a Cisco Aironet power injector labeled *To AP/Bridge*. Connect the other end labeled *To Network* to the 10/100 Ethernet LAN.

Caution The Cisco Aironet Power Injector (Cisco AIR-PWRINJ3= or Cisco AIR-PWRINJ-FIB=) is designed for use with 1100 or 1200 series access points. Using the power injector with other Ethernet-ready devices can damage the equipment.

Caution Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.

Note If you use a power injector to power the access point, you must use the power supply included with your access point and the Cisco Aironet Power Injector specified for the access point.

Connecting to an Ethernet Network with Local Power

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

Step 1 Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point.

Step 2 Plug the other end of the Ethernet cable into an unpowered Ethernet port on your network.

Step 3 Connect the power module's output connector to the 48-VDC power port labeled *48VDC* on the access point.

Step 4 Plug the other end of the power module into an approved 100- to 240-VAC outlet.

Powering Up the Access Point

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. After you observe all three LEDs turning green to indicate the starting of the Cisco IOS operating system, the Status LED blinks green signifying that Cisco IOS is operational. Refer to the "Checking the Autonomous Access Point LEDs" section on page 5-2 or the "Checking the Lightweight Access Point LEDs" section on page 6-3 for LED descriptions.