

Cisco Aironet 5-GHz 8-dBi Omnidirectional Antenna (AIR-ANT5180V-N)

The Cisco Aironet 5-GHz 8-dBi Omnidirectional Antenna is designed for outdoor use with Cisco Aironet Outdoor Access Points with radios operating in the 5-GHz frequency band. This antenna has 8-dBi gain in the 5-GHz frequency band.

For detailed information on this antenna, refer to the document *Cisco Aironet 8-dBi Omnidirectional Antenna (AIR-ANT5180V-N)*. Follow all safety precautions when installing the antennas, for information on safety, refer to [“Safety Precautions when Installing Antennas”](#) section on page A-4.

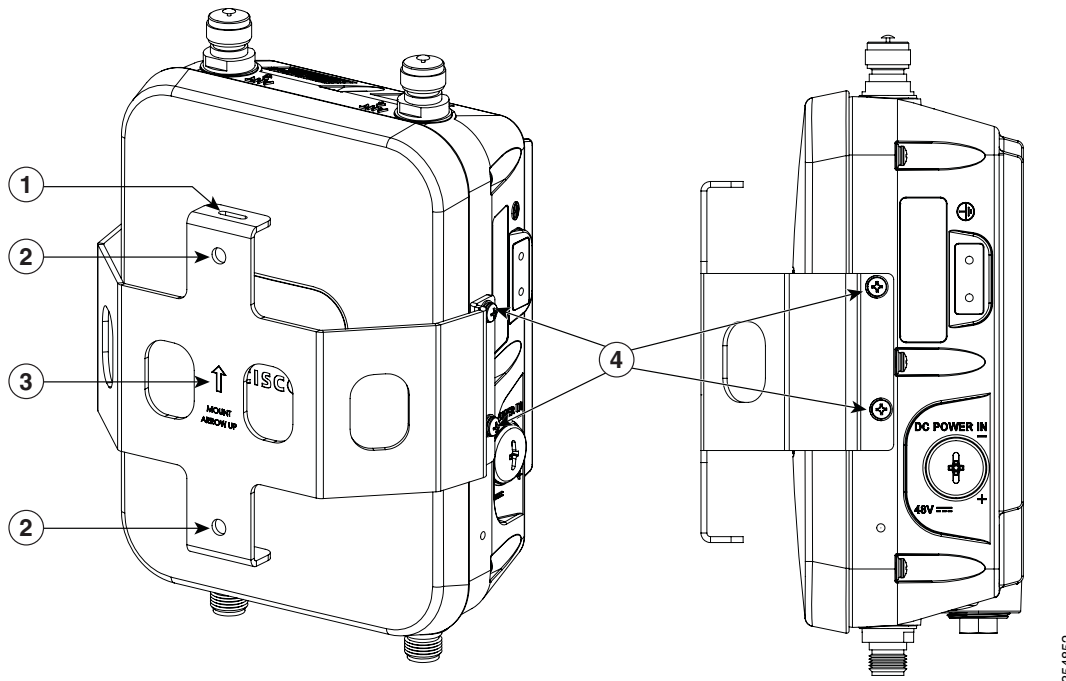
Figure 2-24 Cisco Aironet 5-GHz 8-dBi Omnidirectional Antenna - Installed Only on Model AIR-AP1562E-x-K9



Using a Mounting Bracket for External Directional Antennas

You can use the AIR-ACCAMK-2= bracket for mounting a directional antenna directly on the access point. See [Figure 2-25](#).

Figure 2-25 Directional Antenna Mounting Bracket AIR-ACCAMK-2= Views



1	Slots to be used for managing the antenna cables with cable ties.	3	Note the direction of the arrow. Ensure that the bracket and AP are mounted with the arrow pointing upwards.
2	Mounting holes for the directional antenna.	4	Two of four #8-32 screws and the mounting points used to mount the bracket to the AP.

Installing a Lightning Arrestor

Overvoltage transients can be created through lightning static discharges, switch processes, direct contact with power lines, or through earth currents. The Cisco Aironet AIR-ACC245LA-N Lightning Arrestor limits the amplitude and duration of disturbing interference voltages and improves the over voltage resistance of in-line equipment, systems, and components. A lightning arrestor installed according to these mounting instructions balances the voltage potential, thus preventing inductive interference to parallel signal lines within the protected system.

Installation Considerations

Cisco recommends that you bulkhead mount the lightning arrestor so it can be installed as a wall-feed through on the wall of the protected space.

The importance of obtaining a good ground and bonding connection cannot be overstressed. Consider these points when grounding the lightning arrestor:

- Connect the lightning arrestor components directly to the grounding point.
- The contact points of the ground connection must be clean and free of dust and moisture.
- Tighten threaded contacts to the torque specified by the manufacturer.

Installation Notes

This lightning arrestor is designed to be installed between the antenna cable that is attached to an outdoor antenna and the Cisco Aironet wireless device. You can install the lightning arrestor either indoors or outdoors. It can be connected directly to a wireless device having an external N connector. It can also be mounted inline or as a feed-through. Feed-through installations require 5/8 in. (16 mm) hole to accommodate the lightning arrestor.



Note

This lightning arrestor is part of a lightning arrestor kit. The kit contains a lightning arrestor and a grounding lug.



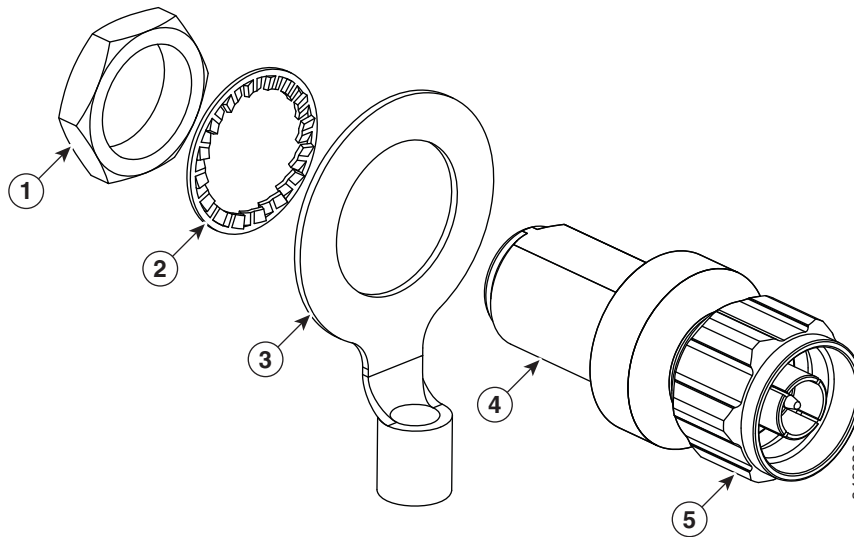
Note

When you install the lightning arrestor, follow the regulations or best practices applicable to lightning protection installation in your local area.

Installing the Lightning Arrestor Outdoors

If you install the lightning arrestor outdoors, use the supplied ground lug and a heavy wire (#6 solid copper) to connect it to a good earth ground, such as a ground rod. The connection should be as short as possible.

Figure 2-26 Lightning Arrestor Details



1	Nut	4	Unprotected side (to antenna)
2	Lockwasher	5	Protected side (to wireless device)
3	Ground lug		

Cable for the Lightning Arrestor

Coaxial cable loses efficiency as the frequency increases, resulting in signal loss. The cable should be kept as short as possible because cable length also determines the amount of signal loss (the longer the run, the greater the loss).

Cisco recommends a high-quality, low-loss cable for use with the lightning arrestor.

Grounding the Access Point

The access point must be grounded before connecting power.

In all outdoor installations and when powering the access point with AC power, you must follow these instructions to properly ground the case:

- Step 1** If using insulated 6-AWG copper ground wire, strip the insulation as required for the grounding lug.
- Step 2** Use the appropriate crimping tool to crimp the bare 6-AWG copper ground wire to the supplied grounding lug.

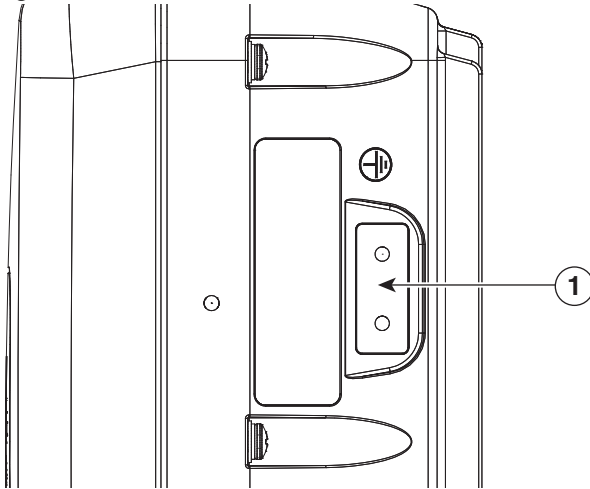


Note The grounding lug and hardware used must comply with local and national electrical codes.

- Step 3** Open the anti-corrosion sealant (supplied), and apply a liberal amount over the metal surface, called the Ground Pad, where the ground strap screw holes are located (see [Figure 2-27](#)).
- Step 4** Connect the grounding lug to the access point grounding screw holes (see [Figure 2-27](#)) using the supplied two Phillips head screws (M4 x10 mm) with lock washers. Tighten the grounding screw to 22 to 24 lb-in (2.49 to 2.71 Nm).

- Step 5** If necessary, strip the other end of the ground wire and connect it to a reliable earth ground, such as a grounding rod or an appropriate grounding point on a metal streetlight pole that is grounded.

Figure 2-27 Position of the Ground Pad on the Right Side of the AP



- | | |
|----------|---|
| 1 | Ground pad, where the ground strap screw holes are located. |
|----------|---|

Powering the Access Point

The 1560 access point supports these power sources:

- DC power – 42- 57 VDC
- Power-over-Ethernet (PoE)

The 1560 access point can be powered via the PoE input from an in-line power injector or a suitably powered switch port. Depending on the configuration and regulatory domain, the required power for full operation is UPoE.

For the 1562I, UPoE powered switch port or a power injector is required for full operation of the 3x3 MIMO on the 2.4 GHz radio in the regulatory domains that allow for high 2.4 GHz transmit power (Regulatory domains -A, -D, -F, -K, -N, -Q, -T, -Z). If the 1562I is powered by a PoE+ (802.3at power) switch port then the access point will automatically disable one of the 2.4 GHz transmitters and the radio will operate in 2x2 MIMO mode.

Table 2-9 AP 1560 Power Matrix

Model	Configuration	Regulatory Domain	Switch Power	AIR-PWRINJ-60RGD1 AIR-PWRINJ-60RGD2	AIR-PWRINJ6 ¹	AD/DC Power Adapter AIR-PWRADPT-RGD1
1562I	3x3:3 (2.4 GHz)	A, B, D, I, K, N, Q, T, Z	UPOE	Yes	No	Yes
	3x3:3 (5 GHz)					
	3x3:3 (2.4 GHz)	C, E, F, G, H, L, M, R, S	UPOE		(Future Support)	
	3x3:3 (5 GHz)					
	2x2:2 (2.4 GHz)	A, B, C, D, E, F, G, H, I, K, L, M, N, Q, R, S, T, Z	802.3at PoE+		Yes	
2x2:2 (5 GHz)						
1562D	2x2:2 (2.4 GHz)	A, B, C, D, E, F, G, H, I, K, L, M, N, Q, R, S, T, Z	802.3at PoE+	Yes	Yes	Yes
	2x2:2 (5 GHz)					
1562E	2x2:2 (2.4 GHz)	N, Q, R, S, T, Z				
	2x2:2 (5 GHz)					

1. The AIR-PWRINJ6 power injector can only be used in an indoor environment. Therefore the cable from the injector must travel from the protected location to the outside mounted access point.

Connecting a Power Injector

The 1560 Series access point supports the following power injectors:

- AIR-PWRINJ-60RGD1
- AIR-PWRINJ-60RGD2

The power injector provides 56 VDC to the access point over the Ethernet cable and supports a total end-to-end Ethernet cable length of 100 m (328 ft) from the switch to the access point.

When your access point is powered by an optional power injector, follow these steps to complete the installation:

- Step 1** Before applying PoE to the access point, ensure that the access point is grounded (see the [“Grounding the Access Point”](#) section on page 2-42).
- Step 2** See the [“Typical Access Point Installation Components”](#) section on page 2-5, to identify the components needed for the installation.
- Step 3** Connect a CAT5e or better Ethernet cable from your wired LAN network to the power injector.

**Warning**

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord. Statement 1023

**Note**

The installer is responsible for ensuring that powering the access point from this type of power injector is allowed by local and/or national safety and telecommunications equipment standards.

**Tip**

To forward bridge traffic, add a switch between the power injector and controller. Refer to the *Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 7.0* for more information.

- Step 4** Ensure that the antennas are connected and that a ground is attached to the access point before you apply power to the access point.
- Step 5** Connect a shielded outdoor-rated Ethernet (CAT5e or better) cable between the power injector and the PoE-in connector of the access point.
- Step 6** Connect the Ethernet cable to the access point PoE-In port. See [“Connecting an Ethernet Cable to the Access Point”](#) section on page 2-53.

Connecting a DC Power Cable to the Access Point

When powering the access point with DC power, you must ensure that DC power can be conveniently removed from the unit. The power should not be removed by disconnecting the DC power connector on the unit.

**Warning**

Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards. Statement 1033

To connect a DC power cable, you need to supply these tools and material:

- Shielded outdoor-rated DC power cable (minimum 18 AWG) with outside cable diameter of 0.20 to 0.35 inch (0.51 to 0.89 cm).
- Adjustable or open-end wrench
- Small flat screw driver
- Two-pin DC power connector (Cisco supplied)

To connect the DC power cable to the access point, follow these steps:

Step 1 Before connecting DC power to the access point, ensure that the ground is connected to the access point. See the “[Grounding the Access Point](#)” section on page 2-42.

Step 2 Turn off all power sources to the access point, including the DC power source.

**Warning**

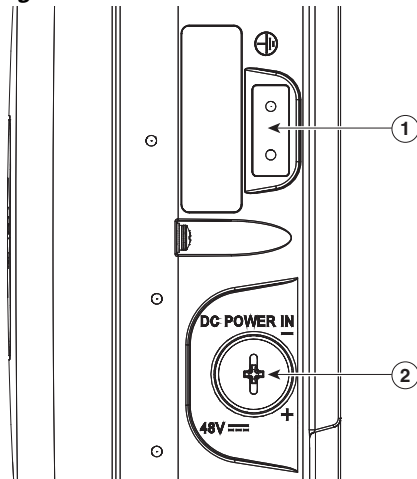
This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

**Caution**

When installing DC power to the access point, always connect the access point end of the cable **FIRST**. When removing the DC power connector, always disconnect the access point end of the cable **LAST**.

Step 3 Use a large Phillips or Flat Blade screw driver to remove the covering plug of the DC Power-In port. Do not discard plug and rubber seal unless you are certain that the port will not have to be re-plugged. (see [Figure 2-28](#) for the location of the DC power connector).

Figure 2-28 Position of the DC Power-In Port on the Right Side of the AP



1	Ground pad.	2	DC Power-In Port (covered).
----------	-------------	----------	-----------------------------

Step 4 Loosen the thread-lock sealing nut of the cable gland by turning it counter clockwise, but do not remove it (see [Figure 2-29](#)).

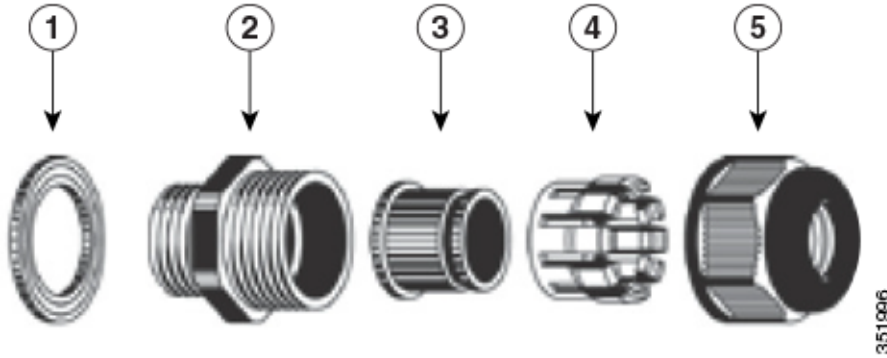
**Note**

Verify that the cable gland has a rubber seal and ensure that it is not damaged.

**Warning**

Failure to install the Cable Gland properly will cause the cable grip to leak.

Figure 2-29 Cable Gland



1	Washer (Gasket)	4	Clamping claw
2	Body	5	Thread-lock sealing nut
3	Sealing insert		



Note The cable gland accepts a cable diameter of 0.20 to 0.35 in. (0.51 to 0.89 cm).

Step 5 Insert a bare end of the DC power cable into the rounded end of the cable gland (see Figure 2-29), and pull approximately 6 inches of cable through the adapter.



Warning

When installing the DC power cable, ensure that cable gland and the rubber gasket are present and installed properly, to avoid water leakage into the enclosure. See Figure 2-29 and Figure 2-32.

Step 6 Strip the DC cable jacket back by about 1 inch to expose the wires and then strip the insulation by about 0.5 inch (or 12 mm) from each wire.

Step 7 Push in the orange colored spring-loaded securing tabs and insert the wire (see Figure 2-30) all the way into the two-position terminal block connector (Cisco Part Number 29-100226-01, Figure 2-31), and then release the tabs. Tug on the wire to ensure that it is properly secured.

Figure 2-30 Push in the securing tab, and wire, as the arrow shows

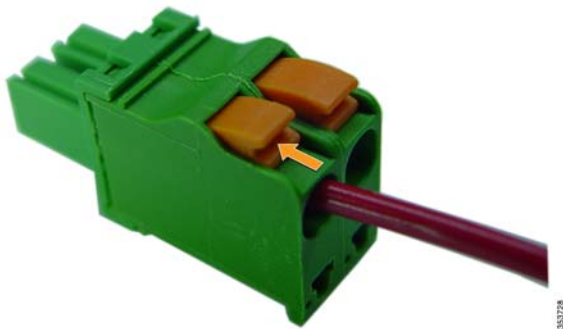
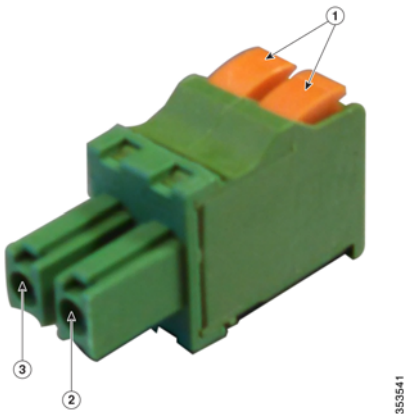


Figure 2-31 Two-Position Terminal Block Connector



1	Securing tabs	3	Ground (DC return)
2	DC +		

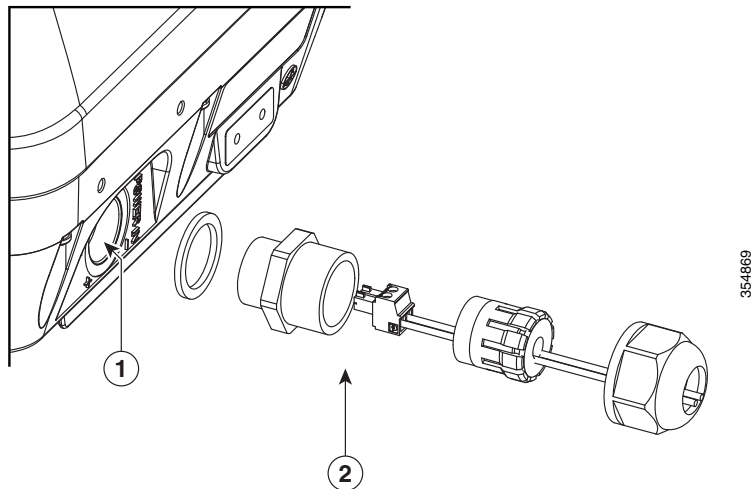
Step 8

Step 9 Insert the two-position terminal strip into the DC power opening in the access point case, and carefully push the terminal strip into the internal connector (see [Figure 2-32](#)).



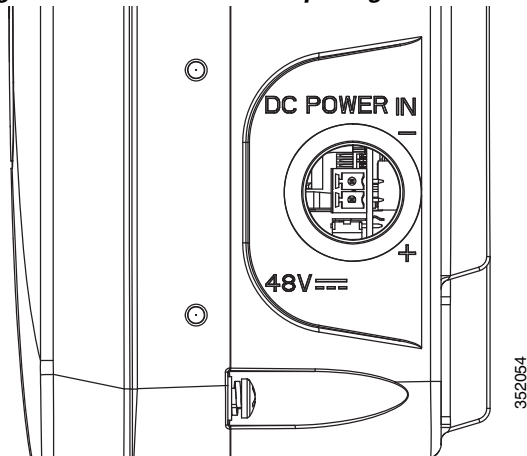
Note Ensure that the polarity of the terminal strip properly matches the polarity markings on the enclosure (see [Figure 2-33](#))

Figure 2-32 Inserting the Terminal Strip into the DC Power Opening in the Access Point Case



1	DC power opening in access point case. Also see Figure 2-33 .	2	Exploded view of the cable gland on the DC power cable
---	---	---	--

Figure 2-33 DC Power Opening in the Access Point Case



- Step 10** Slide the cable gland with the rubber seal towards the access point, and screw the threaded end of the body into the access point, and hand-tighten.
- Step 11** Use an adjustable wrench, a 28-mm wrench to tighten the threaded end of the body to 15 lb-in.
- Step 12** Use an adjustable wrench and tighten the thread-lock seal nut to 15 lb-in.
- Step 13** Ensure that the antennas are connected to the access point before you apply power to the access point.
- Step 14** Turn on the DC power at the designated circuits.

Connecting Streetlight AC Power

The access point can be installed on a streetlight pole and powered from a streetlight outdoor light control using the optional streetlight power tap adapter and AC/DC power adapter, AIR-PWRADPT-RGD1=.

The AC/DC power adapter is used inline from the street light tap to the 1560 DC connector. The AC power tap only can be used with the AC/DC power adapter.

When powering the access point with AC power other than the streetlight power tap adapter, you must ensure that the following conditions are observed:

1. AC power can be conveniently cut from the unit, but not by disconnecting the AC power connector on the unit.
2. You must protect any AC power plugs and AC receptacles from water and other outdoor elements. You can use a UL-listed waterproofing enclosure suitable for covering the AC receptacle and AC power plug that supplies power to the unit as described in Article 406 of the NEC.
3. When you install the access point outdoors or in a wet or damp location, the AC branch circuit that powers the access point should have ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).



Warning

A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.

Statement 1022

**Warning**

Be very careful when connecting the streetlight adapter to Category 3 pole-top power. If you are not careful, you may electrocute yourself or fall. Statement 363

**Caution**

Before connecting or disconnecting a power cord, you must remove AC power from the power cord using a suitable service disconnect.

The schematics of installing the AP on a streetlight pole are given in [Figure 2-34](#) and [Figure 2-35](#). To install an access point on a streetlight pole, follow these steps:

Step 1 Turn off the AC power to the streetlight pole.

Step 2 Turn off power to the AC power source at the designated circuits.

**Warning**

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

**Caution**

For your safety, when connecting the access point AC power connector, always connect the access point end of the cable **FIRST**. When removing the AC power connector, always disconnect the access point end of the cable **LAST**.

Step 3 Ensure that the power to the outdoor light control is turned off and then disconnect the outdoor light control from its fixture.

Step 4 Connect the streetlight power tap adapter, through a field termination unit, to the access point AC/DC power adapter.

**Caution**

When installing the streetlight power tap adapter to the access point AC power connector, always connect the access point end of the cable **first**. When removing the streetlight power tap adapter, always disconnect the access point end of the cable **last**.

**Note**

- The access point must be mounted within 3 feet (1 m) of the outdoor light control.
- The AC/DC power adapter must be grounded. The AC/DC power adapter has an operating range of 100 to 277 VAC 50/60 Hz.

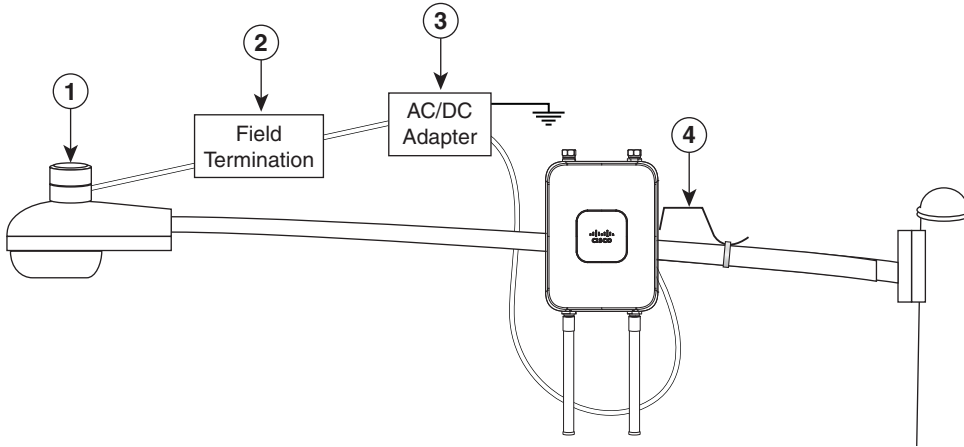
Step 5 Ground the access point to the streetlight pole using a 6-AWG ground wire. For more details, see [Grounding the Access Point, page 2-42](#).

Step 6 Plug the streetlight power tap adapter into the outdoor light control fixture.

Step 7 Ensure that the antennas are connected to the access point.

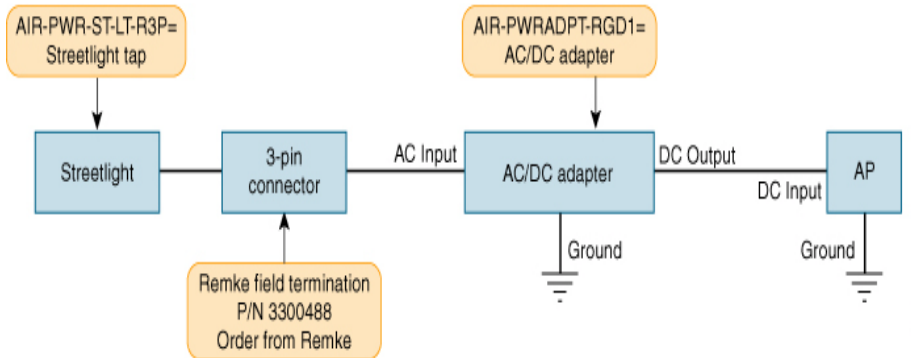
Step 8 Turn on the power to the outdoor light control fixture at the designated circuits, and thereby, turn on the power to the access point.

Figure 2-34 Using Streetlight Power



1	Outdoor light control	3	AC/DC power adapter
2	Field termination	4	6-AWG copper grounding wire

Figure 2-35 Components of the Streetlight Deployment



Note Deployment of the AP as shown in the streetlight deployment in [Figure 2-34](#) requires an alternate AP mounting kit.

Connecting Data Cables

All models of the AP support data connections through the Ethernet port and the Small Form-factor Pluggable (SFP) port. However, both the Ethernet port and the SFP port cannot be used for data at the same time.

If the SFP is detected and active, the Ethernet port is disconnected. If the SFP is not detected, the Ethernet port stays connected.

If you are using the SFP port, to delivery data through a fiber-optic cable, then the AP needs to be powered by DC power, power adapter, or by a power injector.

For details on installing Ethernet, see [Connecting an Ethernet Cable to the Access Point, page 2-53](#).

For details on installing a a fiber-optic cable, see [Connecting a Fiber-optic Cable to the AP, page 2-55](#).

Connecting an Ethernet Cable to the Access Point

You need to supply these tools and materials:

- Shielded outdoor-rated Ethernet (CAT5e or better) cable with 0.2 to 0.35 in. (0.51 to 0.89 cm) diameter
- RJ-45 connector and installation tool
- Adjustable Wrench or 28 mm box wrench
- Large Phillips or Flat Blade screwdriver

To connect the shielded Ethernet cable to the access point, follow these steps:

Step 1 Disconnect power to the power injector, and ensure all power sources to the access point are turned off.



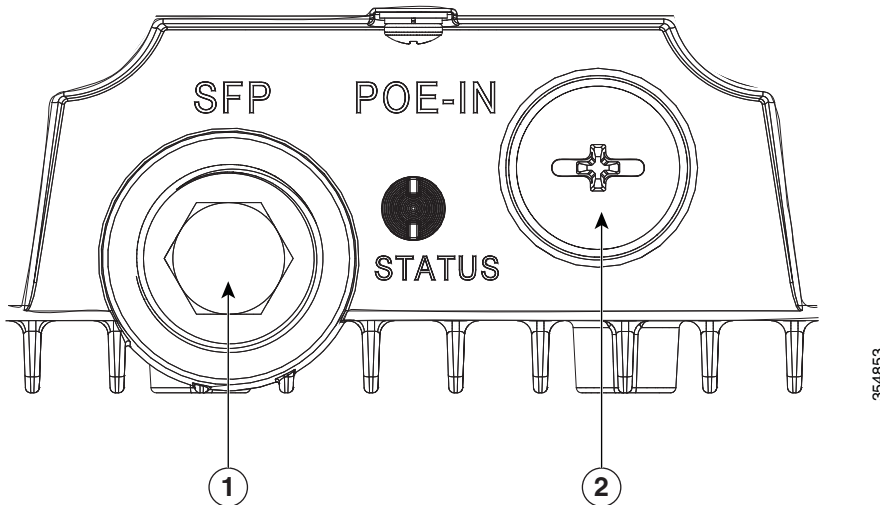
Warning

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028

Step 2 Ensure a 6 AWG ground wire is connected to the access point (see the “[Grounding the Access Point](#)” section on page 2-42).

Step 3 Use a large Phillips or Flat Blade screw driver to remove the covering plug from the access point. Do not discard plug and rubber seal unless you are certain that the port will not have to be re-plugged (see [Figure 2-36](#) for the location).

Figure 2-36 Access Point PoE-In Connector



1 SFP port (covered)

2 PoE-In port (covered)

Step 4 Loosen the Thread-Lock sealing nut of the cable gland by turning it counter clockwise, but do not remove it (see [Figure 2-37](#)).



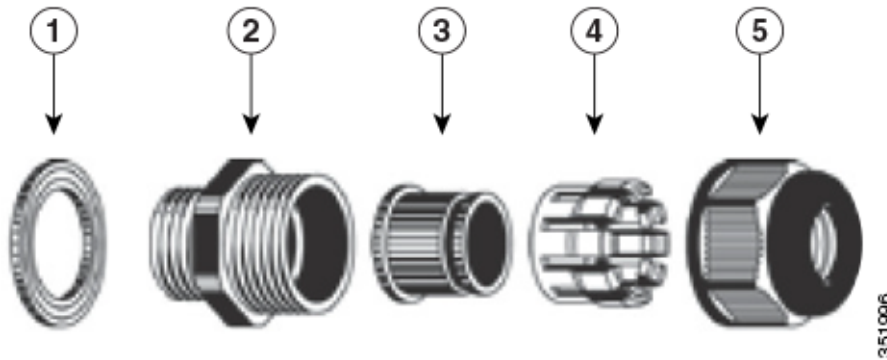
Note

Verify that the cable gland has a rubber seal and ensure that it is not damaged.

**Warning**

Failure to install the cable gland and rubber gasket properly will cause the cable grip to leak.

Figure 2-37 Cable Gland



1	Washer (Rubber Gasket)	4	Clamping claw
2	Body	5	Thread-lock sealing nut
3	Sealing insert		

- Step 5** Insert the unterminated end of the Ethernet cable through the sealing nut end of the cable gland (see [Figure 2-37](#)), and pull several inches of cable through the adapter.
- Step 6** Install an RJ-45 connector on the unterminated end of the Ethernet cable using your Ethernet cable installation tool.

**Warning**

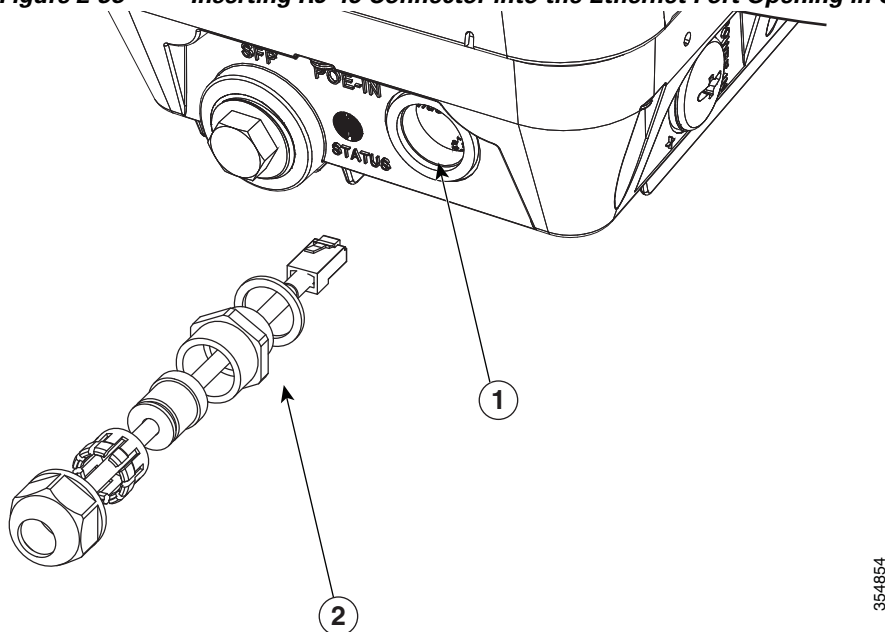
To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord. Statement 1023

**Warning**

When installing the RJ-45 connector, ensure that cable gland and the rubber gasket are present and installed properly, to avoid water leakage into the enclosure. See [Figure 2-37](#) and [Figure 2-38](#).

- Step 7** Carefully insert the RJ-45 cable connector into the Ethernet port opening on the access point, and connect to the internal Ethernet connector (see [Figure 2-38](#)).

Figure 2-38 Inserting RJ-45 Connector into the Ethernet Port Opening in Case



354854

1	Ethernet port opening in access point case.	2	RJ-45 connector, on shielded outdoor-rated Ethernet (CAT5e or better) cable (with an exploded view of the cable gland, on the Ethernet cable).
---	---	---	--

- Step 8** Slide the cable gland with the rubber seal towards the access point, and screw the threaded end of the body into the access point, and hand-tighten.
- Step 9** Use an adjustable wrench or a 28-mm wrench to tighten the threaded end of the body into the enclosure. Tighten to 15 lb-in.
- Step 10** Use an adjustable wrench and tighten the thread-lock seal nut to 15 lb-in.
- Step 11** Ensure that the antennas are connected to the access point before you apply power to the access point.
- Step 12** Route your Ethernet cable, and cut off any excess cable.
- Step 13** Install an RJ-45 connector on the unterminated cable end, and insert it into the power injector.
- Step 14** Turn on the power to the power injector.


Connecting a Fiber-optic Cable to the AP

The Cisco supplied fiber-optic kit enables the access point to support fiber-optic network connections. You require the following materials for connecting the fiber-optic cable to the AP:

- Small form-factor pluggable (SFP) transceiver module
- SFP module adapter

- SC or Duplex LC fiber-optic cables. The outer diameter of the fiber optic cable should be 0.24-0.47 inches (6-12 mm).
- Cable gland. The cable gland cannot hold a cable with diameter more than 0.47" (12 mm).
- Adjustable wrench

You can connect the fiber-optic networking cable to the SFP port (labeled '4' on the base of the AP). The small form-factor pluggable (SFP) transceiver module is used to connect the cable to the SFP port. The SFP port provides both Power-over-Cable and backhaul over fiber options. To install the SFP transceiver module and the cable, follow this procedure:

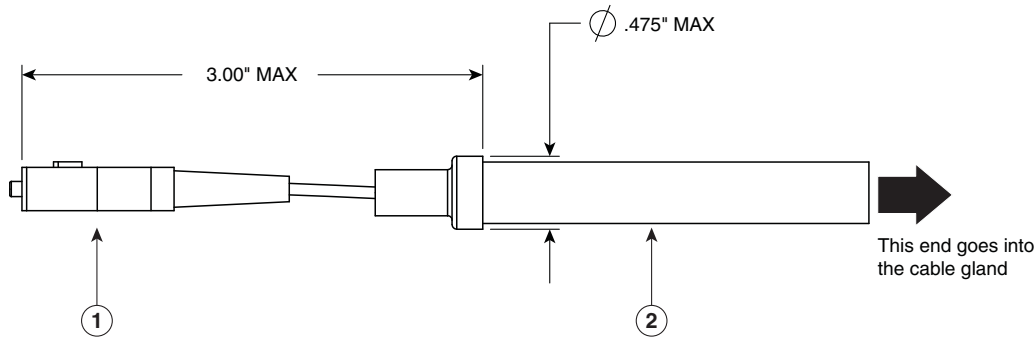
-
- Step 1** Ensure that all power sources have been disconnected from the access point.
- Step 2** Remove the covering plug from the SFP port by following the guidelines given in this step.
- The SFP port covering plug is designed to be removed only once, and then be replaced with the SFP adapter. The plug does not have a rubber O-ring, but is fixed in place using a thread seal tape on the threads during manufacturing. While removing the plug, you need to ensure that its hex bolt-head does not get stripped. For this:
- Place the AP on its back (resting on the heat fins) on a solid, but padded surface, to avoid scratching the paint.
 - Pressing down with your hand on the face of the AP and holding the AP firmly in place, proceed to the next step.
 - Use a 5/8" (16 mm) 6-point socket wrench to loosen the hex bolt-head SFP port plug. Firmly and carefully, turn the socket wrench counter-clockwise to loosen the plug. This requires a torque of 25 ft-lb (34 Nm).
- Though not ideal, a 5/8" (16 mm) 12-point socket wrench can be used too. A crescent wrench is to be used only if the socket wrenches are not available. Do not use a pipe or monkey wrench for this task, as it will strip the hex bolt-head.
- Step 3** Insert the SFP module into the SFP port, and ensure that it latches properly.
- Step 4** Loosen the cable gland's nut (round end of the cable gland) by turning counterclockwise, but do not remove.
- Step 5** Thread the fiber optic cable, from its unterminated end, into the cable gland. See [Figure 2-39](#) and [Figure 2-40](#).
- Thread the cable through the gland all the way till the gland is near the SC or LC optic fiber connectors. The cable gland's nut must remain loose at this time.
-
-  **Note** The SC or LC optic fiber connectors are too big to pass through the cable gland. That is the reason why you need to thread the cable through the gland from the unterminated end (even if the cable is quite long).
-
- Step 6** Insert the SC or LC optic fiber connector-end of the cable, into the SFP module adapter. Do not attach the cable gland to the adapter yet. See [Figure 2-41](#).
- Step 7** Insert the SC or LC optic fiber connector into the SFP module and ensure that it latches into place. See [Figure 2-41](#).
- Step 8** Add sealant or tape around the adapter's pipe thread, and then it screw into the AP chassis.

- Step 9** Keeping the cable gland nut loose, carefully screw the threaded end of the cable gland into the SFP module adapter and hand-tighten. Use an adjustable wrench to tighten the threaded end of the cable gland to 6-7 lb.ft (8.1 to 9.5 Nm).
- Step 10** Tighten the cable gland nut until it is properly fastened around the fiber optic cable. Use an adjustable or open-end wrench to tighten to 2.7 to 3.2 lb.ft (3.66 to 4.34 Nm).



Caution When removing this SFP assembly it is absolutely imperative that you proceed in the reverse order of this installation. Start by loosening the cable gland's nut.

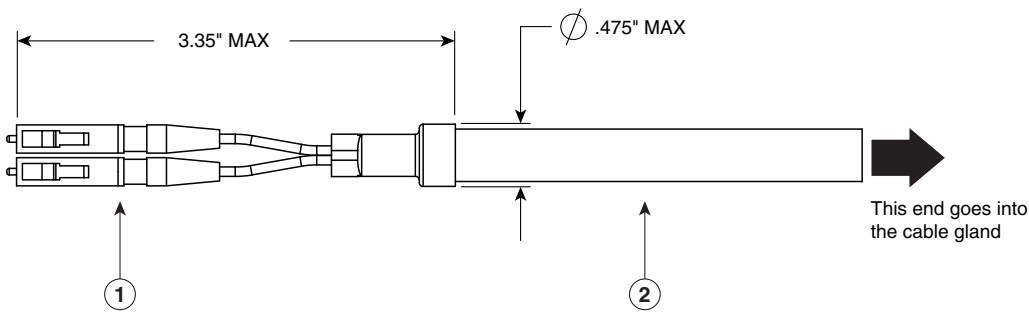
Figure 2-39 SC Fiber-optic cable



353664

1 SC optic fiber connector	2 Optic fiber cable
-----------------------------------	----------------------------

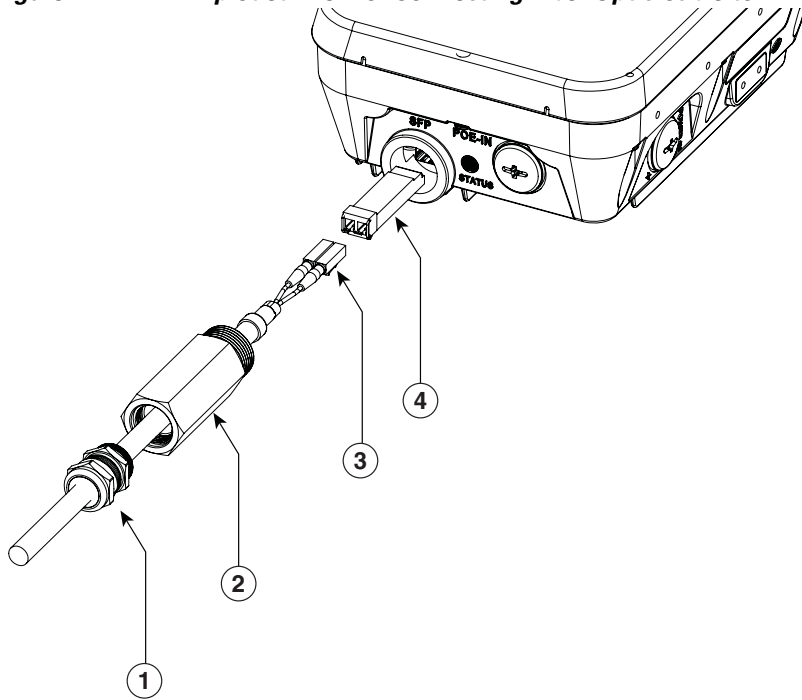
Figure 2-40 Duplex LC Fiber Optic Cable



353665

1 Duplex LC optic fiber connector	2 Optic fiber cable
--	----------------------------

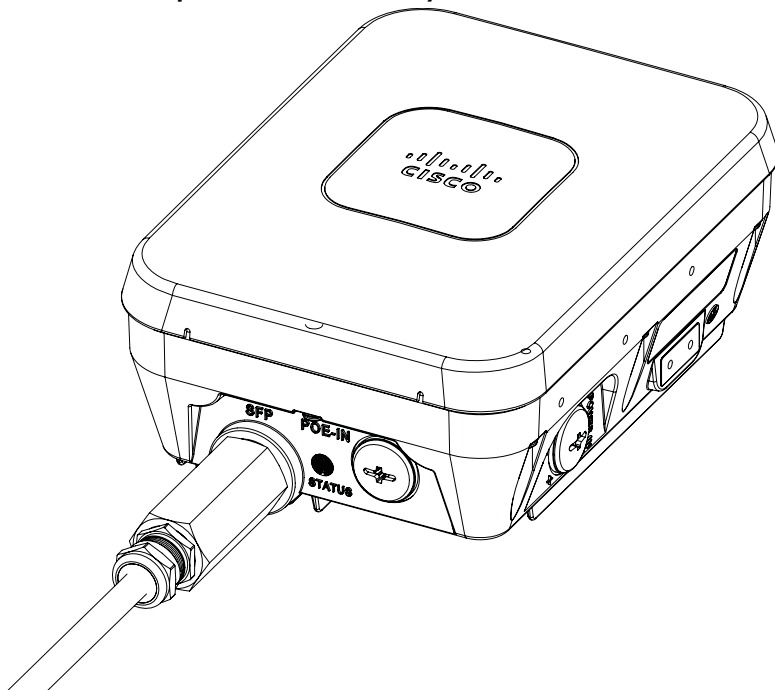
Figure 2-41 Exploded View of Connecting Fiber-Optic Cable to AP



354855

1	Cable gland	3	Duplex LC Fiber-optic cable
2	SFP module adapter	4	SFP transceiver module

Figure 2-42 Fiber-optic Cable Successfully Connected to AP



354860

Configuring the Access Point

When you power up an AP that is not connected to a wired Ethernet, fiber-optic, or cable network to the controller, the access point uses the Cisco Adaptive Wireless Path Protocol (AWPP) to bind to another mesh access point with the best path to a root access point (RAP) connected to the wired network to a controller. The access point sends a discovery request when powered up. If you have configured the access point in the controller correctly, the controller sends back a discovery response to the access point. When that happens, the access point sends out a join request to the controller, and the controller responds with a join confirmation response. Then the access point establishes a Control And Provisioning of Wireless Access Points (CAPWAP) connection to the controller and gets the shared secret configured on the controller.

For information on configuring the access point, see the following documents:

- For Lightweight Access Points and Mesh Access Points, see the *Cisco Wireless LAN Controller Configuration Guide*, which is available at:
[\(URL to be added at FCS\)](#)
- For Mesh Access Points, see the *Cisco Wireless Mesh Access Points, Design and Deployment Guide*, which is available at:
[\(URL to be added at FCS\)](#)



Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the 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/cisco/web/support/index.html>

Sections in this chapter include:

- [Guidelines for Using the Access Point, page 3-2](#)
- [Controller MAC Filter List, page 3-3](#)
- [Using DHCP Option 43, page 3-3](#)
- [Accessing the Console Port and the Reset Button, page 3-4](#)
- [Monitoring the Access Point Status LED, page 3-5](#)
- [Verifying Controller Association, page 3-8](#)
- [Changing the Bridge Group Name, page 3-8](#)

Guidelines for Using the Access Point

You should keep these guidelines in mind when you use the access point:

- The access point only supports Layer 3 CAPWAP communications with the controllers.
In Layer 3 operation, the access point and the controller can be on the same or different subnets. The access point communicates with the controller using standard IP packets. A Layer 3 access point on a different subnet than the controller requires a DHCP server on the access point subnet and a route to the controller. The route to the controller must have destination UDP ports 12222 and 12223 open for CAPWAP communications. The route to the primary, secondary, and tertiary controllers must allow IP packet fragments.
- Before deploying your access points, ensure that the following has been done:
 - Your controllers are connected to switch ports that are configured as trunk ports.
 - Your access points are connected to switch ports that are configured as untagged access ports.
 - A DHCP server is reachable by your access points and has been configured with Option 43. Option 43 provides the IP addresses of the management interfaces of your controllers. Typically, a DHCP server can be configured on a Cisco switch.
 - Optionally, a DNS server can be configured to enable CISCO-CAPWAP-CONTROLLER. Use *local domain* to resolve to the IP address of the management interface of your controller.
 - Your controllers are configured and reachable by the access points.
 - Your controllers are configured with the access point MAC addresses and the MAC filter list is enabled.
 - Your switch must forward DHCP requests.
- After the access points are associated to the controller, you should change the bridge group name (BGN) from the default value. With the default BGN, the mesh access points (MAPs) can potentially try to connect with other mesh networks and slow down the convergence of the network.

Convergence Delays

During deployment, the access points can experience convergence delays due to various causes. The following list identifies some operating conditions that can cause convergence delays:

- A root access point (RAP) attempts to connect to a controller using any of the wired ports (cable, fiber-optic, PoE-in). If the wired ports are operational, the RAP can potentially spend several minutes on each port prior to connecting to a controller.
- If a RAP is unable to connect to a controller over the wired ports, it attempts to connect using the wireless network. This results in additional delays when multiple potential wireless paths are available.
- If a MAP is unable to connect to a RAP using a wireless connection, it then attempts to connect using any available wired port. The access point can potentially spend several minutes for each connection method, before attempting the wireless network again.

Bridge Loop

The access point supports packet bridging between wired and wireless network connections. The same network must never be connected to multiple wired ports on an access point or on two bridged access points. A bridge loop causes network routing problems.

Controller DHCP Server

The controller DHCP server only assigns IP addresses to lightweight access points and wireless clients associated to an access point. It does not assign an IP address to other devices, including Ethernet bridging clients on the mesh access points.

MAP Data Traffic

If the signal on the access point backhaul channel has a high signal-to-noise ratio, it is possible for a MAP to connect to the controller, via parent node, but not be able to pass data traffic, such as pinging the access point. This can occur because the default data rate for backhaul control packets is set to 6 Mb/s, and the backhaul data rate set to auto by the user.

Controller MAC Filter List

Before activating your access point, you must ensure that the access point MAC address has been added to the controller MAC filter list and that **Mac Filter List** is enabled.

**Note**

The access point MAC address and barcode is located on the bottom of the unit. When two MAC addresses are shown, use the top MAC address.

To view the MAC addresses added to the controller MAC filter list, you can use the controller CLI or the controller GUI:

- Controller CLI—Use the **show macfilter summary** controller CLI command to view the MAC addresses added to the controller filter list.
- Controller GUI—Log into your controller web interface using a web browser, and choose **SECURITY > AAA > MAC Filtering** to view the MAC addresses added to the controller filter list.

Using DHCP Option 43

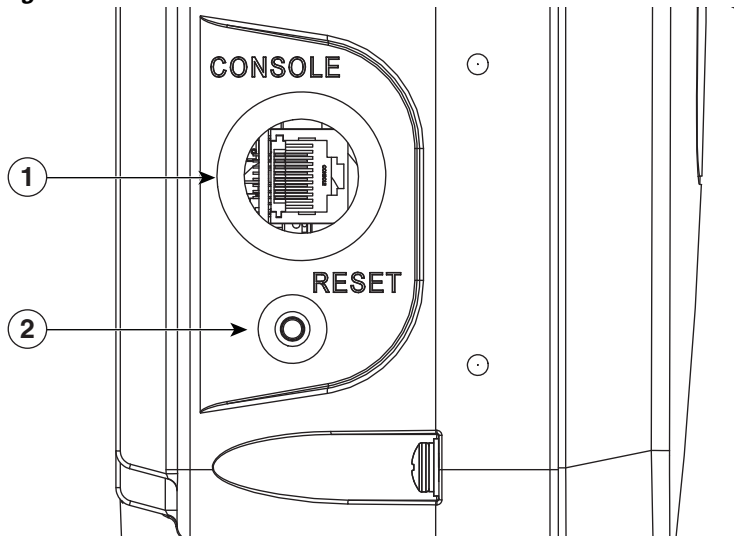
You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. Refer to the product documentation for your DHCP server for instructions on configuring DHCP Option 43. To see sample configurations for DHCP Option 43 for, go to the following URL:

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html>

Accessing the Console Port and the Reset Button

The access point has a console port and a reset button located on the right side (see [Figure 3-1](#)). The console port is located under a covering plug. The reset button is located under a screw.

Figure 3-1 Console Port and Reset Button Location



<p>1 Console Port (uncovered).</p> <p>Use a large Phillips or Flat Blade screw driver to remove the covering plug of the port. Do not discard plug and rubber seal unless you are certain that the port will not have to be re-plugged.</p> <p>Inspect the seal of the plug and properly tighten it every time the plug is removed and replaced. Tighten the plug to 15 lbf-in.</p>	<p>2 Reset Button (uncovered).</p> <p>The reset button is recessed in a small hole that is sealed with a screw and a rubber gasket. For information on how to use the reset button, see the “Resetting the Access Point” section on page 3-4.</p>
--	--

Resetting the Access Point

Using the Reset button you can:

- Reset the AP to the default factory-shipped configuration.
- Clear the AP internal storage, including all configuration files.

To access the Reset button:

-
- Step 1** Use a Phillips screwdriver to remove the reset button screw.
- Ensure that you do not lose the screw and the rubber gasket.
- Step 2** To press the Reset button, use a straightened paper-clip or a small screwdriver or a pen. See the section following this procedure for information on using the Reset button.
- Strictly follow this procedure after you have finished using the Reset button.
- Step 3** Inspect the gasket. If the gasket has any signs of damage, it should be replaced to avoid water leakage into the unit.

- Step 4** Close the recess with the screw and the gasket. Use a Phillips screwdriver to tighten the screw to 1.8 to 2 lb.ft (2.49 to 2.71 Nm).

To use the Reset button, press, and keep pressed, the Reset button on the access point during the AP boot cycle. Wait until the AP status LED changes to Amber. During this, the AP console shows a seconds counter, counting the number of seconds the Reset button is pressed. Then:

- To reset the AP to its default factory-shipped configuration, keep the Reset button pressed for less than 20 seconds. The AP configuration files are cleared.

This resets all configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

- To clear the AP internal storage, including all configuration files and the regulatory domain configuration, keep the Reset button pressed for more than 20 seconds, but less than 60 seconds.

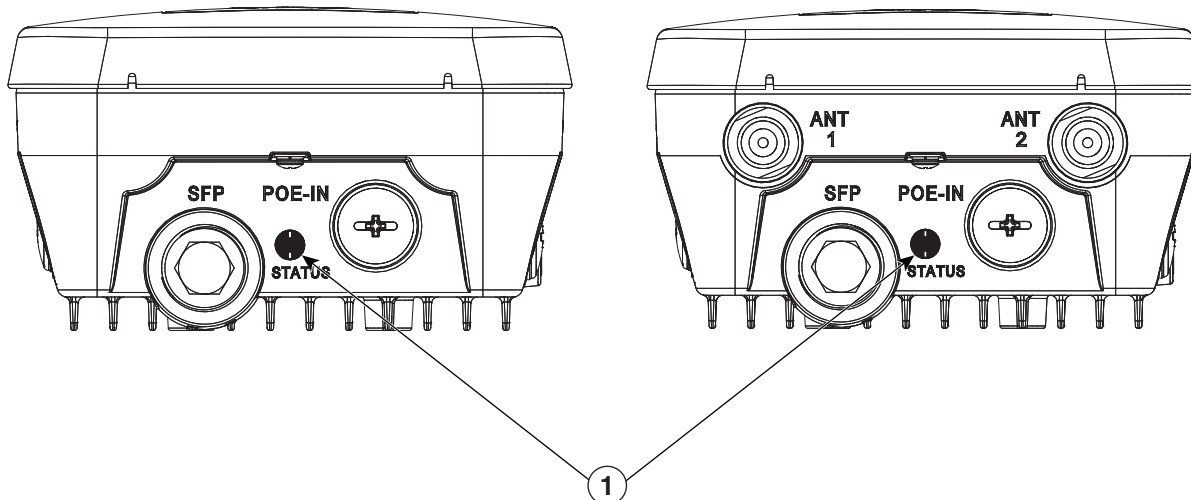
The AP status LED changes from Amber to Red, and all the files in the AP storage directory are cleared.

If you keep the Reset button pressed for more than 60 seconds, the Reset button is assumed faulty and no changes are made.

Monitoring the Access Point Status LED

If your access point is not working properly, look at the LED on the bottom of the unit. You can use them to quickly assess the status of the unit. [Figure 3-2](#) shows the location of the access point LED.

Figure 3-2 Access Point Status LED



354856

- 1** If your access point is not working properly, look at the status LED on the bottom of the unit, to quickly assess the status of the unit. The access point LED signals are listed in [Table 3-1](#).

**Note**

It is expected that there will be small variations in LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer specifications and is not a defect.

The access point LED signals are listed in [Table 3-1](#).

Table 3-1 **Access Point LED Signals**

LED Message Type	Color	Meaning
Boot loader status sequence	Blinking Green	Boot loader status sequence: <ul style="list-style-type: none"> • DRAM memory test in progress • DRAM memory test OK • Board initialization in progress • Initializing FLASH file system • FLASH memory test OK • Initializing Ethernet • Ethernet OK • Starting Cisco IOS • Initialization successful
Boot loader warnings	Blinking Amber	Configuration recovery is in progress (the Reset button has been pushed for 2-3 seconds)
	Red	There is an Ethernet failure or an image recovery (the Reset button has been pushed for 20-30 seconds)
	Blinking Green	An image recovery is in progress (the Reset button has been released)

Table 3-1 Access Point LED Signals

LED Message Type	Color	Meaning
Boot loader errors	Red	There has been a DRAM memory test failure
	Blinking Red and Amber	There has been a FLASH file system failure
	Blinking Red and Off	This sequence may indicate any of the following: <ul style="list-style-type: none"> • Environment variable failure • Bad MAC address • Ethernet failure during image recovery • Boot environment failure • No Cisco image file • Boot failure
AP OS errors	Red	There has been a software failure; a disconnect then reconnect of the unit power may resolve the issue
	Cycling through Red, Green, Amber and Off	This is a general warning of insufficient inline power.
Association status	Chirping (short blips) Green	This status indicates a normal operating condition. The unit is joined to a controller, but no wireless client is associated with it.
	Solid Green	Normal operating condition with at least one wireless client associated with the unit
Operating Status	Blinking Amber	A software upgrade is in progress
	Cycling through Green, Red and Amber	Discovery/join process is in progress
	Rapidly cycling through Red, Green, Amber and Off	This status indicates that the Access Point location command has been invoked.
	Blinking Red	This status indicates that an Ethernet link is not operational
Alignment Mode	Solid Green	Signal level > -44 dBm
	Fast blinking Green	Signal level -47 to -44 dBm
	Medium blinking Green	Signal level -50 to -47 dBm
	Solid Amber	Signal level -53 to -50 dBm
	Fast blinking Amber	Signal level -57 to -53 dBm

Table 3-1 Access Point LED Signals

LED Message Type	Color	Meaning
	Medium blinking Amber	Signal level –60 to –57 dBm
	Slow blinking Amber	Signal level –63 to –60 dBm
	Slow blinking Red	Signal level –66 to –63 dBm
	Medium blinking Red	Signal level –69 to –66 dBm
	Fast blinking Red	Signal level –72 to –69 dBm
	Solid Red	Signal level –75 to –72 dBm
	Off	Signal level < –75 dBm

Verifying Controller Association

To verify that your access point is associated to the controller, follow these steps:

-
- Step 1** Log into your controller web interface using a web browser.
You can also use the controller CLI **show ap summary** command from the controller console port.
 - Step 2** Click **Wireless**, and verify that your access point MAC address is listed under Ethernet MAC.
 - Step 3** Log out of the controller, and close your web browser.
-

Changing the Bridge Group Name

The bridge group name (BGN) controls the association of the access points to a RAP. BGNs can be used to logically group the radios to avoid different networks on the same channel from communicating with each other. This setting is also useful if you have more than one RAP in your network in the same area.

If you have two RAPs in your network in the same area (for more capacity), we recommend that you configure the two RAPs with different BGNs and on different channels.

The BGN is a string of ten characters maximum. A factory-set bridge group name (NULL VALUE) is assigned during manufacturing. It is not visible to you, but allows new access point radios to join a network of new access points. The BGN can be reconfigured from the Controller CLI and GUI. After configuring the BGN, the access point reboots.

After the access points are deployed and associated to the controller, the BGN should be changed from the default value to prevent the MAPs from attempting to associate to other mesh networks.

The BGN should be configured very carefully on a live network. You should always start with the most distant access point (last node) from the RAP and move towards the RAP. If you start configuring the BGN in a different location, then the access points beyond this point (farther away) are dropped, as they have a different BGN.

To configure the BGN for the access points using the controller GUI, follow these steps:

-
- Step 1** Log into your controller using a web browser.
 - Step 2** Click **Wireless**. When access points associates to the controller, the access point name appears in the AP Name list.
 - Step 3** Click on an access point name.
 - Step 4** Find the Mesh Information section, and enter the new BGN in the Bridge Group Name field.
 - Step 5** Click **Apply**.
 - Step 6** Repeat Steps 2 through 5 for each access point.
 - Step 7** Log out from your controller, and close your web browser.
-



Safety Guidelines and Warnings

Translated versions of all safety warnings are available on Cisco.com. Additional safety information, along with regulatory information, is provided in [Appendix B, “Declarations of Conformity and Regulatory Information”](#).



Warning

This equipment is to be installed by trained and qualified personnel, as per these installation instructions. The installer is responsible for obtaining any required local or national safety inspections of the structural integrity of the installation by the local authority/inspection department.



Warning

Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use. Statement 364



Warning

The cables specified in this installation guide that are used with the specified cable glands provide protection against ingress of moisture for a Type 4/IP67 classified enclosure. If substitute cable are used, the installer must ensure that the size (OD) of the cable meets the acceptable range allowed by the cable gland.



Warning

This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 366



Warning

Read the installation instructions before connecting the system to the power source. Statement 1004



Warning

Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040



Warning

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

**Warning****A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.**

Statement 1022

**Warning****To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023**Warning****This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028**Warning****Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Statement 1030

**Warning****Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards.** Statement 1033**Warning****When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046.**Warning****Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, because they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (for example, U.S.:NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 1052**Caution**

Before connecting or disconnecting a power cord, you must remove power from the power cord using a suitable service disconnect.

**Warning****Installation of the equipment must comply with local and national electrical codes.** Statement 1074**Caution**

All installation methods for mounting an access point on any wall surface is subject to the acceptance of local jurisdiction.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to 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 operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For safety and to achieve a good installation, please read and follow these safety precautions:

- Select your installation site with safety, as well as performance in mind. Remember: electric power lines and phone lines look alike. For safety, assume that any overhead line can kill.
- Call your electric power company. Tell them your plans, and ask them to come look at your proposed installation.
- Plan your installation carefully and completely before you begin. Successful raising of a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
- When installing the access point and antennas, remember:
 - Do not use a metal ladder.
 - Do not work on a wet or windy day.
 - Do dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
- Use a rope to lift the access point. If the assembly starts to drop, get away from it and let it fall.
- If any part of the antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.

If an accident should occur, call for qualified emergency help immediately.

Avoiding Damage to Radios in a Testing Environment

The radios on outdoor units (bridges) have higher transmit power levels than radios on indoor units (access points). When you test high-power radios in a link, you must avoid exceeding the maximum receive input level for the receiver. At levels above the normal operating range, packet error rate (PER) performance is degraded. At even higher levels, the receiver can be permanently damaged. To avoid receiver damage and PER degradation, you can use one of the following techniques:

- Separate the omnidirectional antennas by at least 2 ft (0.6 m) to avoid receiver damage or by at least 25 ft (7.6 m) to avoid PER degradation.



Note These distances assume free space path loss and are conservative estimates. Required separation distances for damage and performance degradation levels in actual deployments are less if conditions are not non-line-of-sight.

- Reduce the configured transmit power to the minimum level.

- Use directional antennas, and keep them away from each other.
- Cable the radios together using a combination of attenuators, combiners, or splitters to achieve a total attenuation of at least 60 dB.

For a radiated test bed, the following equation describes the relationships among transmit power, antenna gain, attenuation, and receiver sensitivity:

$$\text{txpwr} + \text{tx gain} + \text{rx gain} - [\text{attenuation due to antenna spacing}] < \text{max rx input level}$$

Where:

txpwr = Radio transmit power level

tx gain = transmitter antenna gain

rx gain = receiver antenna gain

For a conducted test bed, the following equation describes the relationships among transmit power, antenna gain, and receiver sensitivity:

$$\text{txpwr} - [\text{attenuation due to coaxial components}] < \text{max rx input level}$$



Caution

Under no circumstances should you connect the antenna port from one access point to the antenna port of another access point without using an RF attenuator. If you connect antenna ports, you must not exceed the maximum survivable receive level of 0 dBm. Never exceed 0 dBm, or damage to the access point can occur. Using attenuators, combiners, and splitters having a total of at least 60 dB of attenuation ensures that the receiver is not damaged and that PER performance is not degraded.

Safety Precautions when Installing Antennas



Warning

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54). Statement 280

1. Before you install an antenna, contact your Cisco account representative to explain which mounting method to use for the size and type of antenna that you are about to install.
2. Select your installation site with safety, as well as performance, in mind. Remember that electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Contact your electric power company. Tell them your plans and ask them to come look at your proposed installation.
4. Plan your installation carefully and completely before you begin. Each person involved in an installation should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing your antenna, follow these guidelines:
 - Do not use a metal ladder.
 - Do not work on a wet or windy day.
 - Do dress properly—wear shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket.

6. If the assembly starts to drop, move away from it and let it fall. Because the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current, even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer.
7. If any part of the antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company to have it removed safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Performing Site Surveys

Every network application is a unique installation. Before installing multiple access points, you should perform a site survey to determine the optimum use of networking components and to maximize range, coverage, and network performance.

Site surveys reveals problems that can be resolved before the network is operational. Because 802.11a/b/g/n operates in an unlicensed spectrum, there may be sources of interference from other 802.11a wireless devices (especially in multi-tenant buildings) that could degrade your 802.11 signals. A site survey can determine if such interference exists at the time of deployment.

A proper site survey involves temporarily setting up mesh links and taking measurements to determine whether your antenna calculations are accurate. Determine the correct locations and antenna types before you drill holes and route cables and mounting equipment.

Consider the following operating and environmental conditions when performing a site survey:

- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
- Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary, because the extra height also increases potential interference from other unlicensed radio systems and decreases the wireless coverage from the ground.
- Physical environment—Clear or open areas provide better radio range than closed or filled areas.
- Obstructions—Physical obstructions such as buildings, trees, or hills can hinder performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.
- How far is your wireless link?
- Has a previous site survey been conducted?
- Do you have a clear Fresnel zone between the access points or radio line of sight?
- What is the minimum acceptable data rate within the link?
- Do you have the correct antenna (if more than one antenna is being offered?)
- Do you have access to both of the mesh site locations?
- Do you have the proper permits, if required?
- Are you following the proper safety procedures and practices?
- Have you configured the access points before you go onsite? It is always easier to resolve configurations or device problems first.

- Do you have the proper tools and equipment to complete your survey.

Translated Safety Warnings

[\(URL to be added at FCS\)](#)



Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1562 Outdoor Access Point.

This appendix contains the following sections:

- [Manufacturers Federal Communication Commission Declaration of Conformity Statement, page B-2](#)
- [Industry Canada, page B-3](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page B-6](#)
- [Declaration of Conformity for RF Exposure, page B-9](#)
- [Guidelines for Operating Cisco Aironet Access Points in Japan, page B-10](#)
- [VCCI Statement for Japan, page B-11](#)
- [Administrative Rules for Cisco Aironet Access Points in Taiwan, page B-11](#)
- [EU Declaration of Conformity, page B-13](#)

Manufacturers Federal Communication Commission Declaration of Conformity Statement

**Models:**

AIR-AP1562I-B-K9

AIR-AP1562E-B-K9

AIR-AP1562D-B-K9

FCC Certification number:

LDK102104

LKD102103

LDK102104

Manufacturer:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

**Caution**

The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using Cisco-supplied antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

**Caution**

To meet regulatory restrictions, the access point must be professionally installed.

Requirements of operator to register the RLAN device operating Outdoors in the 5150 -5250 MHz band and addressing possible interference issues in this band

Section 15.407(j) of the rules established filing requirements for U-NII operators that deploy a collection of more than 1000 outdoor access points with the 5.15-5.25 GHz band, parties must submit a letter to the FCC lab acknowledging that, should harmful interference to licensed services in this band occur, they will be required to take corrective action. Corrective actions may include reducing power, turning off devices, changing frequency bands, and/or further reducing power radiated in the vertical direction.

This material shall be submitted to:

Federal Communications Commission
Laboratory Division, Office of Engineering and Technology
7435 Oakland Mills Road, Columbia, MD, 21046
Attn: U-NII Coordination

or via website at <https://www.fcc.gov/labhelp>
use subject line U-NII Filing

Industry Canada

Models:	IC Certification Number:
AIR-AP1562I-A-K9	2461B-102104
AIR-AP1562E-A-K9	2461B-102103
AIR-AP1562D-A-K9	2461B-102104

Canadian Compliance Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Antenna Type	Antenna Gain	Antenna Impedance
Dual-band Omni	4/7 dBi	50 ohms
Dual-band Omni	7/4 dBi	50 ohms
Dual-Band Directional	9/10 dBi	50 ohms
Single-Band Directional Patch	13/14 dBi	50 ohms

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

La bande 5 150-5 250 MHz est réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Users are advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL

Declaration of Conformity for RF Exposure

This access point product has been found to be compliant to the requirements set forth in CFR 47 Section 1.1307 addressing RF Exposure from radio frequency devices as defined in Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields. Antennas that have 8 dBi to 14 dBi gain should be located at a minimum of 23.6 inches (60 cm) or more from the body of all persons. Antennas that have less than 8 dBi gain should be located at a minimum of 9.8 inches (25 cm) or more from the body of all persons.

This access point is also compliant to EN 50835 for RF exposure.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Access Point Models:

AIR-AP1562I-E-K9

AIR-AP1562E-E-K9

AIR-AP1562D-E-K9

Declaration of Conformity with regard to the R&TTE Directive 1999/5/EC & Medical Directive 93/42/EEC

This declaration is only valid for configurations (combinations of software, firmware, and hardware) provided and supported by Cisco Systems. The use of software or firmware not provided and supported by Cisco Systems may result in the equipment no longer being compliant with the regulatory requirements.

Български [Bulgarian]:	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviešu [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

142729

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktiv: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

121404

The following standards were applied:

- EMC—EN 301.489-1 v1.8.1; EN 301.489-17 v2.1.1
- Health & Safety—EN60950-1: 2005; EN 50385: 2002
- Radio—EN 300 328 v 1.7.1; EN 301.893 v 1.5.1

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

This device also conforms to the EMC requirements of the Medical Devices Directive 93/42/EEC.



Note

This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

The product carries the CE Mark:



Declaration of Conformity for RF Exposure

The following is the declaration of conformity for RF exposure for the United States, Canada, European Union and Australia.

United States

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on ANSI C 95.1 and FCC OET Bulletin 65C rev 01.01. To maintain compliance, the minimum separation distance for antennas that have 8 dBi to 14 dBi gain, is 23.6 inches (60 cm) from general bystanders. The minimum separation distance from antennas that have less than 8 dBi gain to general bystanders is 9.8 inches (25 cm).

Canada

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on RSS-102 Rev 5.

AP1562E—To maintain compliance, the minimum separation distance for antennas that have 8 dBi to 14 dBi gain, is 23.6 inches (60 cm) from general bystanders. The minimum separation distance from antennas that have less than 8 dBi gain to general bystanders is 9.8 inches (25 cm).

AP1562I and AP1562D—To maintain compliance, the minimum separation distance is 11.8 inches (30 cm).

Ce système a été évalué pour l'exposition aux RF pour les humains en référence à la norme ANSI C 95.1 (American National Standards Institute) limites. L'évaluation a été basée sur RSS-102 Rev 2.

AP1562E: La distance minimale de séparation de l'antenne de toute personne est de 11.8 "(30 cm) pour les gains d'antenne jusqu'à 8 dBi et 23.6" (60 cm) pour les gains d'antenne de 14 dBi pour assurer le respect.

AP1562I & AP1562D: La distance minimale de séparation de l'antenne de toute personne est de 11.8 "(30 cm) pour assurer le respect.

European Union

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. To maintain compliance, the minimum separation distance for antennas that have 8 dBi to 14 dBi gain, is 23.6 inches (60 cm) from general bystanders. The minimum separation distance from antennas that have less than 8 dBi gain to general bystanders is 9.8 inches (25 cm).

Australia

This system has been evaluated for RF exposure for Humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. To maintain compliance, the minimum separation distance for antennas that have 8 dBi to 14 dBi gain, is 23.6 inches (60 cm) from general bystanders. The minimum separation distance from antennas that have less than 8 dBi gain to general bystanders is 9.8 inches (25 cm).

Guidelines for Operating Cisco Aironet Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet access points in Japan. These guidelines are provided in both Japanese and English.

Access Point Model:

AIR-AP1562E-Q-K9

AIR-AP1562I-Q-K9

AIR-AP1562D-Q-K9

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先 : 03-6434-6500

43768

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-6434-6500

VCCI Statement for Japan



Warning

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

警告

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operating Cisco Aironet Access Points in Taiwan. The rules are provided in both Chinese and English.

Chinese Translation

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Chinese Translation

低功率射頻電機技術規範

4.7 無線資訊傳輸設備

4.7.6 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

2009136

English Translation

Low-power Radio-frequency Devices Technical Specifications

4.7

Unlicensed National Information Infrastructure

4.7.6

The U-NII devices shall accept any interference from legal communications and shall not interfere the legal communications. If interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

4.7.7

Manufacturers of U-NII devices are responsible for ensuring frequency stability such that an emission is maintained within the band of operation under all conditions of normal operation as specified in the user manual.

Statement 371—Power Cable and AC Adapter

接続ケーブル、電源コード、ACアダプタ、バッテリーなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となります。また、電気用品安全法により、当該法の認定（PSEとコードに表記）でなくUL認定（ULまたはCSAマークがコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adapters. Using any other cables/adapters could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

EU Declaration of Conformity

All the Declaration of Conformity statements related to this product can be found at the following location:

<http://www.ciscofax.com>

Operation of Cisco Aironet Access Points in Brazil

This section contains special information for operation of Cisco Aironet access points in Brazil.

Access Point Models

AIR-AP1562E-Z-K9

AIR-AP1562I-Z-K9

AIR-AP1562D-Z-K9

Regulatory Information

Figure B-1 contains Brazil regulatory information for the access point models identified in the previous section.

Figure B-1 Brazil Regulatory Information

Portuguese Translation

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

English Translation

This equipment operates on a secondary basis and consequently must accept harmful interference, including interference from stations of the same kind. This equipment may not cause harmful interference to systems operating on a primary basis.



Access Point Pinouts

This appendix describes the pin signals of the access point Ethernet connectors, and the power injector input and output connectors.

[Table C-1](#) describes the pin signals of the access point LAN connector

Table C-1 Access Point LAN Connector Pinouts

Pin Number	Signal Name
1	Ethernet signal pair (10/100/1000BASE-T)
2	
3	Ethernet signal pair (10/100/1000BASE-T)
6	
4	Ethernet signal pair (10/100/1000BASE-T)
5	
7	Ethernet signal pair (10/100/1000BASE-T)
8	
Shield	Chassis ground

[Table C-2](#) describes the pin signals for the power injector input connector (To Switch).

Table C-2 Power Injector Input Connector (To Switch) Pinouts

Pin Number	Signal Name
1	Ethernet signal pair (10/100/1000BASE-T)
2	
3	Ethernet signal pair 10/100/1000BASE-T)
6	
4	Ethernet signal pair (1000BASE-T)
5	
7	Ethernet signal pair (1000BASE-T)
8	
Shield	Chassis ground

