Getting Started Guide

Cisco Aironet 1800i Access Point

First Published: April 5, 2017

1 About this Guide
2 About the Access Point
3 Safety Instructions
4 Unpacking the AP
5 Ports and Connectors on the AP
6 Preparing the AP for Installation
7 Installation Overview
8 Performing a Pre-Installation Configuration
9 Mounting and Powering the Access Point
10 Configuring and Deploying the Access Point
11 Checking the Access Point LED
12 Miscellaneous Usage and Configuration Guidelines
13 Related Documentation
14 Declarations of Conformity and Regulatory Information

1 About this Guide

This guide provides instructions on how to install and configure your Cisco Aironet 1800i access point. This guide also provides mounting instructions and limited troubleshooting procedures.

The Cisco Aironet 1800i access point is referred to as the *access point,* or abbreviated as *AP* in this document.

2 About the Access Point

The Cisco Aironet 1800i access point is an 802.11 a/b/g/n/ac (Wave 2) access point, with internal antennas only. The access point can be mounted on a wall and supports 2x2:2 SS MU-MIMO applications.

Access Point Model Numbers and Regulatory Domains

The Cisco Aironet 1800i access point model has the model number format AIR-AP1800I-*x*-K9, where the '*x*' placeholder represents the regulatory domain. The '*x*' can be any one of the supported regulatory domains as listed at:

http://www.cisco.com/go/aironet/compliance

Access Point Features

A full listing of the access point's features and specification are provided in the *Cisco Aironet 1800i Access Point Data Sheet*, at the following URL:

(URL to be added at CCO)

The features of the 1800i access points are as follows:

- Supported mode(s) of operation at release:
  - Unified (or Local)
  - Cloud
  - Network Sensor
- Two omnidirectional integrated 2.4 GHz dual-band antennas and 5 GHz single band antennas. Peak antenna gain is approximately 3 dBi and 5 dBi in 2.4 GHz and 5 GHz bands respectively.
- Radio features supported are:
  - 2.4 GHz and 5 GHz concurrent radios
  - 2 GHz radio with 2TX x 2RX and two spatial streams SU-MIMO
  - 5 GHz radio with 2TX x 2RX 802.11ac Wave 2 capable with two spatial streams SU-MIMO and MU-MIMO
  - 802.11ac based Explicit Transmit Beamforming
  - Quality of Service (QoS)
  - Radio Resource Management (RRM)
  - Rogue Detection
  - BandSelect
  - Bluetooth Low Energy 4.0
- The AP supports the following external interfaces:
  - One 10/100/1000 BASE-T (Ethernet) Uplink Interface with inline power capability, Auto-MDIX (automatically support either straight through or crossover cables), and 802.3af/at PoE-In.
  - RS-232 console port connection though a custom 4-pin connector.
- Reset button. For information on how to use the Reset button, see "Using the Reset Button" section on page 21.
- One multi-color LED status indicator. See the "Checking the Access Point LED" section on page 19 for information on the colors of the LED status indicator.

  - BLE atnenna gain is 1 dBi

3 Safety Instructions

Translated versions of the following safety warnings are provided in the translated safety warnings document that is shipped with your access point. The translated warnings are also in the *Translated Safety Warnings for Cisco Aironet Access Points*, which is available on Cisco.com.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning

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

Warning

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

Warning

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

Warning

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

Caution

This product and all interconnected equipment must be installed indoors within the same building, including the associated LAN connections as defined by Environment A of the IEEE 802.3af/at Standard.

Note The access point is suitable for use in environmental air space in accordance with section 300.22.C of the National Electrical Code and sections 2-128, 12-010(3), and 12-100 of the Canadian Electrical Code, Part 1, C22.1. You should not install the power supply or power injector in air handling spaces.

Note Use only with listed Information Technology Equipment (ITE) equipment. For more information on ITE equipment, refer to article 645 of the latest National Electrical Code (NEC).

4 Unpacking the AP

To unpack the access point, follow these steps:

Step 1 Unpack and remove the access point and the mounting accessories, from the shipping box.

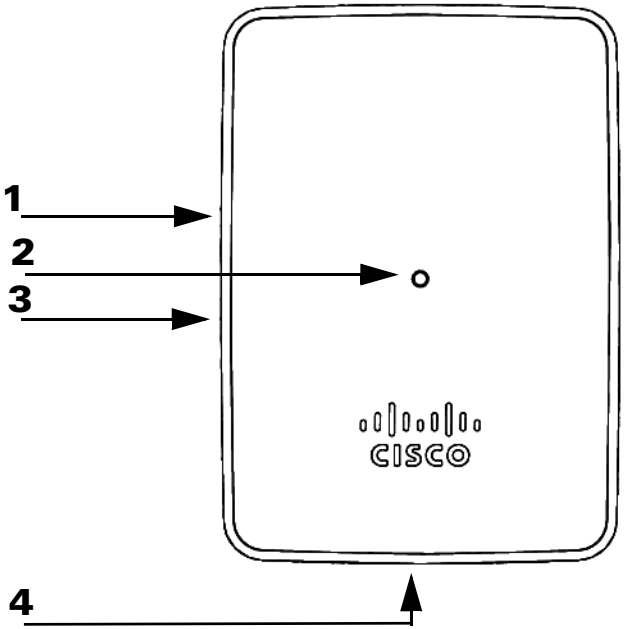
Step 2 Return any packing material to the shipping container and save it for future use.

Step 3 Verify that you have received the items listed below. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

- The access point.
- Mounting bracket AIR-AP-BRACKET-NS.

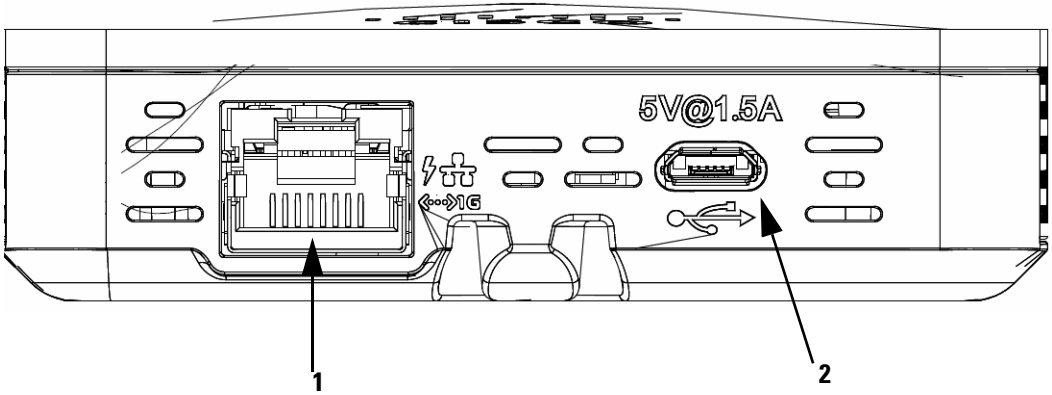
5 Ports and Connectors on the AP

Figure 1 Access Point Status LED and Ports Location



1	Reset button, on the right side of the AP. For information on how to use the Reset button, see "Using the Reset Button" section on page 21.
2	Status LED. For more information, see the "Access Point Status LED" section on page 19
3	Kensington security lock slot, on the right side of the AP.
4	USB port and the PoE port (Gigabit Ethernet uplink port), on the base of the AP.

Figure 2 Power-over-Ethernet and USB Ports on the Base



1	10/100/1000 BASE-T (Ethernet) Uplink Interface with inline power capability, Auto-MDIX (automatically support either straight through or crossover cables), and 802.3af/at PoE-In	**2**	USB port for powering the AP, using 5V, 1.5A power.

6 Preparing the AP for Installation

Before you mount and deploy your access point, we recommend that you perform a site survey (or use the site planning tool) to determine the best location to install your access point.

You should have the following information about your wireless network available:

- Access point locations.
- Access point mounting options: vertically oriented, on a wall or a desk.
- Powered by 802.3af or 802.3at, through PoE from a network device or a PoE power injector or hub (usually located in a wiring closet).

Note Access points mounted in a building's environmental airspace must be powered using PoE to comply with safety regulations.

Cisco recommends that you make a site map showing access point locations so that you can record the device MAC addresses from each location and return them to the person who is planning or managing your wireless network.

7 Installation Overview

Installing the access point involves these operations:

Step 1 Performing a Pre-Installation Configuration, page 10 (optional)

Step 2 Mounting and Powering the Access Point, page 13

Step 3 Configuring and Deploying the Access Point, page 16

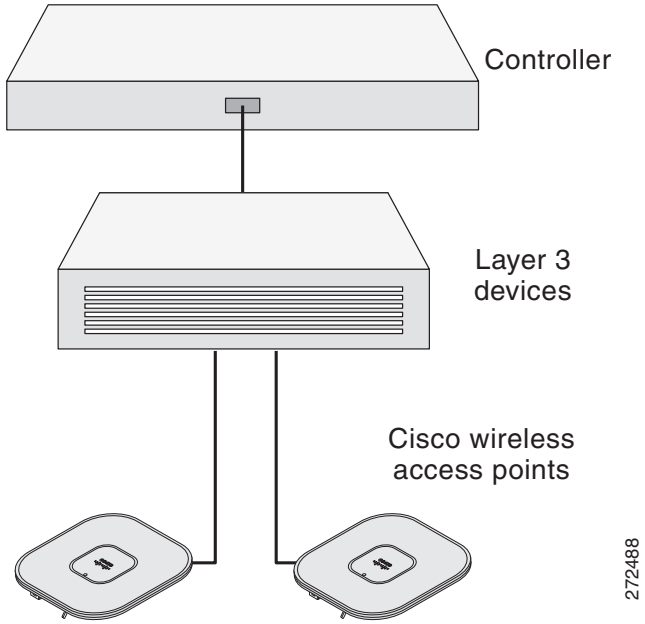
8 Performing a Pre-Installation Configuration

The following procedures ensure that your access point installation and initial operation go as expected. This procedure is optional.

Note Performing a pre-installation configuration is an optional procedure. If your network controller is properly configured, you can install your access point in its final location and connect it to the network from there. See the "Deploying the Access Point on the Wireless Network" section on page 18 for details.

The pre-installation configuration setup is illustrated in Figure 3.

Figure 3 Pre-Installation Configuration Setup



To perform pre-installation configuration, perform the following steps:

Step 1 Make sure that the Cisco wireless LAN controller DS port is connected to the network. Use the CLI, web-browser interface, or Cisco Prime Infrastructure procedures as described in the appropriate Cisco wireless LAN controller guide.

a. Make sure that access points have Layer 3 connectivity to the Cisco wireless LAN controller Management and AP-Manager Interface.

b. Configure the switch to which your access point is to attach. See the *Cisco Wireless LAN Controller Configuration Guide* for the release you are using, for additional information.

c. Set the Cisco wireless LAN controller as the master so that new access points always join with it.

d. Make sure DHCP is enabled on the network. The access point must receive its IP address through DHCP.

e. CAPWAP UDP ports must not be blocked in the network.

f. The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the "Configuring DHCP Option 43" section on page 24 for more information.

Note The access point requires a Gigabit Ethernet (GbE) link to prevent the Ethernet port from becoming a bottleneck for traffic because wireless traffic speeds exceed transmit speeds of a 10/100 Ethernet port.

Step 2 Apply power to the access point.

a. As the access point attempts to connect to the controller, the LED cycles through a green, red, and amber sequence, which can take up to 5 minutes.

Note If the access point remains in this mode for more than five minutes, the access point is unable to find the Master Cisco wireless LAN controller. Check the connection between the access point and the Cisco wireless LAN controller and be sure that they are on the same subnet.

b. If the access point shuts down, check the power source.

c. After the access point finds the Cisco wireless LAN controller, it attempts to download the new operating system code if the access point code version differs from the Cisco wireless LAN controller code version. While this is happening, the Status LED blinks amber.

d. If the operating system download is successful, the access point reboots.

Step 3 Configure the access point if required. Use the controller CLI, controller GUI, or Cisco Prime Infrastructure to customize the access-point-specific 802.11ac network settings.

Step 4 If the pre-installation configuration is successful, the Status LED is green indicating normal operation. Disconnect the access point and mount it at the location at which you intend to deploy it on the wireless network.

Step 5 If your access point does not indicate normal operation, turn it off and repeat the pre-installation configuration.

Note When you are installing a Layer 3 access point on a different subnet than the Cisco wireless LAN controller, be sure that a DHCP server is reachable from the subnet on which you will be installing the access point, and that the subnet has a route back to the Cisco wireless LAN controller. Also be sure that the route back to the Cisco wireless LAN controller has destination UDP ports 5246 and 5247 open for CAPWAP communications. Ensure that the route back to the primary, secondary, and tertiary wireless LAN controller allows IP packet fragments. Finally, be sure that if address translation is used, that the access point and the Cisco wireless LAN controller have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)

9 Mounting and Powering the Access Point

The Cisco Aironet 1800i series access points can be mounted, in a vertical orientation, on a wall or desk, to a height of 3 feet. The mounting is done using the wall-mount bracket AIR-AP-BRACKET-NS.

To mount the AP on a wall or desk:

Step 1 Identify the location for mounting the AP.

Step 2 Use the wall-mount bracket AIR-AP-BRACKET-NS, as a template to mark the two screw-hole locations for fastening the bracket to the wall or desk.

Step 3 At the marked locations, drill a hole into the wall or desk.

Step 4 Fasten the AIR-AP-BRACKET-NS to the wall using two 18mm screws.

Step 5 Hold the back of the AP against the wall, above the bracket, and then slide the AP down onto the bracket, till it clicks into place. The hooks on the bracket will click into the recesses on the back of the AP.

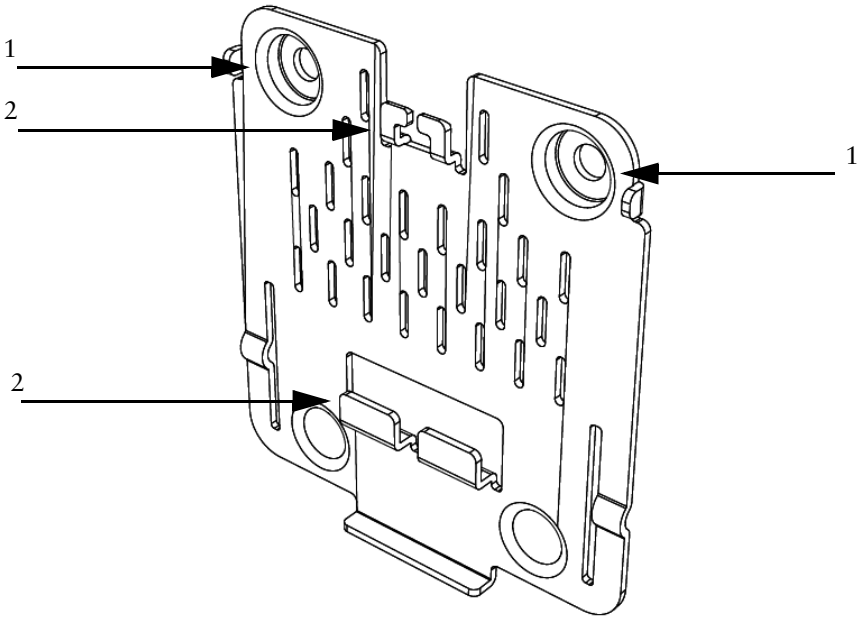
Step 6 Proceed with connecting the data and power cables.

The AP can be powered using:

- AC power, using the AC-USB adapter AIR-MOD-USB, supplying 5V DC, 1.5A power.
- PoE, 802.3af Class 0 power or greater, from:
  - a network device or power injector.
  - Cisco power injectors AIR-PWRINJ5 (for 802.3af) or AIR-PWRINJ6 (for 802.3at).

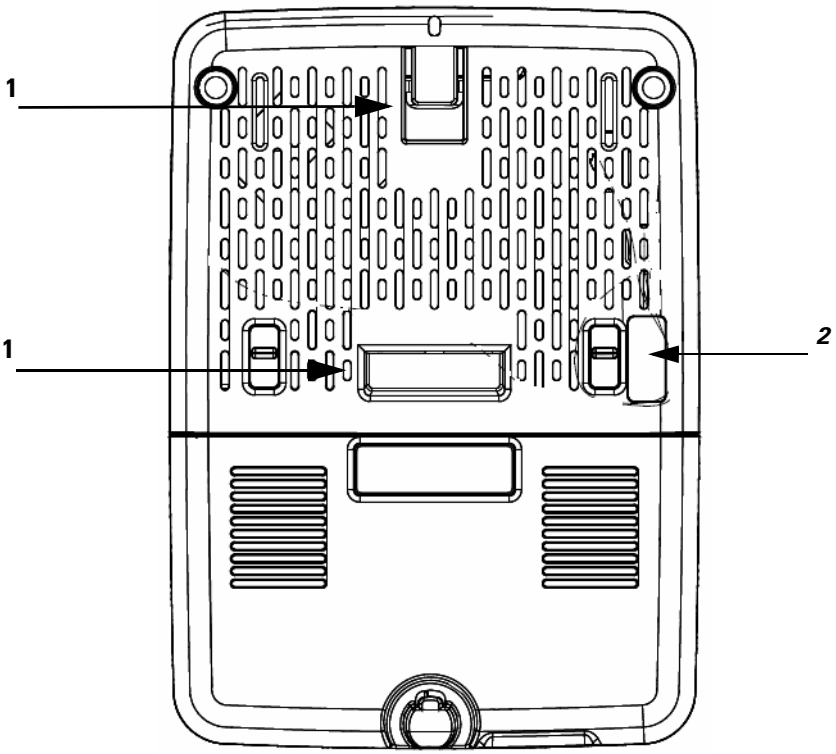
The PoE and USB ports are located on the base of the AP. When both AC power and PoE power is available, the PoE power takes precedence.

Figure 4 Wall and Desk Mounting Bracket AIR-AP-BRACKET-NS



1	Screw holes for fastening the bracket to the wall or desk.	**2**	Hooks which click into the recesses on the back the AP, for mounting the AP on the bracket.

Figure 5 Back of the AP



1	Recesses on the back of the AP into which the hooks on the wall-mount bracket slide and click into place.	**2**	RS-232 console interface port, hidden under a mylar label. You need to use the custom console cable AIR-MOD-UART-xx.

10 Configuring and Deploying the Access Point

This section describes how to connect the access point to a wireless LAN controller. The configuration process takes place on the controller. See the *Cisco Wireless LAN Controller Configuration Guide* for additional information.

The Controller Discovery Process

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, inter-operable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Note For additional information about the discovery process and CAPWAP, see the *Cisco Wireless LAN Controller Software Configuration Guide*. This document is available on Cisco.com.

Note CAPWAP support is provided in controller software release 5.2 or later. However, your controller must be running the release that supports 1800i series access points, as specified in the access point's data sheet.

Note You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

Note Make sure that the controller is set to the current time. If the controller is set to a time that has already passed, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- **Layer 3 CAPWAP discovery**—Can occur on different subnets than the access point and uses IP addresses and UDP packets rather than MAC addresses used by Layer 2 discovery.
- **Locally stored controller IP address discovery**—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called *priming the access point*. For more information about priming, see the "Performing a Pre-Installation Configuration" section on page 10.
- **DHCP server discovery**—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43" section on page 24.
- **DNS discovery**—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Deploying the Access Point on the Wireless Network

After you have mounted the access point, follow these steps to deploy it on the wireless network:

Step 1 Connect and power up the access point.

Step 2 Observe the access point LED (for LED descriptions, see "Checking the Access Point LED" section on page 19).

- **a.** When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks sequentially green, red, and off. When the access point has joined a controller, the LED is chirping green if no clients are associated or green if one or more clients are associated.
- **b.** If the LED is not on, the access point is most likely not receiving power.
- **c.** If the LED blinks sequentially for more than 5 minutes, the access point is unable to find its primary, secondary, and tertiary Cisco wireless LAN controller. Check the connection between the access point and the Cisco wireless LAN controller, and be sure the access point and the Cisco wireless LAN controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco wireless LAN controller. Also, if the access point is not on the same subnet as the Cisco wireless LAN controller, be sure that there is a properly configured DHCP server on the same subnet as the access point. See the "Configuring DHCP Option 43" section on page 24 for additional information.

Step 3 Reconfigure the Cisco wireless LAN controller so that it is not the Master.

Note A Master Cisco wireless LAN controller should be used only for configuring access points and not in a working network.

11 Checking the Access Point LED

Access Point Status LED

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

The access point status LED indicates various conditions which are described in Table 1.

Table 1 LED Status Indications

Message Type	LED State	Message Meaning
Boot loader status sequence	Blinking Green	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 the Cisco AP-OS operating system of the AP
		Initialization successful
Association status	Chirping Green (Chirping means shorter blips of the LED that are distinctly different from a blinking LED.)	Normal operating condition, but no wireless client associated
	Green	Normal operating condition with at least one wireless client association

Table 1 LED Status Indications (continued)

Message Type	LED State	Message Meaning
Operating status	Blinking Amber	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.	Access point location command invoked from controller web interface.
	Blinking Red	Ethernet link is not operational.
Boot loader warnings	Blinking Amber	Configuration recovery in progress (Reset button pushed for 2 to 3 seconds)
	Red	Ethernet failure or image recovery (Reset button pushed for 20 to 30 seconds)
	Blinking Green	Image recovery in progress (Reset button released)
Boot loader errors	Blinking Red-Red-Off	DRAM memory test failure
	Blinking Red and Amber	FLASH file system failure
	Blinking Red and off	One of the following: • Environment variable failure • Bad MAC address • Ethernet failure during image recovery • Boot environment failure • No Cisco image file • Boot failure
Cisco Access Point Operating System (AP-OS) errors	Blinking Red-Red-Red-Red-Off	Software failure; try disconnecting and reconnecting unit power
	Cycling through Red, Green, Amber and off.	General warning; insufficient inline power

Ethernet Port LEDs

The Ethernet port has two LEDs for showing Link (Green) and Activity (Amber) statuses. They are integrated on the RJ45 connector. For a description of the statuses they indicate, see the following table.

	10M Link	10M Active	100M Link	100M Active	1000M Link	1000M Active
Link (Green) LED State	Off	Off	Off	Off	On	On
Activity (Amber) LED State	On	Blinking	On	Blinking	On	Blinking

12 Miscellaneous Usage and Configuration Guidelines

Using the Reset Button

Using the Reset button you can:

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

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 the 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, encryption keys, the IP address, and the SSID. However, the regulatory domain provisioning is not reset.
- 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.

Troubleshooting the Access Point to Cisco Controller Join Process

Note Ensure that your controller is running the latest Cisco Wireless Controller Software Release as specified in the access point's data sheet.

Access points can fail to join a controller for many reasons: a RADIUS authorization is pending; self-signed certificates are not enabled on the controller; the access point's and controller's regulatory domains don't match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point. Therefore, it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining problems without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to it and maintains information for any access points that have successfully joined it.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

You can view join-related information for up to three times the maximum number of access points supported by the platform for the 2500 series controllers and the Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers.

Note The maximum number of access points varies for the Cisco WiSM2, depending on which controller software release is being used.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default when any of the following conditions are met:

- An access point running software release 8.0.x.x or later has been newly deployed.

- An existing access point running software release 8.0.x.x or later has been reset after clearing the configuration.

If any of these conditions are met and the access point has not yet joined a controller, you can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global syslog_server_IP_address** command. In this case, the controller sends the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific Cisco_AP syslog_server_IP_address** command. In this case, the controller sends the new specific syslog server IP address to the access point.
- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points and view the access point join information only from the controller CLI.

Important Information for Controller-based Deployments

Keep these guidelines in mind when you use 1800i series access points:

- The access point can only communicate with Cisco wireless LAN controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

Configuring DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling them to find and join a controller.

The following is a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Aironet lightweight access points. For other DHCP server implementations, consult product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

The 1800i series access point uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the 1800i access point is:

Cisco AP c1800i

The format of the TLV block is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
<pool name> is the name of the DHCP pool, such as AP1800i
<IP Network> is the network IP address where the controller resides, such as
10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 43 line using the following syntax:

option 43 hex *<hex string>*

The *hex string* is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.

13 Related Documentation

All user documentation for the Cisco Aironet 1800i series access point is available at the following URL:

(To be added at FCS)

For detailed information and guidelines for configuring and deploying your access point in a wireless network, see the *Cisco Wireless LAN Controller Configuration Guide*, at the following URL:

(To be added at FCS)

14 Declarations of Conformity and Regulatory Information

This section provides declarations of conformity and regulatory information for the Cisco Aironet 1800i Access Point. You can find additional information at this URL:

www.cisco.com/go/aironet/compliance

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Tested To Comply
With FCC Standards

FOR HOME OR OFFICE USE

Access Point Models	Certification Number
AIR-AP1800I-B-K9	LDK102112

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 the integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

VCCI Statement for Japan

Warning

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

警告 この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

ＶＣＣＩ－Ｂ

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.

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

208697

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

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 adaptors. Using any other cables/adaptors 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.

Industry Canada

Access Point Models	Certification Number
AIR-AP1800I-A-K9	2461B-102112

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	3/5dBi	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.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Access Point Models:

AIR-AP1800I-E-K9

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

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 asi 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.

Nederlands [Dutch]:	**Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.**
Malti [Maltese]:	**Dan l-apparat huwa konformi mal-ħtiġiet 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.**
Română [Romanian]	**Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 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 direktív: 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.**
Türk [Turkish]	**Bu cihaz 1999/5/EC Direktifi'nin temel gereklerine ve ilgili diğer hükümlerine uygundur.**

142730

The following standards were applied:

EMC—EN 301.489-1 v1.9.2; EN 301.489-17 v2.2.1

Health & Safety—EN60950-1: 2006; EN 50385: 2002

Radio—EN 300 328 v 1.8.1; EN 301.893 v 1.7.1

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

This section contains information on compliance with guidelines related to RF exposure.

Generic Discussion on RF Exposure

The Cisco products are designed to comply with the following national and international standards on Human Exposure to Radio Frequencies:

- US 47 Code of Federal Regulations Part 2 Subpart J
- American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1 (99)
- International Commission on Non Ionizing Radiation Protection (ICNIRP) 98
- Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz
- Australia Radiation Protection Standard

To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco approved accessories.

This Device Meets International Guidelines for Exposure to Radio Waves

The 1800i access point device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by an independent scientific organization (ICNIRP) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

Separation Distance		
MPE	Distance	Limit
0.06 mW/cm^2	20 cm (7.87 inches)	1.00 mW/cm^2

The World Health Organization has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing he antennas at a greater separation distance then recommended.

This Device Meets FCC Guidelines for Exposure to Radio Waves

The 1800i access point device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in FCC Part 1.1310. The guidelines are based on IEEE ANSI C 95.1 (92) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

Separation Distance		
MPE	Distance	Limit
0.06 mW/cm^2	20 cm (7.87 inches)	1.00 mW/cm^2

The US Food and Drug Administration has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. The FCC recommends that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing the antennas at a greater separation distance then recommended or lowering the transmitter power output.

This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves

The 1800i access point device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in Health Canada Safety Code 6. The guidelines include a substantial safety margin designed into the limit to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

Separation Distance			
Frequency	MPE	Distance	Limit
2.4 GHz	0.17 W/m^2	20 cm (7.87 inches)	5.4 W/m^2
5 GHz	0.66 W/m^2		9.2 W/m^2

Health Canada states that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure you can easily do so by reorienting antennas away from the user, placing the antennas at a greater separation distance than recommended, or lowering the transmitter power output.

Cet appareil est conforme aux directives internationales en matière d'exposition aux fréquences radioélectriques

Cet appareil de la gamme 1800i comprend un émetteur-récepteur radio. Il a été conçu de manière à respecter les limites en matière d'exposition aux fréquences radioélectriques (champs électromagnétiques de fréquence radio), recommandées dans le code de sécurité 6 de Santé Canada. Ces directives intègrent une marge de sécurité importante destinée à assurer la sécurité de tous, indépendamment de l'âge et de la santé.

Par conséquent, les systèmes sont conçus pour être exploités en évitant que l'utilisateur n'entre en contact avec les antennes. Il est recommandé de poser le système là où les antennes sont à une distance minimale telle que précisée par l'utilisateur conformément aux directives réglementaires qui sont conçues pour réduire l'exposition générale de l'utilisateur ou de l'opérateur.

Distance d'éloignement			
Fréquence	MPE	Distance	Limite
2.4 GHz	0.17 W/m^2	20 cm (7.87 inches)	5.4 W/m^2
5 GHz	0.66 W/m^2		9.2 W/m^2

Santé Canada affirme que la littérature scientifique actuelle n'indique pas qu'il faille prendre des précautions particulières lors de l'utilisation d'un appareil sans fil. Si vous voulez réduire votre exposition encore davantage, selon l'agence, vous pouvez facilement le faire en réorientant les antennes afin qu'elles soient dirigées à l'écart de l'utilisateur, en les plaçant à une distance d'éloignement supérieure à celle recommandée ou en réduisant la puissance de sortie de l'émetteur.

Additional Information on RF Exposure

You can find additional information on the subject at the following links:

- Cisco Systems Spread Spectrum Radios and RF Safety white paper at this URL: http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm
- FCC Bulletin 56: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
- FCC Bulletin 65: Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields

You can obtain additional information from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection at this URL: www.who.int/emf
- United Kingdom, National Radiological Protection Board at this URL: www.nrpb.org.uk
- Cellular Telecommunications Association at this URL: www.wow-com.com
- The Mobile Manufacturers Forum at this URL: www.mmfai.org

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operating Cisco Aironet access points in Taiwan. The rules for all access points are provided in both Chinese and English.

Chinese Translation

<u>低功率電波輻射性電機管理辦法</u>

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

<u>低功率射頻電機技術規範</u>

4.7 無線資訊傳輸設備

4.7.5 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

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。

202591

English Translation

Low-power Radio-frequency Devices Technical Specifications

4.7 Unlicensed National Information Infrastructure

4.7.5 Within the 5.25-5.35 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

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.

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-AP1800I-Z-K9

Figure 6 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.

Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following location: http://www.ciscofax.com

15 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

© 2017 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)