



## **Cisco Aironet 1000 Series Lightweight Access Point Hardware Installation Guide**

April 2007

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-9403-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A 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 commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.



# CONTENTS

## **Preface** vii

Audience vii

Purpose vii

Organization vii

Conventions viii

Related Publications x

Finding the Product Serial Number xi

Obtaining Documentation, Obtaining Support, and Security Guidelines xii

---

## **CHAPTER 1**

### **Overview** 1-1

Guidelines for Using the Access Points 1-2

Hardware Features 1-2

    Single or Dual-Radio Operation 1-4

    Antennas Supported 1-4

    Ethernet Port 1-5

    LEDs 1-5

    Power Sources 1-5

    UL 2043 Certification 1-6

    Anti-Theft Features 1-6

Network Configuration Example 1-7

---

## **CHAPTER 2**

### **Installing the Access Point** 2-1

Safety Information 2-2

- FCC Safety Compliance Statement 2-2
- General Safety Guidelines 2-2
- Warnings 2-2
- Unpacking the Access Point 2-3
  - Package Contents 2-3
- Basic Installation Guidelines 2-3
- Before Beginning the Installation 2-4
  - Access Point Layout and Connectors 2-5
- Controller Discovery Process 2-6
- Deploying the Access Points on the Wireless Network 2-7
- Mounting Overview 2-8
  - Mounting Access Points Using a Ceiling-Mount Base 2-10
  - Mounting Access Points Using the Ceiling-Mount Clips 2-11
  - Mounting the Access Point Using a Projection Wall Mount Bracket 2-13
  - Mounting the Access Point Using the Flush-Mount Bracket 2-15
- Securing the Access Point Using a Security Cable 2-17
- Connecting the Ethernet and Power Cables 2-17
  - Connecting to an Ethernet Network with an Inline Power Source 2-18
  - Connecting to an Ethernet Network with Local Power 2-19
- Powering Up the Access Point 2-19
- Returning MAC Information 2-20

**CHAPTER 3**

**Troubleshooting 3-1**

- Guidelines for Using the Access Points 3-2
- Using DHCP Option 43 3-2
- Checking the Access Point LEDs 3-3
- Low Power Condition 3-5

---

**APPENDIX A****Translated Safety Warnings A-1**

---

**APPENDIX B****Declarations of Conformity and Regulatory Information B-1**

Manufacturers Federal Communication Commission Declaration of Conformity Statement **B-2**

VCCI Statement for Japan **B-3**

Department of Communications—Canada **B-4**

Canadian Compliance Statement **B-4**

European Community, Switzerland, Norway, Iceland, and Liechtenstein **B-5**

Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive) **B-5**

Declaration of Conformity for RF Exposure **B-7**

Guidelines for Operating Cisco Aironet Access Points in Japan **B-8**

Japanese Translation **B-8**

English Translation **B-8**

Administrative Rules for Cisco Aironet Access Points in Taiwan **B-9**

Access Points with IEEE 802.11a Radios **B-9**

Chinese Translation **B-9**

English Translation **B-9**

All Access Points **B-10**

Chinese Translation **B-10**

English Translation **B-10**

Declaration of Conformity Statements **B-11**

Declaration of Conformity Statements for European Union Countries **B-11**

---

**APPENDIX C**      **Access Point Specifications**   C-1

---

**APPENDIX D**      **Channels and Power Levels**   D-1

---

**APPENDIX E**      **Priming Access Points Prior to Deployment**   E-1

---

**APPENDIX F**      **Configuring DHCP Option 43**   F-1

    Overview   F-2

    Configuring Option 43 for 1000 Series Access Points   F-3

    Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Access Points   F-4



## Preface

---

### Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1000 Series Lightweight Access Point, hereafter referred to as the *access point*. These access points are part of the Cisco Integrated Wireless Network Solution and require no manual configuration before they are mounted. The access point is automatically configured by a Cisco Wireless LAN Controller using the Lightweight Access Point Protocol (LWAPP).

To use this guide, you should have experience working with a Cisco Wireless LAN Controller and be familiar with the concepts and terminology of wireless local area networks.

### Purpose

This guide provides the information you need to install your access point. For information about the Cisco Wireless LAN Controllers, refer to the Cisco documentation sets available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Wireless** and the documentation is listed under the “Wireless LAN Controllers” section.

### Organization

This guide is organized into these chapters:

[Chapter 1, “Overview,”](#) lists the software and hardware features of the access point and describes the access point’s role in your network.

[Chapter 2, “Installing the Access Point,”](#) describes how to mount the access point on a desktop, wall, or ceiling, how to connect Ethernet, serial, and power cables, and provides an installation summary, safety warnings, and general guidelines.

[Chapter 3, “Troubleshooting,”](#) provides troubleshooting procedures for basic problems with the access point.

[Appendix A, “Translated Safety Warnings,”](#) indicates how to access the document that provides translations of the safety warnings that appear in this publication.

[Appendix B, “Declarations of Conformity and Regulatory Information,”](#) provides declarations of conformity and regulatory information for the access point.

[Appendix C, “Access Point Specifications,”](#) lists technical specifications for the access point.

[Appendix D, “Channels and Power Levels,”](#) indicates how to access the document that lists the access point radio channels and the maximum power levels supported by the world’s regulatory domains.

[Appendix E, “Priming Access Points Prior to Deployment,”](#) describes the procedure to pre-configure an access point with IP addresses and controller information.

[Appendix F, “Configuring DHCP Option 43,”](#) describes the procedure to configure DHCP Option 43.

## Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ( { } ) group required choices, and vertical bars ( | ) separate the alternative elements.
- Braces and vertical bars within square brackets ( [ { | } ] ) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (<>).

Notes, cautions, and timesavers use these conventions and symbols:



**Tip**

---

Means the following will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information.

---



**Note**

---

Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

---



**Caution**

---

Means reader be careful. In this situation, you might do something that could result equipment damage or loss of data.

---



**Warning**

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. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)

**Waarschuwing**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)

**Varoitus**

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä “Translated Safety Warnings” (käännetyt turvallisuutta koskevat varoitukset).)

**Attention**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).

**Warnung**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel “Translated Safety Warnings” (Übersetzung der Warnhinweise).)

**Avvertenza**

Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, “Translated Safety Warnings” (Traduzione delle avvertenze di sicurezza).

**Advarsel**

Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget “Translated Safety Warnings” [Oversatte sikkerhetsadvarsler].)

**Aviso**

Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice “Translated Safety Warnings” - “Traduções dos Avisos de Segurança”).

<b>¡Advertencia!</b>	<b>Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado “Translated Safety Warnings.”)</b>
<b>Varning!</b>	<b>Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)</b>

---

## Related Publications

These documents provide complete information about the access point:

These documents provide complete information about the outdoor access point:

- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*
- *Quick Start: Cisco Aironet 1000 Series Lightweight Outdoor Mesh Access Point*
- *Cisco Wireless LAN Controller Configuration Guide*

Click this link to browse to the Cisco Wireless documentation home page:

[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)

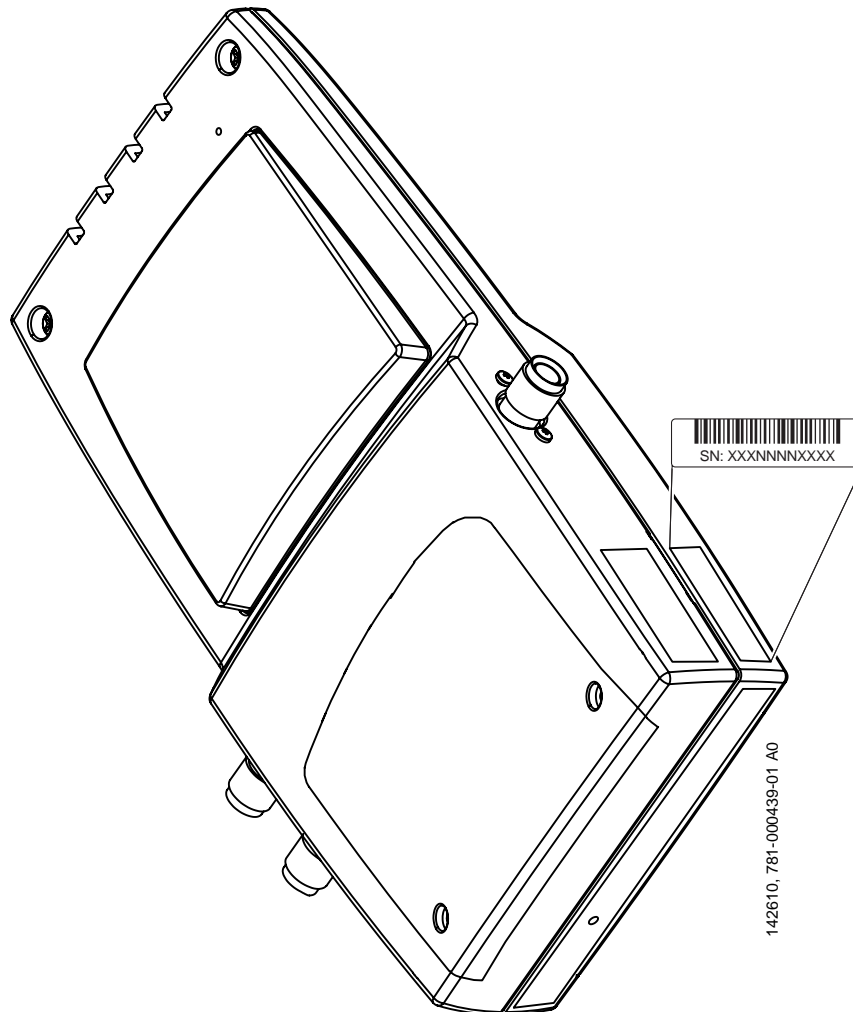
To browse to the 1000 series access point documentation, click **Cisco Aironet 1000 Series** listed under “Access Points.”

To browse to the Cisco Wireless LAN Controller documentation, click **Cisco 4400 Series Wireless LAN Controllers** or **Cisco 2000 Series Wireless LAN Controllers** listed under “Wireless LAN Controllers.”

# Finding the Product Serial Number

The access point serial number is on the right side of the housing (refer to [Figure 1](#)).

**Figure 1** Location of Serial Number Label



The access point serial number label contains the following information:

- Model number, such as *AIR-AP1000-x-k9*
- Serial number, such as *VDF0636XXXX* (11 alphanumeric digits)
- MAC address, such as *00abc65094f3* (12 hexadecimal digits)
- Location of manufacture, such as *Made in Singapore*

You need your product serial number when requesting support from the Cisco Technical Assistance Center.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



# CHAPTER 1

## Overview

---

The Cisco Aironet 1000 Series Lightweight Access Points (hereafter called *access points*) combine mobility and flexibility with the enterprise-class features required by networking professionals. These access points are part of the Cisco Integrated Wireless Network Solution and require no manual configuration before they are mounted. The access point is automatically configured by a Cisco Wireless LAN Controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

The access point contains two integrated radios: a 2.4-GHz radio (IEEE 802.11g) and a 5-GHz radio (IEEE 802.11a). Using a controller, you can configure the radios separately with different settings on each.

In the Cisco Centralized Wireless LAN Architecture, access points operate in the lightweight mode (as opposed to autonomous mode). The access points associate to a controller. The controller manages the configuration, firmware, and control transactions such as 802.1x authentication. In addition, all wireless traffic is tunneled through the controller.

LWAPP is an Internet Engineering Task Force (IETF) draft protocol that defines the control messaging for setup and path authentication and run-time operations. LWAPP also defines the tunneling mechanism for data traffic.

In an LWAPP environment, a lightweight access point discovers a controller by using LWAPP discovery mechanisms and then sends it an LWAPP join request. The controller sends the access point an LWAPP join response allowing the access point to join the controller. When the access point is associated with a controller, it downloads new operating system software if the versions on the access point and controller do not match. After an access point is associated to a controller, you are able to reassign it to any controller on your network.

LWAPP secures the control communication between the access point and controller by means of a secure key distribution, utilizing X.509 certificates on both the access point and controller.

This chapter provides information on the following topics:

- [Guidelines for Using the Access Points, page 1-2](#)
- [Hardware Features, page 1-2](#)
- [Network Configuration Example, page 1-7](#)

# Guidelines for Using the Access Points

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

- The access points can only communicate with controllers and can not operate independently.
- The access points communicate only with controllers and do not support Wireless Domain Services (WDS). The access points cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support Layer 2 or Layer 3 LWAPP communications with the controllers. In Layer 2 operation, the access point and the controller must be on the same subnet and communicate with each other using MAC addresses in encapsulated Ethernet frames. This operation is not scalable to larger networks and not recommended by Cisco.

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. Layer 3 operation is scalable and is recommended by Cisco. 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 LWAPP communications. The route to the primary, secondary, and tertiary controllers must allow IP packet fragments.

- Before deploying your access points ensure 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 is used to provide 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-LWAPP-CONTROLLER.<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.

## Hardware Features

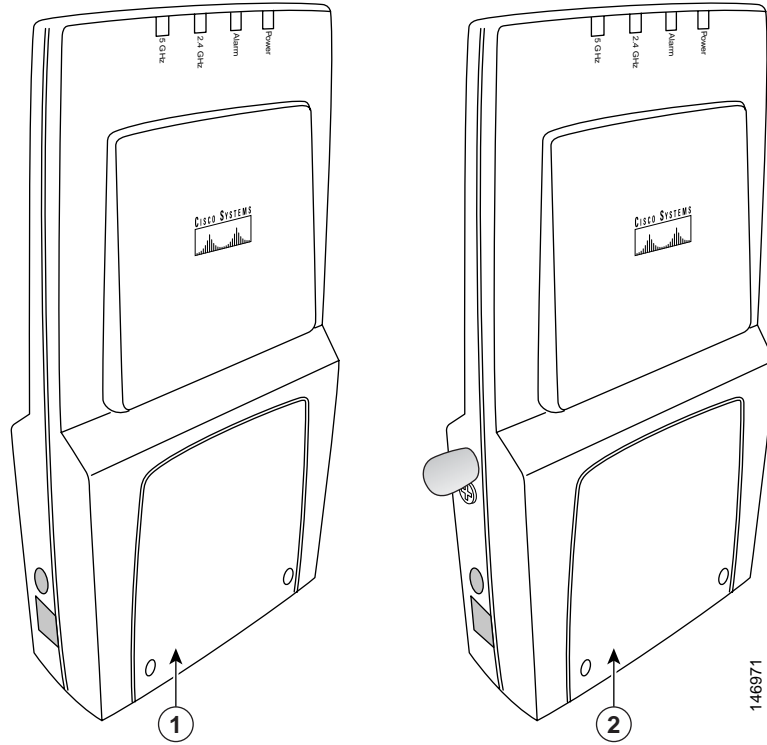
Key hardware features of the access point include:

- Single or dual-radio operation (see [page 1-4](#))
- Ethernet port (see [page 1-5](#))
- LEDs, (see [page 1-5](#))
- Multiple power sources (see [page 1-5](#))
- Anti-theft features (see [page 1-6](#))
- UL 2043 certification (see [page 1-6](#))

Refer to [Appendix C, “Access Point Specifications,”](#) for a list of access point specifications.

[Figure 1-2](#) shows the access point.

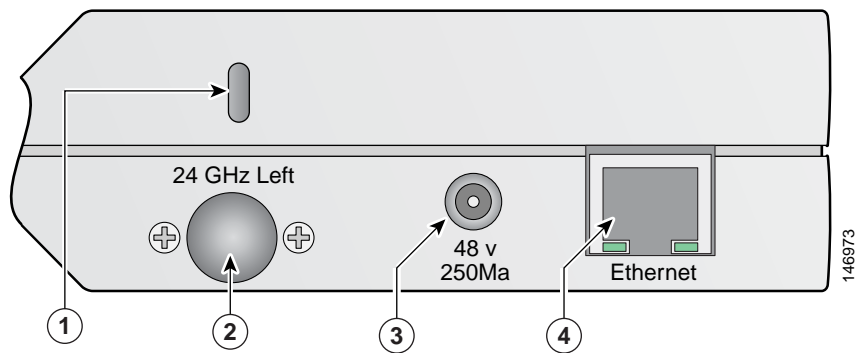
**Figure 1-1 Access Point Configurations**



<p><b>1</b> Integrated antennas only (AIR-AP1010)</p>	<p><b>2</b> Integrated antennas and external antenna connectors (AIR-AP1020 and AIR-AP1030)</p>
---	---

Figure 1-2 illustrates the left side connectors on the access point.

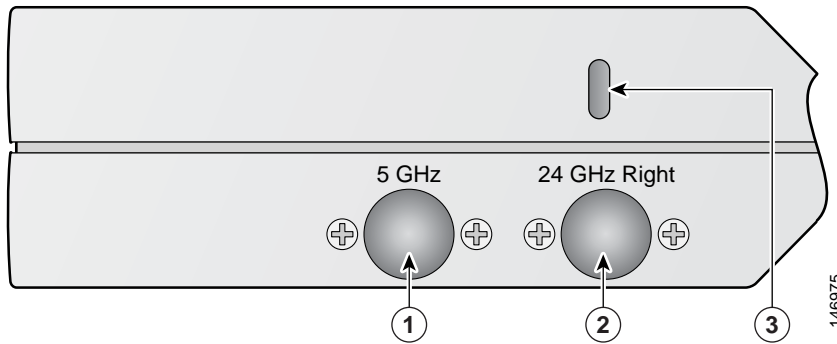
**Figure 1-2 Access Point Left Side Connectors**



<p><b>1</b> Security key slot</p> <p><b>2</b> 2.4-GHz antenna connector (left)</p>	<p><b>3</b> 48-VDC power port</p> <p><b>4</b> Ethernet port (RJ-45)</p>
--	---

Figure 1-3 illustrates the right side connectors on the access point.

**Figure 1-3 Access Point Right Side Connectors**



<b>1</b>	5-GHz antenna connector (right)	<b>3</b>	2.4-GHz antenna connector (right)
<b>2</b>	Security key slot		

### Single or Dual-Radio Operation

The access point supports single or simultaneous dual radio operation using a 2.4-GHz 802.11g radio and a 5-GHz 802.11a radio. The radios use integrated sector patch antennas or external antennas (see the “Antennas Supported” section).

The 5-GHz radio incorporates an Unlicensed National Information Infrastructure (UNII) radio transceiver operating in the UNII 5-GHz frequency bands.

### Antennas Supported

The access points are available in three configurations:

- AIR-AP1010—Supports only integrated antennas
- AIR-AP1020—Supports integrated and external antennas
- AIR-AP1030—Supports integrated and external antennas

The 2.4 GHz and 5 GHz radios have two integrated 6 dBi directional patch antennas. The integrated antennas provide diversity operation for the 2.4 GHz radio. The antennas are located on the front and back sides of the access point.



**Caution**

The access point, the antennas, and the power source (power injector or power module) are not designed for outdoor use and must be located in an indoor environment.



Table 1-1 lists the supported external antennas.

**Table 1-1 Supported External Antennas**

2.4-GHz Antennas	Gain (dBi)	5-GHz Antennas	Gain (dBi)
AIR-ANT5959 diversity omnidirectional	2.0	AIR-ANT5135D-R omnidirectional	3.5
AIR-ANT4941 dipole	2.2	AIR-ANT5160V-R omnidirectional	6.0
AIR-ANT1728 omnidirectional	5.2		
AIR-ANT2506 omnidirectional	5.2		
AIR-ANT3213 diversity omnidirectional	5.2		
AIR-ANT1729 patch	6.0		
AIR-ANT2012 diversity patch	6.5		

## Ethernet Port

The auto-sensing Ethernet port accepts an RJ-45 connector, linking the access point to your 10BASE-T or 100BASE-T Ethernet LAN (see [Figure 1-2](#)). The access point can receive power through the Ethernet cable from a power injector, switch, or power patch panel. The Ethernet MAC address is printed on the label on the side of the access point (refer to the [“Finding the Product Serial Number”](#) section on [page xi](#)).

## LEDs

The access point has four LEDs to provide a visual indication of access point operations (refer to the [“Checking the Access Point LEDs”](#) section on [page 3-3](#) for additional information).

- Power LED
- Alarm LED
- 2.4 GHz LED
- 5 GHz LED

## Power Sources

The access point can receive power from an external power module or from inline power using the Ethernet cable. The access point supports the IEEE 802.3af inline power standard. Using inline power, you do not need to run a power cord to the access point because power is supplied over the Ethernet cable.



**Warning**

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

The access point supports the following power sources:

- Power module (AIR-PWR-1000=)
- Inline power:
  - Cisco Aironet 1000 series access point power injector (AIR-PWRINJ-1000AF=)
  - An inline power capable switch, such as the Cisco Catalyst 3550 PWR XL, 3560-48PS, 3570-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
  - Other inline power switches supporting the IEEE 802.3af inline power standard


**Note**

The access point requires 12 W of inline power. Some switches and patch panels might not provide enough power to operate the access point. If the access point is unable to determine that the power source can supply sufficient power, the access point does not activate the radios and does not turn on the Power LED.

## UL 2043 Certification

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


**Caution**

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


**Caution**

The external antennas, the power injector (AIR-PWRINJ-1000AF=) and the power module (AIR-PWR-1000=) are not tested to UL 2043 and should not be placed in a building's environmental air space.


**Caution**

The Ethernet cables to your access points must be rated for above the ceiling mounting.

## Anti-Theft Features

The access point supports two security cable keyholes (see [Figure 1-2](#) and [Figure 1-3](#)) to secure the access point using a standard security cable, like those used on laptop computers.

# Network Configuration Example

The access points support Layer 2 or Layer 3 network operation. In Layer 2 configurations, the access point and the controller are on the same subnet and communicate with encapsulated Ethernet frames using MAC addresses rather than IP addresses. Layer 2 configurations are typically not scalable into larger networks. Additionally, Layer 2 operation is supported only by the Cisco 4400 series controllers.

Access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco.

Figure 1-4 illustrates a typical Layer 3 wireless network configuration containing access points and a controller.

**Figure 1-4** Typical Layer 3 Access Point Network Configuration Example

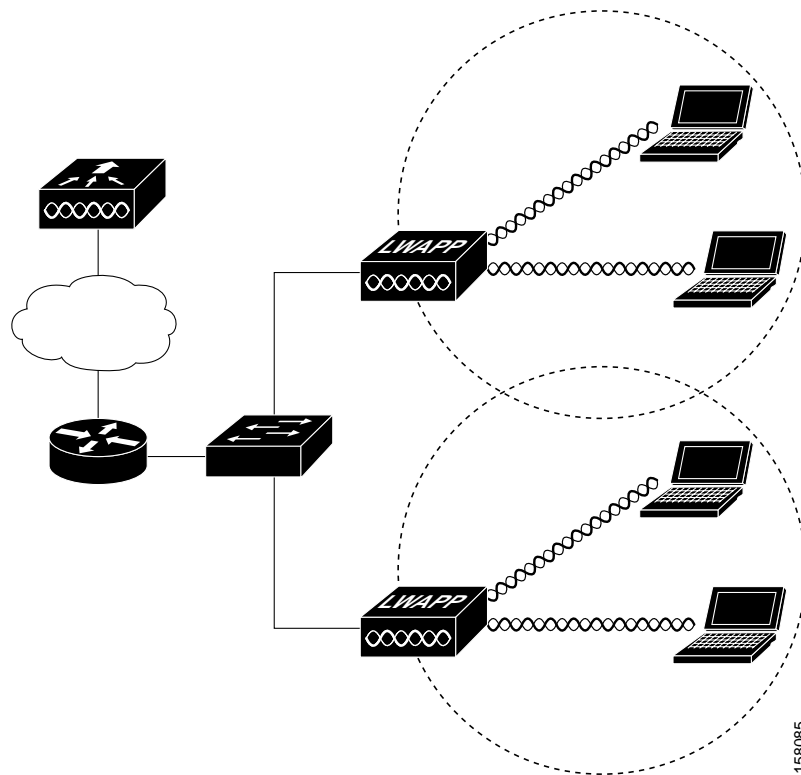
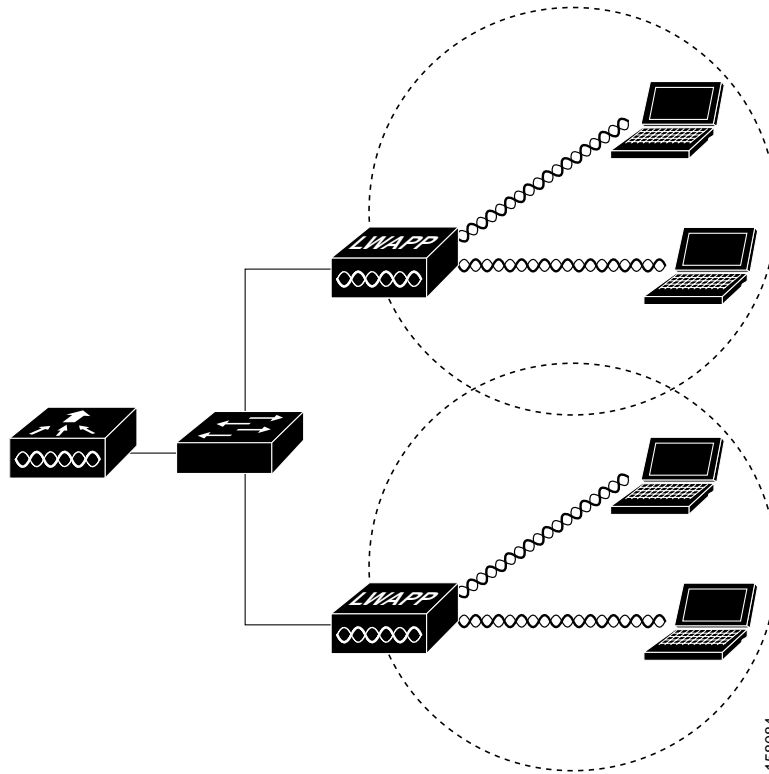


Figure 1-5 illustrates a typical Layer 2 network configuration. In a Layer 2 configuration, the controller and the access points are on the same subnet.

**Figure 1-5** Typical Layer 2 Access Point Network Configuration Example



158084



## CHAPTER 2

# Installing the Access Point

---

This chapter describes the installation of the access point and includes these sections:

- [Safety Information, page 2-2](#)
- [Warnings, page 2-2](#)
- [Unpacking the Access Point, page 2-3](#)
- [Basic Installation Guidelines, page 2-3](#)
- [Before Beginning the Installation, page 2-4](#)
- [Controller Discovery Process, page 2-6](#)
- [Controller Discovery Process, page 2-6](#)
- [Mounting Overview, page 2-8](#)
- [Securing the Access Point Using a Security Cable, page 2-17](#)
- [Connecting the Ethernet and Power Cables, page 2-17](#)
- [Powering Up the Access Point, page 2-19](#)
- [Returning MAC Information, page 2-20](#)

# Safety Information

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

## FCC Safety Compliance Statement

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper installation of this radio according to the instructions found in this manual will result in user exposure that is substantially below the FCC recommended limits.

## General Safety Guidelines

Do not hold any component containing a radio so that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.

## Warnings

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



Warning

**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

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

Statement 245B



Warning

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



Warning

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



Warning

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

**Warning**

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

## Unpacking the Access Point

Follow these steps to unpack the access point:

- 
- Step 1** Open the shipping container and carefully remove the contents.
  - Step 2** Return all packing materials to the shipping container and save it.
  - Step 3** Ensure that all items listed in the “Package Contents” section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized Cisco sales representative.
- 

## Package Contents

Each access point package contains the following items:

- Cisco Aironet 1000 series lightweight access point
- Ceiling mount kit (ceiling-mount base, two ceiling-mount clips, two screws, and two washers)
- *Quick Start Guide: Cisco Aironet 1000 Series Lightweight Access Points*
- *Translated Safety Warnings for Cisco Aironet 1000 Series Lightweight Access Points*
- Cisco product registration and Cisco documentation feedback cards

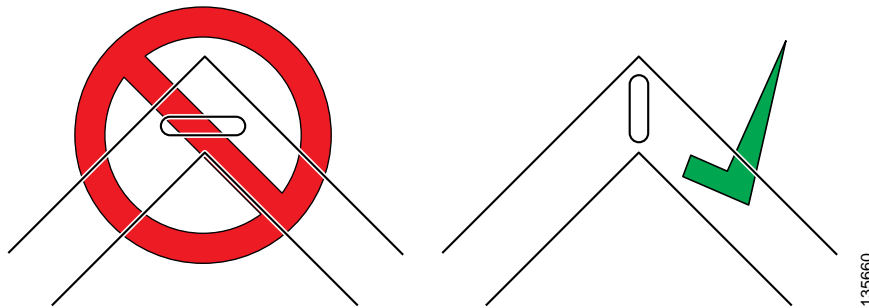
## Basic Installation Guidelines

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

- Ensure a site survey has been performed to determine the optimum placement of access points. Refer to the *Cisco Aironet 1000 Series Lightweight Access Point Deployment Guide* for site survey information.
- Check the latest release notes to ensure that your controller software version supports the access points to be installed. You can find the controller release notes by selecting your controller under **Wireless LAN Controllers** at this URL:  
[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)
- Ensure that access points are not mounted closer than 20 cm (7.9 in) from the body of all persons.
- Do not mount the access point within 3 ft (91.4 cm) of metal obstructions. Refer to the *Cisco Aironet 1000 Series Lightweight Access Point Deployment Guide* for additional information.
- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.
- Always mount the access point vertically (standing up or hanging down).

- Do not mount the access point outside of buildings.
- Do not mount the access points on building perimeter walls unless outside coverage is desired.
- When mounting an access point in the corner of a right-angle hallway intersection, mount the access point at a 45-degree angle to the two hallways (see [Figure 2-1](#)). The access point internal antennas are not omnidirectional and cover a larger area when mounted this way.

**Figure 2-1** *Mounting the Access Point in the Correct Direction*



- Ensure that the access point is on the same subnet as the primary, secondary, or tertiary controllers or has a DHCP server on the subnet with a route to the controllers.

## Before Beginning the Installation

Before you begin the installation, review these sections to become familiar with the access point, the mounting hardware, and the deployment procedure:

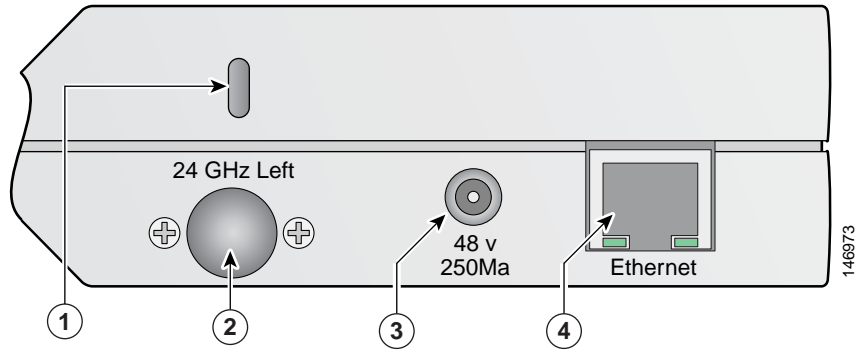
- [Access Point Layout and Connectors, page 2-5](#)
- [Controller Discovery Process, page 2-6](#)
- [Controller Discovery Process, page 2-6](#)
- [Mounting Overview, page 2-8](#)



# Access Point Layout and Connectors

Figure 2-2 illustrates the connectors on the left side of the access point.

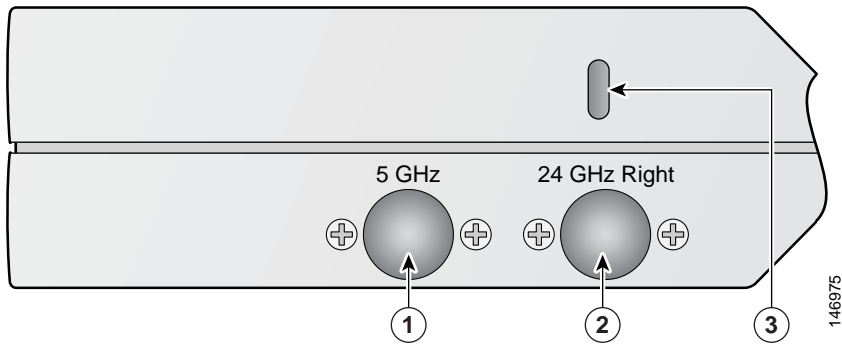
**Figure 2-2 Access Point Left Side Connectors**



<b>1</b>	Security cable keyslot	<b>6</b>	48-VDC power port
<b>2</b>	2.4-GHz antenna connector (left)	<b>7</b>	Ethernet port (RJ-45)

Figure 2-3 illustrates the right side of the access point.

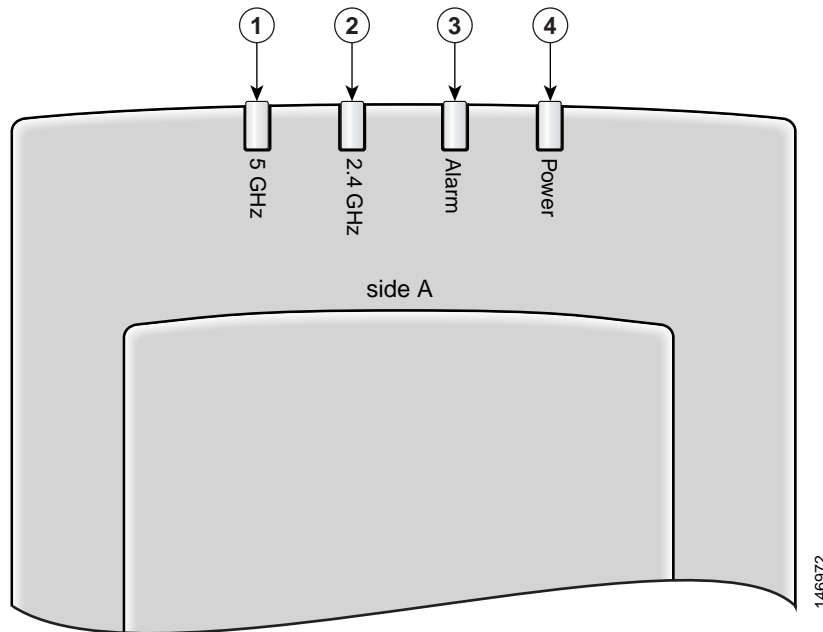
**Figure 2-3 Access Point Right Side Connectors**



<b>1</b>	5-GHz antenna connector	<b>3</b>	Security cable keyslot
<b>2</b>	2.4-GHz antenna connector (right)		

Figure 2-4 illustrates the access point LEDs on the top of the unit.

**Figure 2-4 Access Point LEDs**



<b>1</b>	5-GHz LED	<b>3</b>	Alarm LED
<b>2</b>	2.4-GHz LED	<b>4</b>	Power LED

## Controller Discovery Process

The access point supports these controller discovery processes:

- Layer 2 LWAPP discovery—Only sent on the same subnet as the access point and uses encapsulated Ethernet frames containing MAC addresses for communication between the access point and the controller. Encapsulated Ethernet frames are not suitable for Layer 3 deployments where the controller is not on the same subnet as the access points.
- Over-the-air wireless discovery—If enabled on the controller, all the associated access points transmit wireless LWAPP neighbor messages. New access points receive the controller IP address from the wireless LWAPP neighbor messages. This feature should be disabled when all access points are installed. Also, this feature is only supported by Cisco 1000 series lightweight access points and Cisco 4400 controllers.
- Locally stored controller IP addresses—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point non-volatile memory. The process of storing controller IP addresses in access points for later deployment is called priming the access point. For additional information, refer to the [“Priming Access Points Prior to Deployment”](#) section on page E-1.

- DHCP server discovery—Uses DHCP Option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option. For additional information, refer to the [“Configuring DHCP Option 43” section on page F-1](#).
- DNS server discovery—The access point uses the name *CISCO-LWAPP-CONTROLLER.<local domain>* to discover the controller IP addresses from a DNS server. Where *<local domain>* is the access point domain name.

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

## Deploying the Access Points on the Wireless Network

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

- Ensure a site survey has been performed.
- Ensure your network infrastructure devices are operational and properly configured.
- Ensure your controllers are connected to switch trunk ports.
- Ensure your switch is configured with untagged access ports for connecting your access points.
- Ensure a DHCP server with Option 43 configured is reachable by your access points.
- Review the [“Mounting Overview” section on page 2-8](#).

To deploy your access points, follow these steps:

- 
- Step 1** Obtain the access point location map created during your building site survey.
- Step 2** Review the access point locations and identify the specific mounting methods required for each access point location.
- Step 3** For each access point perform these steps:
- a. Record the access point MAC address on the access point location map (see the [“Returning MAC Information” section on page 2-20](#)).
  - b. Mount the access point at the indicated destination using the specified mounting method. For specific mounting instructions, see these sections:
    - Horizontal surface, such as a ceiling (see the [Mounting Access Points Using a Ceiling-Mount Base, page 2-10](#)).
    - Below a suspended ceiling (see the [“Mounting Access Points Using the Ceiling-Mount Clips” section on page 2-11](#)).
    - Perpendicular to a vertical surface, such as a wall (see the [“Mounting the Access Point Using a Projection Wall Mount Bracket” section on page 2-13](#)).
    - Parallel to a vertical surface, such as a wall ( see the [“Mounting the Access Point Using the Flush-Mount Bracket” section on page 2-15](#)).
  - c. Optionally secure the access point using a security cable (see the [“Securing the Access Point Using a Security Cable” section on page 2-17](#)).
  - d. Connect the access point cables (Ethernet, optional power, optional antennas). For instructions see the [“Connecting the Ethernet and Power Cables” section on page 2-17](#).

- e. On power up, verify that the access point is associated to a controller and operating normally. The Power LED should be green, the Alarm LED should be off, and the radio LEDs should be blinking. For additional information, see the [“Powering Up the Access Point”](#) section on page 2-19.

**Step 4** After all access points are deployed and operating correctly, ensure that a controller is not configured as a master controller. A master controller should only be used for configuring access points and not in a working network.

---

## Mounting Overview

You can mount the access point on any of the following surfaces:

- Horizontal or vertical flat surfaces, such as walls or ceilings
- Suspended ceilings (above and below)



### Caution

The access point, the antennas, and the power source (power injector or power module) are not designed for outdoor use and must be located in an indoor environment.

---



### Caution

The power injectors and power modules should not be placed in a building’s environmental air space, such as above suspended ceilings.

---



### Note

The access point provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space (such as above suspended ceilings) in accordance with Section 300-22(C) of the National Electrical Code (NEC).

---



### Note

When mounting the access point in a building’s environmental air space, you must use only the metal projection-mount or the flush-mount brackets (not the plastic ceiling-mount base or the hanging-ceiling clips), and the access point must be powered using PoE. Also, only the integrated antennas can be used.

---



### Note

When mounting the access point in a building’s environmental air space, you must use Ethernet cable suitable for operation in environmental air space in accordance with Section 300-22(C) of the National Electrical Code (NEC).

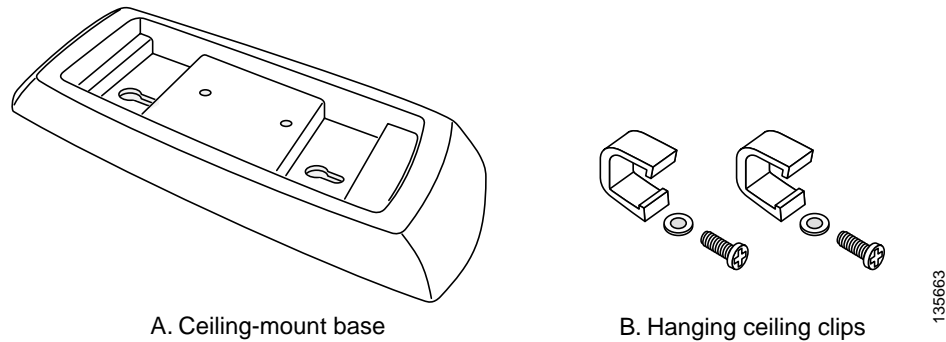
---

The access point supports mounting hardware to allow wall, ceiling, or suspended ceiling mounting:

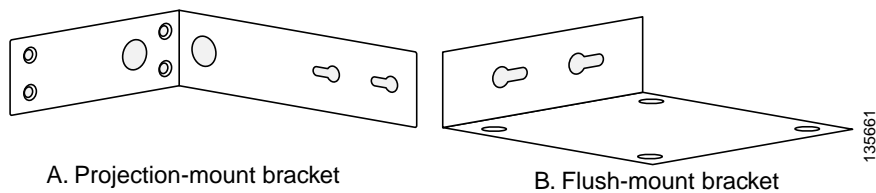
- Ceiling-mount base for mounting the access point to a horizontal surface—supplied with the access point (see [Figure 2-5](#))
- Two suspended ceiling hanging-clips for mounting the access point below a suspended ceiling—supplied with the access point (see [Figure 2-6](#))
- Metal projection-mount bracket (user orderable) for mounting the access point to a vertical wall (see [Figure 2-6](#))

- Metal flush-mount bracket (user orderable) for mounting the access point to a vertical wall (see [Figure 2-6](#))
- Ceiling-mount bezel kit (user orderable) for mounting the access point above a suspended ceiling tile. For additional information, refer to the *Quick Start Guide: Ceiling Mount Bezels for Cisco Aironet 1000 Series Lightweight Access Points*.

**Figure 2-5 Factory-Supplied Mounting Options**



**Figure 2-6 Orderable Mounting Brackets**



Refer to the [Table 2-1](#) to identify the materials you need to mount your access point, then go to the section containing the specific mounting procedure.

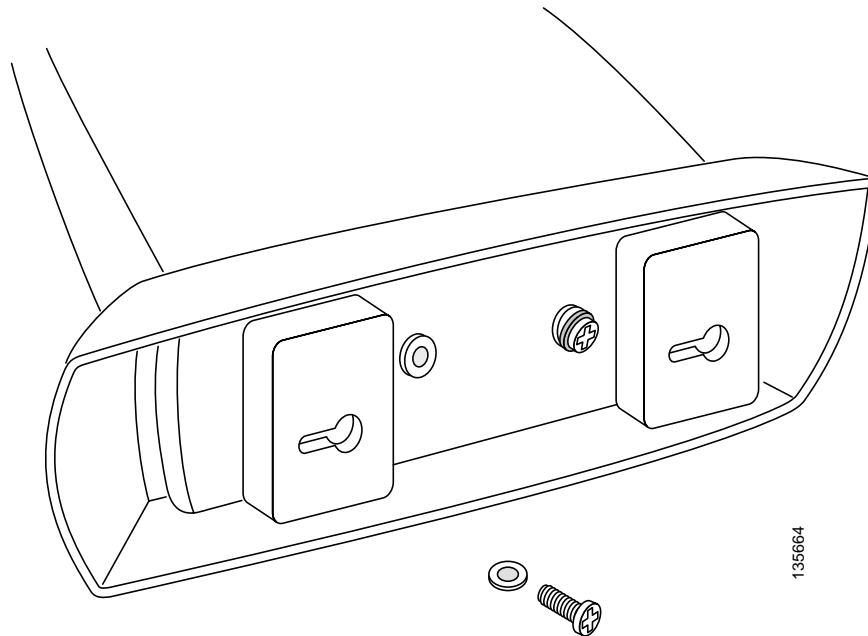
**Table 2-1 Material Needed to Mount Access Point**

Mounting Method	Materials Required	Supplied
Horizontal surface	Ceiling-mount base with two screws and two washers Two screws and optional wall anchors Standard screwdriver Drill and drill bit	Yes User supplied User supplied User supplied
Suspended ceiling	Two hanging-clips with two screws and two washers Standard screwdriver	Yes User supplied
Vertical surface	Projection-mount bracket with two screws and two washers Four screws and optional wall anchors Standard screwdriver Drill and drill bit	Orderable User supplied User supplied User supplied
Vertical surface	Flush-mount bracket with two screws and two washers Four screws and optional wall anchors Standard screwdriver Drill and drill bit	Orderable User supplied User supplied User supplied

## Mounting Access Points Using a Ceiling-Mount Base

When you are mounting the access point to horizontal surface, such as the ceiling of a building, use the ceiling-mount base to mount the access point. The ceiling-mount base can also be used to mount the access point to a desktop or shelf.

**Figure 2-7 Attaching the Access Point and Ceiling-Mount Base**



Follow these steps to attach the ceiling-mount base to the access point and mount the access point to a horizontal surface, such as a ceiling.

- 
- Step 1** Copy the MAC address(es) from the label(s) on the access point onto the corresponding location on your access point location map. MAC addresses have the format 00xxxxxxxxxx.
  - Step 2** Find the required mounting location as identified on your access point location map.
  - Step 3** Use the ceiling-mount base to mark the two screw key slots on the ceiling location. ensure to leave enough space around the access point and base to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver security cable into the sides of the access point.
  - Step 4** Install two screws in the marked key slots locations. Use appropriate screws and anchors (user supplied). Tighten the screws until the heads are about 1/8 inch from the ceiling surface.
  - Step 5** Attach the ceiling-mount base to the bottom of the access point using the factory-supplied machine screws and washers (refer to [Figure 2-7](#)).
  - Step 6** Position the access point with the ceiling-mount base so its keyhole slots are on over the screw heads and slide the ceiling-mount base in the direction of the key slots.




---

**Note** If the ceiling screws do not securely hold the access point, remove the ceiling-mount base and tighten the ceiling screws until they hold the access point securely.

---

**Step 7** Attach the cables to the access point.



**Note** When the access point is powered up and is associated with a controller (Power LED is green, Alarm LED is off, and the radio LEDs are blinking), the access point is broadcasting its beacon.

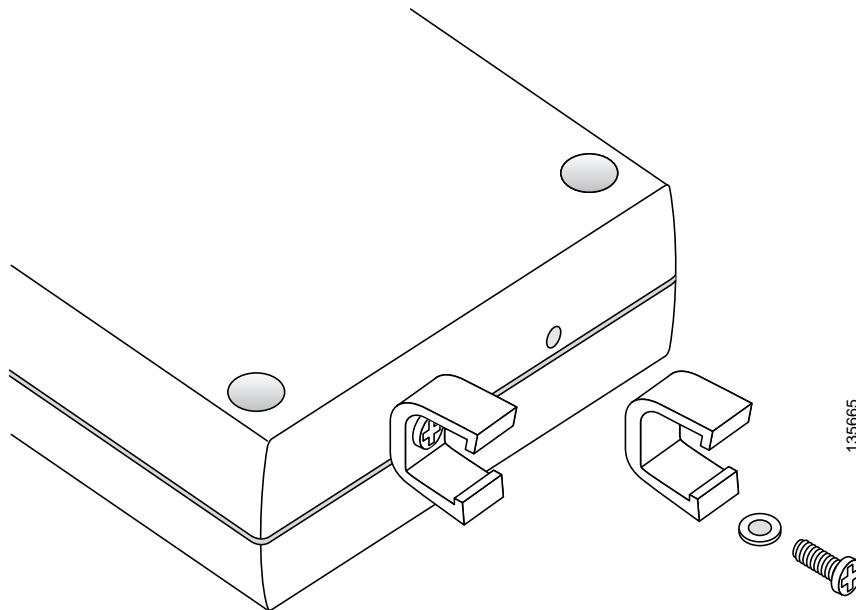
**Step 8** Repeat these steps for each access point on a horizontal surface.

After mounting all horizontal surface access points, return to deploying the access points, "[Step 3-c](#)" on [page 2-7](#).

## Mounting Access Points Using the Ceiling-Mount Clips

When you are mounting the access point under a suspended ceiling, use the ceiling-mount clips to mount the access point to the suspended ceiling rails.

**Figure 2-8** Attaching the Ceiling-Mount Clips to the Access Point

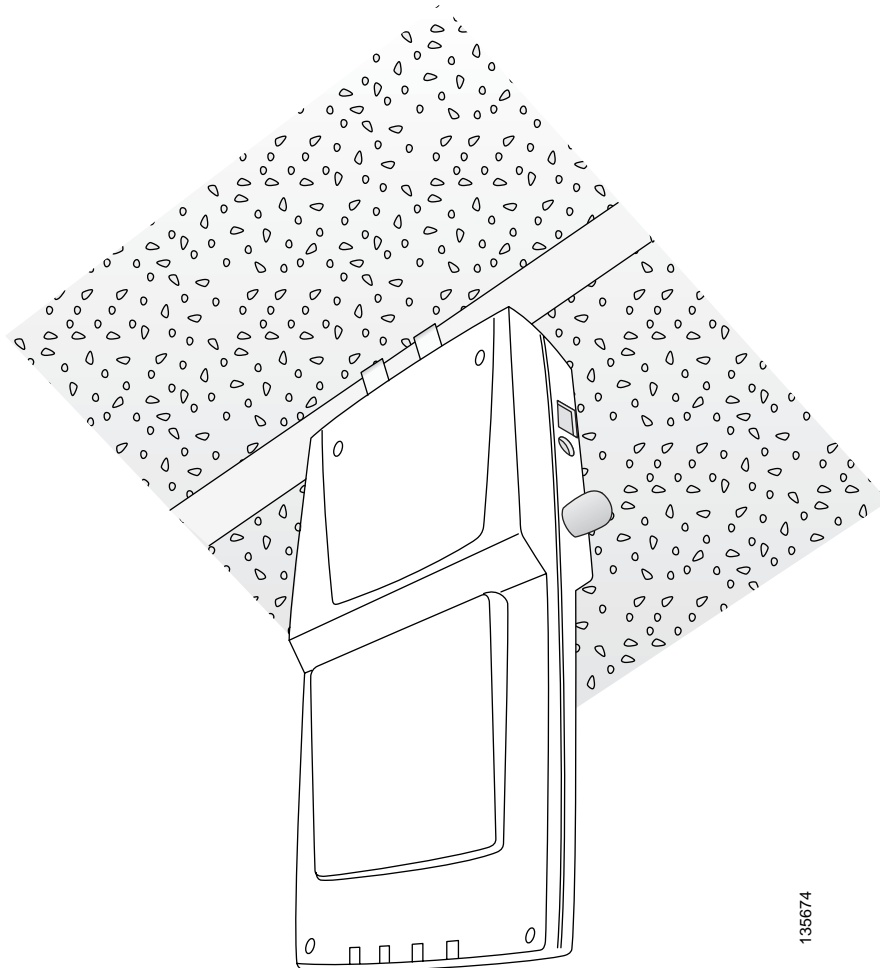


Follow these steps to attach the ceiling-mount clips to the access point and mount the access point to suspended ceiling rails:

- Step 1** Copy the MAC address from the label on the access point onto the corresponding location on the access point location map. MAC addresses have the format 00xxxxxxxx.
- Step 2** Attach the ceiling-mount clips to the bottom of the access point using the factory-supplied machine screws and washers (see [Figure 2-8](#)).

- Step 3** Snap the ceiling-mount clips onto a suspended ceiling rail (see [Figure 9](#)). Ensure you leave enough space around the access point to plug the Ethernet cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver security cable into the sides of the access point.

**Figure 9** *Mounting the Access Point with Ceiling-Mount Clips to a Suspended Ceiling Rail*



- Step 4** Attach the cables (Ethernet and optional antennas) to the sides of the access point.



**Note** Ensure that the cables are routed away from the access point integrated antennas.



**Note** When the access point is powered up and is associated with a controller (Power LED is green, Alarm LED is off, and the radio LEDs are blinking), the access point radios are operational and broadcasting their beacons.

- Step 5** Repeat Steps 1 to 4 for each suspended ceiling access point location.  
After mounting all suspended ceiling access points, return to deploying the access points, ["Step 3-c" on page 2-7](#).



## Mounting the Access Point Using a Projection Wall Mount Bracket

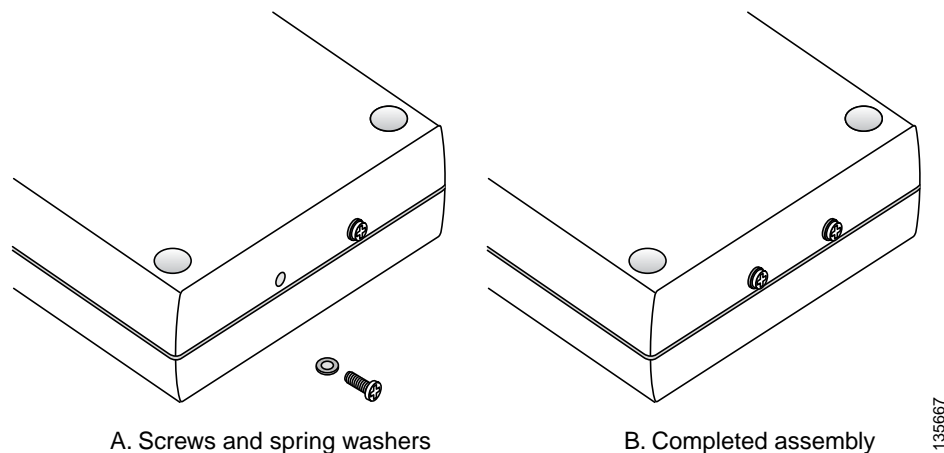
When you are mounting the access point out from a vertical wall (flat sides along the wall or hallway), use an optional factory-orderable projection-mount L-bracket (see [Figure 2-6](#)). Follow these steps to attach the access point to the projection-mount bracket and mount the access point to a vertical wall:

- Step 1** Before proceeding, gently screw the two factory-supplied screws and spring washers into the bottom of the access point (see [Figure 2-10](#)). Ensure the spring washers have their convex (high center sections) pointing toward the screw heads.



**Note** Do not tighten the screw heads flush with the access point surface or the bracket will not fit under the screw heads.

**Figure 2-10** Attaching the Mounting Screws to the Access Point

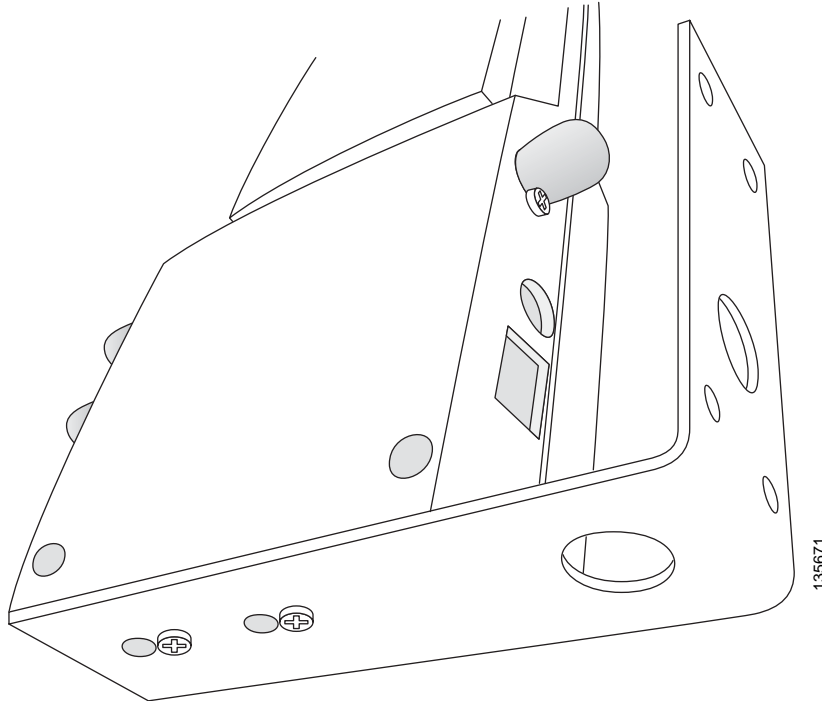


- Step 2** Copy the MAC address(es) from the label(s) on the access point onto the corresponding location on the access point location map. MAC addresses have the format 00xxxxxxxxxx.
- Step 3** Find the required mounting location as identified on your access point location map.
- Step 4** Use the projection-mount bracket to mark the four screw holes on the wall. Ensure to leave enough space around the access point and base to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver security cable into the sides of the access point.
- Step 5** Mount the projection-bracket to the wall using four screws in the marked locations. Use appropriate screws and wall anchors (user supplied). Tighten the wall screws.
- Step 6** Position the two screws in the base of the access point over the projection-bracket keyhole slots and slide the access point in the direction of the key slots (see [Figure 2-11](#)). If you are unable to attach the access point to the bracket, remove the access point and loosen the two access point screws.



**Note** After attaching the access point to the bracket, tighten the screws until they securely hold the access point.

**Figure 2-11** Attaching the Access Point to the Projection-Mount Bracket



**Step 7** Attach the cables to the sides of the access point. The Ethernet cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver security cables can be routed through the large holes in the mounting bracket.



**Note** Ensure that the cables are routed away from the access point integrated antennas.



**Note** When the access point is powered up and is associated with a controller (Power LED is green, 2.4 GHz LED is yellow, and 5.4 GHz LED is amber), the access point is broadcasting its beacon.

**Step 8** Repeat Steps 1 to 7 for each projection-mount bracket location.

After mounting all your projection-mount access points, return to deploying the access points, "[Step 3-c](#)" on page 2-7.

## Mounting the Access Point Using the Flush-Mount Bracket

When mounting the access point against a vertical wall (flat side toward the inside of the building), use an optional factory-orderable flush-mount bracket. Follow these steps to mount the bracket and attach the access point:

- Step 1** Before proceeding, gently screw the two factory-supplied screws and spring washers into the bottom of the access point (see [Figure 2-10](#)). Ensure the spring washers have their convex (high center sections) pointing toward the screw heads.



**Note** Do not tighten the screw heads flush with the access point surface or the bracket will not fit under the screw heads.

- Step 2** Copy the MAC address(es) from the label(s) on the access point onto the corresponding location on the access point location map. MAC addresses have the format 00xxxxxxxxxx.

- Step 3** Find the required mounting location as identified on your access point location map.

- Step 4** Use the flush-mount bracket to mark the four screw holes on the wall. Ensure to leave enough space around the access point and base to plug the CAT-5 cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver security cable into the sides of the access point.

- Step 5** Mount the flush-mount bracket to the wall using four screws in the marked locations. Use appropriate screws and wall anchors (user supplied). Tighten the wall screws.

- Step 6** Position the two screws in the base of the access point over the flush-mount bracket keyhole slots and slide the access point in the direction of the key slots (see [Figure 2-12](#)). If you are unable to attach the access point to the bracket, remove the access point and loosen the two access point screws.

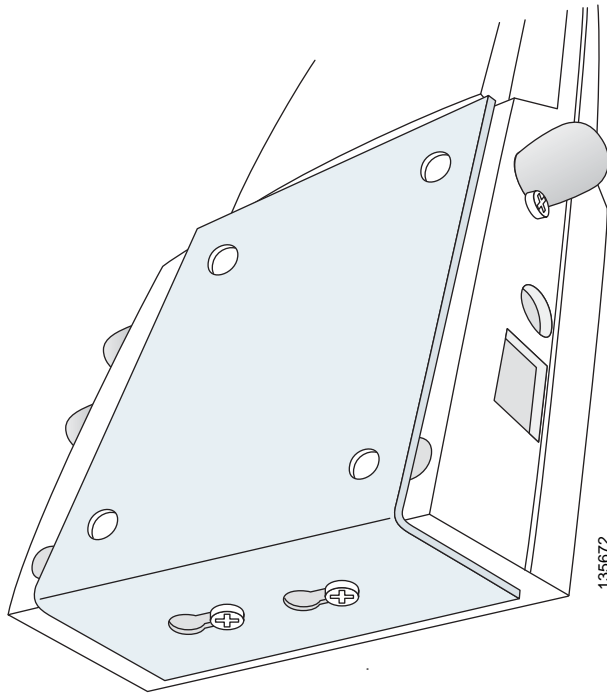


**Note** Ensure the side of the access point with the door is facing away from the wall. This ensures that the correct antenna is facing the building, and makes future upgrades easier.



**Note** After attaching the access point to the bracket, tighten the screws until they securely hold the access point.

**Figure 2-12** Attaching the Access Point to the Flush-Mount Bracket



- Step 7** Attach the cables to the sides of the access point (the Ethernet cable, optional external antenna cable(s), optional power supply cable, and optional Kensington MicroSaver security cable).



**Note** Ensure that the cables are routed away from the access point integrated antennas.



**Note** When the access point is powered up and is associated with a controller (Power LED is green, Alarm LED is off, and the radio LEDs are blinking), the access point is broadcasting its beacon.

- Step 8** Repeat Steps 1 to 7 for each flush-mount bracket location.  
After mounting all your flush-mount access points, return to deploying the access points, "[Step 3-c](#)" on [page 2-7](#).

## Securing the Access Point Using a Security Cable

You can secure the access point by installing a standard security cable (such as the Kensington MicroSaver, model number 64068) into the access point security cable slot (see [Figure 2-3](#)). The security cable can be used with any of the mounting methods described in this guide provided the cable can be secured to a nearby immovable object.

Follow these steps to install the security cable.

- 
- Step 1** Loop the security cable around a nearby immovable object.
  - Step 2** Insert the key into the security cable lock.
  - Step 3** Insert the security cable latch into the security key slot on the access point.
  - Step 4** Rotate the key right or left to secure the security cable lock to the access point.
  - Step 5** Remove the key from security cable lock.
  - Step 6** Repeat Steps 1 to 4 for each access point requiring a security cable.

After securing your access points, go to the [“Connecting to an Ethernet Network with an Inline Power Source”](#) section on page 2-18.

---

## Connecting the Ethernet and Power Cables

The access point receives power through the Ethernet cable or an external power module.



---

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

---



---

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 standard).

---

The access point power options:

- Option 1—Switches with sufficient inline power:
  - An inline power capable switch, such as the Cisco Catalyst 3550 PWR XL, 3560-48PS, 3750-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
  - Other inline power switches supporting the IEEE 802.3af inline power standard
- Option 2—Switches without sufficient inline power can use the power injector:
  - Cisco Aironet Power Injector (AIR-PWRINJ-1000AF=)
- Option 3—Local power using the power module (AIR-PWR-1000=)

**Note**

Some older switches and patch panels might not provide enough power to operate the access point. At power-up, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. All access LEDs are off.

## Connecting to an Ethernet Network with an Inline Power Source

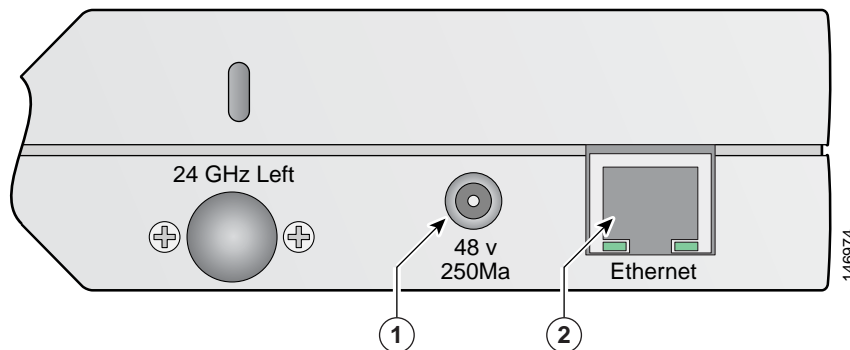
**Note**

If your access point is connected to in-line power, do not connect the power module to the access point.

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

- Step 1** Connect a Category 5 Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point (see [Figure 2-13](#)).

**Figure 2-13** Ethernet and Power Ports



<b>1</b>	Ethernet port	<b>2</b>	48 VDC power port
----------	---------------	----------	-------------------

- Step 2** Connect the other end of the Ethernet cable to one of the following:
- A switch with inline power (see the [“Connecting the Ethernet and Power Cables”](#) section on [page 2-17](#)).
  - The Ethernet connector on the power injector (AIR-PWRINJ-1000AF) labeled *J1 DATA & PWR*. Also connect a Category 5 Ethernet cable from the power injector Ethernet connector labeled *J2 DATA* to a non-powered Ethernet port on your 10/100 Ethernet LAN.
- Step 3** Repeat Steps 1 to 2 for each access point requiring in-line power.

## Connecting to an Ethernet Network with Local Power



---

**Note** If your access point is connected to in-line power, do not connect the power module to the access point.

---

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

- 
- Step 1** Connect a Category 5 Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point (see [Figure 2-13](#)).
- Step 2** Plug the other end of the Ethernet cable into an non-powered Ethernet port on your 10/100 Ethernet LAN.
- Step 3** Connect the power module output connector to the access point's 48-VDC power port (see [Figure 2-13](#)).
- Step 4** Plug the power module power cord into an approved 100- to 240-VAC outlet.
- 

## Powering Up the Access Point

After you power up the access point, it begins a power-up sequence that you can check by observing the access point LEDs. The red Alarm LED turns on for about 15 to 20 seconds and then all LEDs blink sequentially back and forth, indicating that the access point is trying to find a controller. Refer to [“Checking the Access Point LEDs” section on page 3-3](#) for LED descriptions.

After the access point finds the controller, the access point downloads new operating system code if the access point code version differs from the controller code version. During the download process, all access point LEDs blink simultaneously. When the operating system download is successful, the access point reboots.

Normal operation is indicated when the Alarm LED is off, the Power LED is green, and the 2.4 GHz and 5 GHz LEDs are blinking to indicate radio activity.

If no LEDs are on, the access point might not be receiving sufficient power.

If all the LEDs blink sequentially for more than five minutes, the access point is unable to find its primary, secondary, or tertiary controllers. Check the connection between the access point and its controllers and ensure they are on the same subnet or that the access point has a route back to its primary, secondary, and tertiary controllers. If the access point is not on the same subnet as the controllers, ensure there is a properly configured DHCP server on the same subnet as the access point. See the [“Using DHCP Option 43” section on page 3-2](#) for DHCP information.



---

**Note** To allow client roaming between access points, the access points must be on the same subnet.

---



---

**Note** Connect only one power source to the access point, for example: When using in-line power, do not connect the power module to the access point.

---

## Returning MAC Information

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





## CHAPTER 3

# 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/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)

Sections in this chapter include:

- [Guidelines for Using the Access Points](#), page 3-2
- [Checking the Access Point LEDs](#), page 3-3
- [Low Power Condition](#), page 3-5

## Guidelines for Using the Access Points

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

- The access points can only communicate with controllers and cannot operate independently.
- The access points do not support Wireless Domain Services (WDS). The access points cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support Layer 2 or Layer 3 LWAPP communications with the controllers. In Layer 2 operation, the access point and the controller must be on the same subnet and communicate with each other using MAC addresses in encapsulated Ethernet frames. This operation is not scalable to larger networks and not recommended by Cisco.

In Layer 3 operation, the access point and the controller can be on the same or different subnets. Layer 3 operation is scalable and is recommended by Cisco. 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 LWAPP 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 is used to provide the IP addresses of the Management Interface of your controllers. Typically, a DHCP server can be configured on a Cisco switch.
  - Optionally a DNS server can be configured to enable CISCO-LWAPP-CONTROLLER.<local domain> to resolve to the IP addresses of the Management Interface of your controllers.
  - Your controllers are configured and reachable by the access points

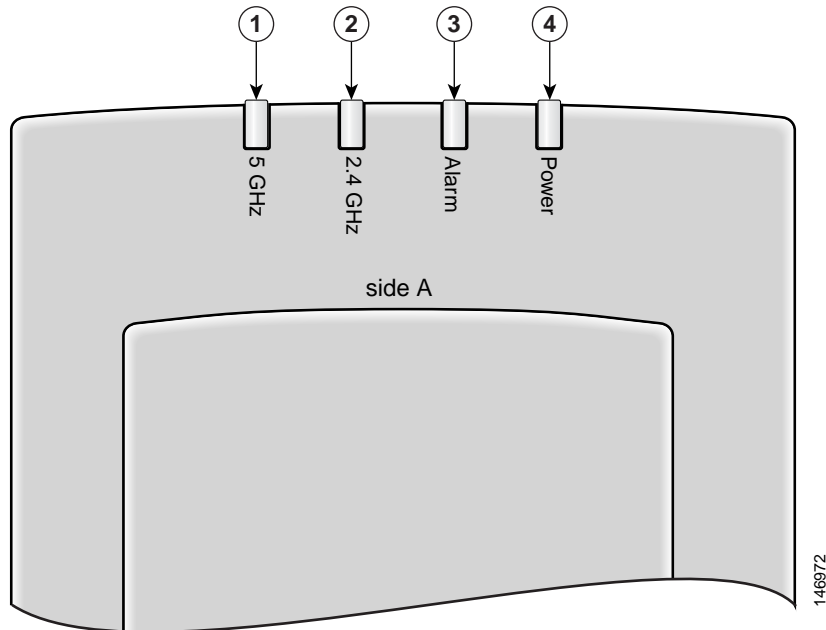
## Using DHCP Option 43

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. For additional information, refer to the [“Configuring DHCP Option 43” section on page F-1](#).

## Checking the Access Point LEDs

If your access point is not working properly, check the access point LEDs on the top of the unit. You can use the LED indications to quickly assess the unit's status. [Figure 3-1](#) shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

**Figure 3-1** Access Point LEDs



<b>1</b>	5-GHz LED	<b>3</b>	Alarm LED
<b>2</b>	2.4-GHz LED	<b>4</b>	Power LED

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

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

Power LED	Alarm LED	2.4 GHz LED	5 GHz LED	Meaning
Off	Off	Off	Off	No power or insufficient power. Check the power source and ensure that sufficient power is supplied to the access point. See <a href="#">Low Power Condition, page 3-5</a> .
Off	Red	Off	Off	Power applied and access point powering up (typical 10-20 seconds). If the red Alarm LED remains on for more than 1 minute, remove power from the access point and contact TAC for assistance.
All LEDs sequentially cycle on and off				Access point searching for a controller or DHCP server. If the access point remains in this mode for more than 5 minutes, it is unable to find the controller. Check the connection between the access point and the controller. Also verify a DHCP server is available on the access point subnet.
Green	Off	Blinking Yellow	Blinking Amber	Normal operation, both radios transmitting beacons or transmitting and receiving data packets. If one or both radio LEDs remain off, this indicates a problem with the wireless network. Check the controller configuration for the access point.
Green	Off	On or off	Blinking Amber	Normal operation, 5-GHz radio activity. If one or both radio LEDs remain off, this indicates a problem with the wireless network. Check the controller configuration for the access point.
Green	Off	Blinking Yellow	On or off	Normal operation, 2.4-GHz radio activity. If one or both radio LEDs remain off, this indicates a problem with the wireless network. Check the controller configuration for the access point.
All LEDs blink on and off simultaneously				Associated to controller and downloading new code.
Off	Blinking red	Off	Off	Duplicate access point IP address detected. Advise your network administrator about the problem.
Off	Off	Off	Off	No power or low power condition.
Blinking Green	Off	Off	Off	Site survey mode on AIR-AP1010 and AIR-AP1020
Blinking Green	Off	Off	Off	Disconnected from root AP on AIR-AP1030.

# Low Power Condition

**Warning**

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

The access point can be powered from the 48-VDC power module or from an in-line power source. The access point supports the IEEE 802.3af power standard for in-line power sources.

For operation, the access point (powered device) requires 12 W of input power.

**Note**

When the access point is being used in a PoE configuration, the power drawn from the power sourcing equipment (PSE), such as a switch or power injector, is higher by an amount dependent on the length of the interconnecting cable.

The power module (AIR-PWR-1000=) and the Cisco Aironet power injector (AIR-PWRINJ-1000af=) are capable of supplying the required operating power, but some inline power sources are not capable of supplying sufficient power. Also, some high-power inline power sources, might not be able to provide sufficient power to all ports at the same time.

**Note**

An 802.3af compliant switch (Cisco or non-Cisco) is capable of supplying sufficient power for full operation.

**Note**

If your access point is connected to in-line power, do not connect the power module to the access point.

On power up, the access point is placed into low power mode (both radios are deactivated), the access point power negotiation determines if sufficient power is available. If there is sufficient power then the access point begins to power up (Alarm LED is red and other LEDs are off); otherwise, the access point turns off all LEDs and remains in low power mode to prevent a possible over-current condition.





# APPENDIX **A**

## Translated Safety Warnings

---

For translated safety warnings, refer to the safety warning document that shipped with your access point or that is available on Cisco.com.

To browse to the document on Cisco.com, follow these steps:

- 
- Step 1** Click this link to the Cisco Wireless documentation home page:  
[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)
  - Step 2** Click **Cisco Aironet 1000 Series** listed under Wireless LAN Access.
  - Step 3** Click **Install and Upgrade Guides**.
  - Step 4** Click **Safety Warnings for Cisco Aironet 1000, 1100, 1130AG, 1200, and 1240AG Series Access Points**.
-







## APPENDIX **B**

# Declarations of Conformity and Regulatory Information

---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1000 Series Lightweight Access Points.

This appendix contains the following sections:

- [Manufacturers Federal Communication Commission Declaration of Conformity Statement, page B-2](#)
- [Industry Canada, page B-4](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page B-5](#)
- [Declaration of Conformity for RF Exposure, page B-7](#)
- [Guidelines for Operating Cisco Aironet Access Points in Japan, page B-8](#)
- [Administrative Rules for Cisco Aironet Access Points in Taiwan, page B-9](#)
- [Declaration of Conformity Statements, page B-11](#)
- [Declaration of Conformity Statements for European Union Countries, page B-11](#)

# Manufacturers Federal Communication Commission Declaration of Conformity Statement



**Model:**

AIR-AP1010-A-K9 / AIR-AP1020-A-K9 / AIR-AP1030-A-K9  
 AIR-AP1010-B-K9 / AIR-AP1020-B-K9 / AIR-AP1030-B-K9

**FCC Certification number:**

LDK102057

**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.

---

**Caution**

Within the 5.15 to 5.25 GHz band (5 GHz radio channels 34 to 48) the U-NII devices are restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite System (MSS) operations.

## 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**

VCCI 準拠クラスB機器（日本）  
この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス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ください。

# Industry Canada

**Model:**

AIR-AP1010-A-K9 / AIR-AP1020-A-K9 / AIR-AP1030-A-K9  
AIR-AP1010-B-K9 / AIR-AP1020-B-K9 / AIR-AP1030-B-K9

**Certification number:**

2461B-102057

## Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte les exigences du Règlement sur le matériel brouilleur du Canada.

This device complies with Class B Limits of Industry Canada. 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.

Cisco Aironet 2.4-GHz Access Points are certified to the requirements of RSS-210 for 2.4-GHz spread spectrum devices, and Cisco Aironet 54-Mbps, 5-GHz Access Points are certified to the requirements of RSS-210 for 5-GHz spread spectrum devices. This device must be operated indoors according to the Canadian regulations. For further information, contact your local Industry Canada office.

# European Community, Switzerland, Norway, Iceland, and Liechtenstein

## Model:

AIR-AP1010-E-K9 / AIR-AP1020-E-K9 / AIR-AP1030-E-K9

## Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive)

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.

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 ουσιαστικές 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.
Latviski [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.

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-ohra 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 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.

121404

This device complies with the EMC requirements (EN 60601-1-2) of the Medical Directive 93/42/EEC.

For 2.4 GHz radios, the following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

**Note**

This equipment is intended to be used in all EU and EFTA countries. For more details, contact Cisco Corporate Compliance.

**Caution**

The access point, the antennas, and the power source (power injector or power module) are not designed for outdoor use and must be located in an indoor environment.

For 54 Mbps, 5 GHz access points, the following standards were applied:

- Radio: EN 301.893
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

The following CE mark is affixed to the access point with a 2.4 GHz radio and a 54 Mbps, 5 GHz radio:



## Declaration of Conformity for RF Exposure

The radio has been found to be compliant to the requirements set forth in CFR 47 Sections 2.1091, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices as defined in Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields. The equipment should be installed more than 20 cm (7.9 in.) from your body or nearby persons.

The access point must be installed to maintain a minimum 20 cm (7.9 in.) co-located separation distance from other FCC approved indoor/outdoor antennas used with the access point. Any antennas or transmitters not approved by the FCC cannot be co-located with the access point. The access point's co-located 2.4 GHz and 5 GHz integrated antennas support a minimum separation distance of 8 cm (3.2 in.) and are compliant with the applicable FCC RF exposure limit when transmitting simultaneously.

**Note**

---

Dual antennas used for diversity operation are not considered co-located.

---

# 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.

## Model:

AIR-AP1010-J-K9 / AIR-AP1020G-J-K9 / AIR-AP1030G-J-K9  
AIR-AP1010-P-K9 / AIR-AP1020-P-K9 / AIR-AP1030-P-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 : 03-5549-6500

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: 03-5549-6500



# 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.

## Access Points with IEEE 802.11a Radios

### Chinese Translation

本設備限於室內使用

### English Translation

This equipment is limited for indoor use.

## All Access Points

### 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.

## Declaration of Conformity Statements

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

<http://www.ciscofax.com>

## Declaration of Conformity Statements for European Union Countries

The Declaration of Conformity statement for the European Union countries is listed on the following pages:



**DECLARATION OF CONFORMITY**  
with regard to the **R&TTE Directive 1999/5/EC**  
according to EN 45014

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

Declare under our sole responsibility that the product,

*Product:* **AIR-AP1010-E-K9**  
**AIR-AP1020-E-K9**  
**AIR-AP1030-E-K9**  
*1000 Series IEEE802.11 a/b/g Access Point*

Fulfils the essential requirements of the Directive 1999/5/EC

The following standards were applied:

**EMC**                    **EN 301.489-1 v1.4.1: 2002-08; EN 301.489-17 v1.2.1: 2002-09**

**Health & Safety** **EN60950: 2000; EN 50385: 2002**

**Radio**                **EN 301.893 v 1.2.3: 2003-08**  
**EN 300 328 v 1.4.1: 2003-04**

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

The product carries the CE Mark:



Date & Place of Issue:        **13 April 2005, San Jose**

Signature:

**Tony Youssef**  
Director Corporate Compliance  
Cisco Systems, 125 West Tasman Drive  
San Jose, CA 95134 - USA

Additional information:

*EMC Test Report:*                    **Elliot Laboratories: R 56965**  
*Safety Test Report:*                **CSA International: CB 218920-1564365; Cisco Systems EDCS-442311**  
*Radio Test Report:*                **Elliot Laboratories: R 56674 (2.4 GHz) & R56675 (5 GHz)**

146679

*DofC 442316rev1*



### Annex to DofC# 442316 Information on Antennas and Power Levels

The AIR-AP1010-E-K9 has 6 dBi integral antennas. The AIR-AP1020-E-K9 and AIR-AP1030-E-K9 are equipped with antenna connectors to allow the use of dedicated antennas for both the 2.4 GHz and the 5 GHz part.

This Declaration of Conformity also covers the antennas listed in table 1 and table 2 as they were assessed in combination with the product (AIR-AP1020-E-K9 and AIR-AP1030-E-K9) against the essential requirements of the Directive 1999/5/EC. For each of the antennas, the tables list the maximum output power setting for the product in order to result in a total eirp level below the applicable limit.

Any combination of output power and antenna resulting in an eirp level above the regulatory limit is illegal and is outside the scope of this declaration. Antennas not listed in the tables below are also outside the scope of this document.

**Table 1: Dedicated antennas for 2,4 GHz**

Antenna P/N	Antenna Gain (dBi)	Maximum Power Setting <sup>(1)</sup>	Antenna Name
AIR-ANT4941	2.2	100 %	Dipole Antenna
AIR-ANT5959	2.0	100 %	Diversity Omni-Directional Antenna
AIR-ANT1728	5.2	100 %	Omni Ceiling Mount Antenna
AIR-ANT2506	5.2	100 %	Omni Mast Mount Antenna
AIR-ANT3213	5.2	100 %	Diversity Omni Antenna
AIR-ANT1729	6.0	100 %	Patch Wall Mount Antenna
AIR-ANT2012	6.5	100 %	Diversity Patch Antenna
AIR-ANT3549	9.0	50 %	Hemispherical Patch Antenna

**Note 1:** Possible settings are 100%, 50%, 25 %, 12,5 % and 6,25%. A setting of 100 % corresponds to a maximum conducted output power of 13,5 dBm (at 2.4 GHz). For all combinations, the total radiated power level (including antenna gain) is equal to or below 20 dBm (eirp).

**Table 2: Dedicated antennas for 5 GHz**

Antenna (Cisco P/N)	Gain (dBi)	Freq Band (MHz)	Regulatory eirp Limit (mW)	Maximum Power Setting <sup>(2)</sup>	Antenna Description
AIR-ANT5135D-R	3.5	5150 - 5350	200	100 %	Dipole Antenna
		5470 - 5725 <sup>(1)</sup>	1000	100 %	
AIR-ANT5160V-R	6	5150 - 5350	200	100 %	Omni Antenna
		5470 - 5725 <sup>(1)</sup>	1000	100 %	

**Note 1:** Operation in 5470 to 5725 MHz not allowed in France.

**Note 2:** Possible settings are 100%, 50%, 25 %, 12,5 % and 6,25%. A setting of 100 % corresponds to a maximum conducted output power of 17 dBm / 50 mW (at 5 GHz). For all combinations, the total radiated power level (including antenna gain) is equal to or below 23 dBm (eirp).

April 13, 2005

Tony Youssef  
Director Corporate Compliance

146680

■ Declaration of Conformity Statements for European Union Countries



# APPENDIX **C**

## Access Point Specifications

Table C-1 lists the technical specifications for the Cisco Aironet 1000 Series Lightweight Access Point.

**Table C-1** Access Point Specifications

Category	Specifications		
	802.11b	802.11g	802.11a
Size	5.7 in. W x 1.6 in. D x 9.6 in. H 24.4 cm W x 4.1 cm D x 24.4 cm H		
Indicators	Four indicators on the top of the unit: Power, Alarm, 2.4 GHz, 5 GHz.		
Connectors	Right side: 5-GHz RP-TNC antenna connector, 2.4-GHz RP-TNC antenna connector  Left side: 2.4-GHz RP-TNC antenna connector, power connector (for 48VDC AC power module), RJ-45 connector for 10BASE-T or 100BASE-T Ethernet connections.		
Input voltage	48 VDC (nominal)		
Input power	12 W		
Operating temperature	32 to 104°F (0 to 40°C)		
Storage temperature	-13 to 158°F (-25 to 70°C)		
Humidity	10 to 90% non-condensing		
Weight	With ceiling-mount clips: 1.3 lbs (0.6 kg) With optional wall brackets: 2.2 lbs (1 kg)		
Modulation	Complementary Code Keying (CCK)	Orthogonal Frequency Division Multiplex (OFDM)	
Subcarrier modulation	BPSK (1 Mbps) QPSK (2 Mbps) CCK (5.5 and 11 Mbps)	BPSK (6 and 9 Mbps) QPSK (12 and 18 Mbps) 16-QAM (24 and 36 Mbps) 64-QAM (48 and 54 Mbps)	BPSK (6 Mbps and 9 Mbps) QPSK (12 Mbps and 18 Mbps) 16-QAM (24 and 36 Mbps) 64-QAM (48 and 54 Mbps)

Table C-1 Access Point Specifications (continued)


Category	Specifications		
	802.11b	802.11g	802.11a
Power output settings	CCK	OFDM	OFDM
	100, 50, 12.5, and 6.25 percent settings on the controller		
	100 mW (20 dBm) conducted	50 mW (17 dBm) conducted	
	Maximum output power depends on the regulatory domain in which the access point is installed		
Antenna	AIR-AP1010		
	<ul style="list-style-type: none"> <li>Two integrated 6 dBi patch antennas (2.4 and 5 GHz)</li> </ul>		
Antenna	AIR-AP1020 and AIR-AP1030		
	<ul style="list-style-type: none"> <li>Two integrated 6 dBi patch antennas (2.4 and 5 GHz)</li> <li>Three external antenna connectors</li> </ul>		
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)	5.15 to 5.25 GHz 5.25 to 5.35 GHz 5.475 to 5.725 GHz 5.725 to 5.85 GHz  (Depending on the regulatory domain in which the access point is installed)	
Data rates	1, 2, 5.5, and 11 Mbps	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	
Typical indoor range (across open office environment)	160 ft (49 m) @ 11 Mbps 410 ft (125 m) @ 1 Mbps	90 ft (27 m) @ 54 Mbps 180 ft (100 m) @ 18 Mbps 300 ft (91 m) @ 6 Mbps	45 ft (14 m) @ 54 Mbps 110 ft (34 m) @ 18 Mbps 165 ft (50 m) @ 6 Mbps
Compliance	The 1000 series access point complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings.		
	 <p><b>Caution</b> The power injector and power module have not been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.</p>		
Safety	Designed to meet:		
	<ul style="list-style-type: none"> <li>IEC 60950-1</li> <li>UL 60950-1</li> <li>CSA 60950-1</li> <li>EN 60950-1</li> <li>UL 2043</li> </ul>		
Radio Approvals	FCC Parts 15.247 Canada RSS-210 Japan ARIB-STD-33A Japan ARIB-STD-66 Europe EN-300.328	FCC Part 15.407 Canada RSS-210 Japan ARIB STD-T71 EN 301.893	




Table C-1 Access Point Specifications (continued)

Category	Specifications		
	802.11b	802.11g	802.11a
EMI and Susceptibility	FCC Part 15.107 and 15.109 ICES-003 (Canada) EN 55022 EN 60601-1-2:2001 VCCI EN 301.489-1 EN 301.489-17 EN 55022 EN 55024		
RF Exposure	OET-65C RSS-102 ANSI C95.1		



Table C-1 Access Point Specifications (continued)

Category	Specifications		
	802.11b	802.11g	802.11a
Power output settings	<b>CCK</b>	<b>OFDM</b>	<b>OFDM</b>
	100, 50, 12.5, and 6.25 percent settings on the controller		
	100 mW (20 dBm) conducted	50 mW (17 dBm) conducted	
	Maximum output power depends on the regulatory domain in which the access point is installed		
Antenna	AIR-AP1010		
	<ul style="list-style-type: none"> <li>Two integrated 6 dBi patch antennas (2.4 and 5 GHz)</li> </ul>		
Antenna	AIR-AP1020 and AIR-AP1030		
	<ul style="list-style-type: none"> <li>Two integrated 6 dBi patch antennas (2.4 and 5 GHz)</li> <li>Three external antenna connectors</li> </ul>		
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)	5.15 to 5.25 GHz 5.25 to 5.35 GHz 5.475 to 5.725 GHz 5.725 to 5.85 GHz  (Depending on the regulatory domain in which the access point is installed)	
Data rates	1, 2, 5.5, and 11 Mbps	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	
Typical indoor range (across open office environment)	160 ft (49 m) @ 11 Mbps 410 ft (125 m) @ 1 Mbps	90 ft (27 m) @ 54 Mbps 180 ft (100 m) @ 18 Mbps 300 ft (91 m) @ 6 Mbps	45 ft (14 m) @ 54 Mbps 110 ft (34 m) @ 18 Mbps 165 ft (50 m) @ 6 Mbps
Compliance	The 1000 series access point complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings.		
	 <p><b>Caution</b> The power injector and power module have not been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.</p>		
Safety	Designed to meet:		
	<ul style="list-style-type: none"> <li>IEC 60950-1</li> <li>UL 60950-1</li> <li>CSA 60950-1</li> <li>EN 60950-1</li> <li>UL 2043</li> </ul>		
Radio Approvals	FCC Parts 15.247 Canada RSS-210 Japan ARIB-STD-33A Japan ARIB-STD-66 Europe EN-300.328	FCC Part 15.407 Canada RSS-210 Japan ARIB STD-T71 EN 301.893	

**Table C-1** Access Point Specifications (continued)

Category	Specifications		
	802.11b	802.11g	802.11a
EMI and Susceptibility	FCC Part 15.107 and 15.109 ICES-003 (Canada) EN 55022 EN 60601-1-2:2001 VCCI EN 301.489-1 EN 301.489-17 EN 55022 EN 55024		
RF Exposure	OET-65C RSS-102 ANSI C95.1		





## APPENDIX **D**

# Channels and Power Levels

---

For channel and maximum power level settings, refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges* document available on the Cisco Wireless documentation page of Cisco.com.

To browse to the document, follow these steps:

- 
- Step 1** Click this link to the Cisco Wireless documentation home page:  
[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)
  - Step 2** Click **Cisco Aironet 1000 Series** listed under Access Points.
  - Step 3** Click **Install and Upgrade Guides**.
  - Step 4** Click **Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges**.
-





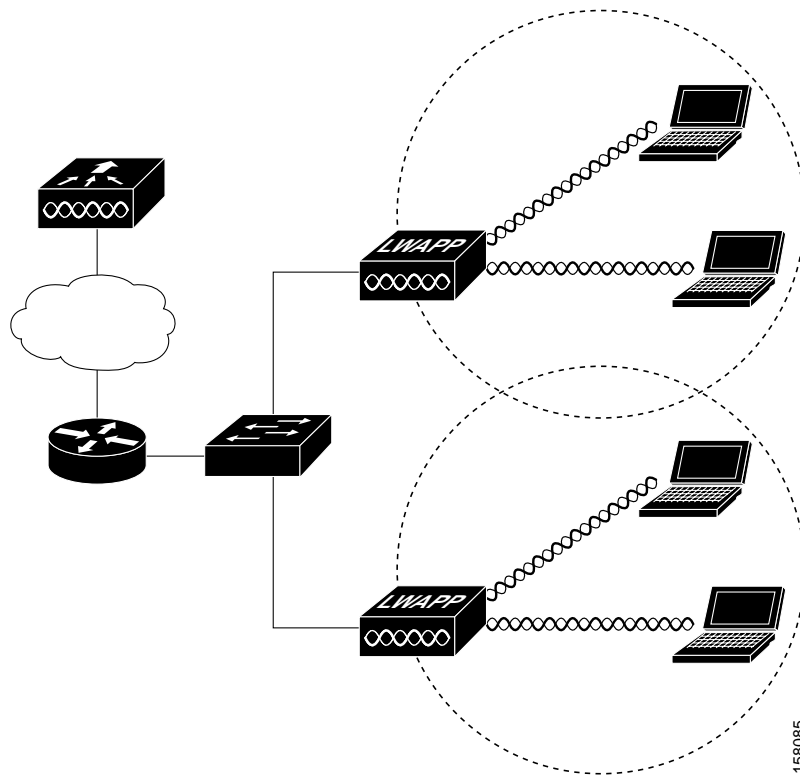
# APPENDIX **E**

## Priming Access Points Prior to Deployment

This section describes an optional procedure designed to prime or stage your access points in a convenient location rather than after they are installed in possibly difficult to reach locations. This helps limit potential installation problems to primarily Ethernet and power areas.

[Figure E-1](#) illustrates a typical priming configuration for your access points.

**Figure E-1** Typical Priming Configuration





Before deploying your access points to their final locations, follow these steps to prime your access points:

- Step 1** In a Layer 2 environment, where the access points are located on the same subnet as the controller, the access point communicates directly with the controller.
- Step 2** In a Layer 3 environment, ensure a DHCP server (typically on your switch) is enabled on the same subnet as your access points. The access points will receive its IP address and controller information using DHCP Option 43.

The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, OTAP, 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 [“Using DHCP Option 43” section on page 3-2](#) for more information.



**Note** For a Layer 3 access point on a different subnet than the controller, ensure the route to the controller has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure the routes to the primary, secondary, and tertiary controllers allow IP packet fragments.

- Step 3** Ensure that your controller is connected to a switch trunk port.
- Step 4** Configure the controller in LWAPP Layer 3 mode and ensure that its DS Port is connected to the switch. Use the CLI, web-browser interface, or Cisco WCS procedures as described in the appropriate controller guide.

- a.** In multi-controller environments, You can set one controller’s DS port to **Master** (you can use the *config network master-base disable* CLI command or you can use the controller GUI) so that new access points always associate with it. You can use the **show network config** CLI command to determine if the controller DS port is the master.

All access points associate to the master controller. From one location, you can configure access point settings such as primary, secondary, and tertiary controllers. This allows you to redistribute your access points to other controllers on the network.

You can also use a Cisco WCS server to control, configure, and redistribute all your access points from a single location.

- Step 5** Apply power to the access points:
- a.** Connect your access points to untagged access ports on your POE capable switch. You can optionally use power modules (AIR-PWR-1000=) or power injectors (AIR-PWRINJ-1000AF=) to power your access points.
- b.** After you power up the access point, it begins a power-up sequence that you can check by observing the access point LEDs. The red Alarm LED turns on for about 15 to 20 seconds and then all LEDs blink sequentially back and forth, indicating that the access point is trying to find a controller.



**Note** If the access point remains in this mode for more than 5 minutes, the access point is unable to find the master controller. Check the connection between the access point and the controller and ensure they are on the same subnet.

- c.** If the access point shuts down (all LEDs off), check to ensure that sufficient power is available.
- d.** When the access point associates with the controller, if the access point code version differs from the controller code version, the access point downloads the operating system code from the controller. All the access point LEDs blink simultaneously during the download.

- Step 6** If the operating system download is successful, the access point reboots. Normal operation is indicated when the Alarm LED is off, the Power LED is green, and the 2.4 GHz and 5 GHz LEDs are blinking to indicate radio activity.



---

**Note** If the Alarm LED remains red for more than a minute, remove power from the access point and contact Cisco Technical Support for assistance.

---

- Step 7** Use the controller CLI, controller GUI, or Cisco WCS to configure the access point with primary, secondary, and tertiary controller names.
- Step 8** If the access point is in a Controller Mobility Group, use the controller CLI, controller GUI, or Cisco WCS to configure the Controller Mobility Group name.
- Step 9** Use controller CLI, controller GUI, or Cisco WCS to configure the access point-specific 802.11a, 802.11b, and 802.11g network settings.
- Step 10** If the configuration priming was successful, the Power LED is green, the Alarm LED is off, and the radio LEDs are blinking to indicate normal operation.
- Step 11** Repeat Steps 4 to 9 for each access point.

When you successfully complete the configuration priming of all your access points, ensure the Master setting is disabled on your controller. You can begin deploying the access points to their final destinations (refer to the [“Deploying the Access Points on the Wireless Network”](#) section on page 2-7).

---





## APPENDIX **F**

# Configuring DHCP Option 43

---

This appendix describes the steps needed to configure DHCP Option 43 on a Windows 2003 Enterprise DHCP server, such as a Cisco Catalyst 3750 series switch, for use with lightweight access points. This appendix contains these sections:

- [Overview, page F-2](#)
- [Configuring Option 43 for 1000 Series Access Points, page F-3](#)
- [Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Access Points, page F-4](#)

# Overview

This section contains 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 the DHCP server documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.


**Note**

DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

Cisco Aironet 1000 series access points use a comma-separated string format for DHCP Option 43. Other Cisco Aironet access points use 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 60). The VCI strings for Cisco access points capable of operating in lightweight mode are listed in [Table F-1](#):

**Table F-1**      *Lightweight Access Point VCI Strings*

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	A irespace A P1200
Cisco Aironet 1100 series	C isco A P c1100
Cisco Aironet 1130 series	C isco A P c1130
Cisco Aironet 1200 series	C isco A P c1200
Cisco Aironet 1240 series	C isco A P c1240
Cisco Aironet 1300 series	C isco A P c1300
Cisco Aironet 1500 series	C isco A P L A P1510

The format of the TLV block for 1100, 1130, 1200, 1240, and 1300 series access points is listed below:

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

# Configuring Option 43 for 1000 Series Access Points

To configure DHCP Option 43 for Cisco 1000 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

- 
- Step 1** Enter configuration mode at the Cisco IOS command line interface (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 AP1000
<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 60 line using the following syntax:

```
option 60 ascii "Airespace.AP1200"
```

The quotation marks must be included.

- Step 4** Add the option 43 line using the following syntax:

```
option 43 ascii "Comma Separated IP Address List"
```

For example, if you are configuring option 43 for Cisco 1000 series access points using the controller IP addresses 10.126.126.2 and 10.127.127.2, add the following line to the DHCP pool in the Cisco IOS CLI:

```
option 43 ascii "10.126.126.2,10.127.127.2"
```

The quotation marks must be included.

---

# Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Access Points

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, and 1300 series lightweight access points 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 AP1240  
 <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 60 line using the following syntax:

```
option 60 ascii "VCI string"
```

For the *VCI string*, use the value from [Table F-1](#). The quotation marks must be included.

- Step 4** 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 listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```

---



## INDEX

---

### A

- access point
  - discovery [1-1](#)
  - guidelines [1-2](#)
  - types [1-4](#)
- administrative rules, Taiwan [B-9](#)
- antennas
  - external [1-5](#)
  - integrated [C-2](#)
- anti-theft feature [1-6](#)

---

### C

- Canadian compliance [B-4](#)
- ceiling-mount clips [2-11](#)
- ceiling mounting process [2-10](#)
- configuring DHCP Option 43 [F-2](#)
- conformity statement [B-2](#)
- connectors [C-1](#)
  - left side [1-3](#)
  - right side [1-4](#)
- controller [1-1](#)
- controller discovery process [2-6](#)

---

### D

- data rates [C-2](#)
- declarations of conformity [B-1](#)
- deployment
  - access points [2-7](#)
  - process [2-7](#)
- DHCP Option 43 [3-2, F-1](#)

- DHCP pool [F-2](#)
- discovery process
  - DHCP server [2-7](#)
  - DNS server [2-7](#)
  - Layer 2 [2-6](#)
  - locally stored [2-6](#)
  - Over-the-air wireless (OTW) [2-6](#)
- dual radio [1-4](#)

---

### E

- EMI and susceptibility standards [C-3](#)
- Ethernet
  - connector [2-18](#)
  - port [1-5](#)
- extended temperature range [2-3, 2-4](#)

---

### F

- FCC Declaration of Conformity [B-2](#)
- frequency range [C-2](#)

---

### G

- guidelines
  - installation [2-3](#)
  - operating in Japan [B-8](#)
  - using access points [3-2](#)

---

### H

- hardware features [1-2](#)



**I**

inline power [2-18](#)  
input power [C-1](#)  
input voltage [C-1](#)  
installation guidelines [2-3](#)

**K**

key features [1-2](#)  
keyhole slots [1-6](#)

**L**

Layer 2 operation [1-8](#)  
Layer 3 operation [1-2, 1-7](#)  
LED indicators

- location [3-3, C-1](#)
- markings [1-5](#)
- power up sequence [2-19](#)
- signals [3-4](#)

lightweight access points [1-1](#)  
low power condition [3-5](#)  
LWAPP [1-1](#)

**M**

MAC information [2-20](#)  
modulation [C-1](#)  
mounting

- ceiling [2-10](#)
- flush-mount bracket [2-15](#)
- projection-mount bracket [2-14](#)
- suspended ceiling clips [2-11](#)
- vertical wall [2-13](#)

mounting options [2-8](#)

**O**

operating temperature [C-1](#)

**P**

package contents [2-3](#)  
power

- cabling [2-17](#)
- connector [2-18](#)
- input [C-1](#)
- options [2-17](#)
- output [C-2](#)
- sources [1-5](#)

power injector [2-17](#)  
power module [2-17](#)  
priming access points [E-1](#)  
process, controller discovery [2-6](#)

**R**

radio

- approvals [C-2](#)
- integrated [1-1](#)
- range [C-2](#)

regulatory

- information [B-1](#)

RF exposure [B-7](#)  
RF exposure standards [C-3](#)

**S**

Safety Compliance, FCC [2-2](#)  
safety standards [C-2](#)  
safety warnings, translated [A-1](#)  
securing the access point [2-17](#)  
size [C-1](#)  
specifications [C-1](#)

---

**T**

temperature

operating [C-1](#)

storage [C-1](#)

troubleshooting [3-1](#)

type-length-value (TLV) [F-2](#)

---

**U**

UL2043 [1-6, C-2](#)

unpacking [2-3](#)

---

**V**

Vendor Class Identifier (VCI) [F-2](#)

vendor class identifier (VCI) [F-2](#)

---

**W**

warnings [2-2, A-1](#)

weight [C-1](#)

Wireless Domain Services (WDS) [1-2](#)

