



CISCO CONFIDENTIAL - Draft A1



Cisco Aironet 1250 Series Access Point Hardware Installation Guide

June 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-8247-02

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.



CISCO CONFIDENTIAL - Draft A1

CONTENTS

Preface ix

Audience ix

Purpose ix

Organization ix

Conventions x

Related Publications xii

Locating the Product Serial Number xiii

Obtaining Documentation, Obtaining Support, and Security Guidelines xiv

CHAPTER 1

Overview 1-1

Product Terminology 1-1

Autonomous Access Points 1-1

Lightweight Access Points 1-2

Guidelines for Using Cisco Aironet Lightweight Access Points 1-2

Hardware Features 1-3

Radio Module Slots 1-5

Single or Dual-Radio Operation 1-5

Operating Modes 1-5

Transmit Beam Forming 1-5

Maximum Ratio Combining 1-6

Antennas Supported 1-6

LEDs 1-6

Ethernet Port 1-7

Console Port 1-7

Power Sources 1-7

UL 2043 Compliance 1-8

Anti-Theft Features 1-9

Network Examples with Autonomous Access Points 1-10

Root Unit on a Wired LAN 1-10

Repeater Unit that Extends Wireless Range 1-11

Central Unit in an All-Wireless Network 1-12

Bridge Network with Wireless Clients 1-12

Workgroup Bridge Network 1-13

CISCO CONFIDENTIAL - Draft A1

Point-to-Point Bridge Configuration	1-14
Network Example with Lightweight Access Points	1-14

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	2-4
Before Beginning the Installation	2-4
Access Point Bottom Connector Access Openings	2-4
Installation Summary	2-5
Mounting Overview	2-5
Mounting on a Horizontal or Vertical Surface	2-7
Mounting Below a Suspended Ceiling	2-8
Mounting Above a Suspended Ceiling	2-9
Mounting Access Point on a Desktop or Shelf	2-13
Connecting the Ethernet and Power Cables	2-14
Connecting to an Ethernet Network with an Inline Power Source	2-15
Connecting to an Ethernet Network with Local Power	2-16
Powering Up the Access Point	2-16
Installing or Removing the Mounting Plate Latch	2-17
Installing the Mounting Plate Latch	2-17
Removing the Mounting Plate Latch	2-17
Installing the Access Point to the Mounting Plate	2-18
Mounting Plate Not Attached to a Surface	2-18
Mounting Plate Attached to a Surface	2-19
Securing the Access Point	2-20
Securing the Access Point to the Mounting Plate	2-20
Using a Security Cable to Secure the Access Point	2-22
Removing the Access Point From the Mounting Plate	2-23
Removing a Radio Module	2-24
Inserting a Radio Module	2-26

CISCO CONFIDENTIAL - Draft A1**CHAPTER 3****Troubleshooting 1250 Series Autonomous Access Points 3-1**

Checking the Autonomous Access Point LEDs	3-2
Checking the Power Injector LEDs	3-4
Checking Basic Settings	3-5
Default IP Address Behavior	3-5
Enabling the Radio Interfaces	3-5
SSID	3-6
WEP Keys	3-6
Security Settings	3-6
Low Power Condition on Autonomous Access Points	3-6
Intelligent Power Management - need changes	3-7
Inline Power Status Messages	3-8
Configuring Power Using the CLI - needs changes	3-10
Issuing the Cisco IOS Command Using the CLI	3-12
Configuring the Access Point System Power Settings Using a Browser - Need changes	3-12
Running the Carrier Busy Test - Needs changes	3-14
Running the Ping Test - Needs Changes ??	3-15
Resetting to the Default Configuration	3-16
Using the MODE Button	3-16
Using the Web Browser Interface	3-16
Reloading the Access Point Image - Needs Changes ??	3-17
Using the MODE Button	3-17
Web Browser Interface	3-18
Browser HTTP Interface	3-18
Browser TFTP Interface	3-19
Obtaining the Access Point Image File	3-20
Connecting to the Access Point Locally	3-20
Obtaining the TFTP Server Software	3-21

CHAPTER 4**Troubleshooting 1250 Series Lightweight Access Points 4-1**

Guidelines for Using Cisco Aironet Lightweight Access Points	4-2
Using DHCP Option 43	4-2
Checking the Lightweight Access Point LEDs	4-3
Checking the Power Injector LEDs	4-5
Low Power Condition for Lightweight Access Points	4-6
Intelligent Power Management - need changes	4-7
Inline Power Status Messages	4-7

CISCO CONFIDENTIAL - Draft A1

Configuring Power Using Controller CLI Commands	4-10
Manually Configuring Controller Information Using the Access Point CLI	4-11
Configuring Controller Information	4-12
Clearing Manually Entered Controller Information	4-12
Manually Resetting the Access Point to Defaults	4-12
Returning the Lightweight Access Point to Autonomous Mode	4-12
Using a Controller to Return the Access Point to Autonomous Mode	4-13
Using the MODE Button to Return the Access Point to Autonomous Mode	4-13
MODE Button Setting	4-14
Obtaining the Autonomous Access Point Image File	4-14
Connecting to the Access Point Locally	4-14
Obtaining the TFTP Server Software	4-15

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-4
Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC	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

CISCO CONFIDENTIAL - Draft A1**APPENDIX C****Access Point Specifications C-1****APPENDIX D****Channels and Power Levels D-1****APPENDIX E****Console Cable Pinouts E-1**

Overview E-2

Console Port Signals and Pinouts E-2

APPENDIX F**Priming Lightweight Access Points Prior to Deployment F-1****APPENDIX G****Configuring DHCP Option 43 for Lightweight Access Points G-1**

Overview G-2

Configuring Option 43 for 1000 Series Access Points G-2

Configuring Option 43 for 1100, 1130, 1200, 1240, 1250, and 1300 Series Lightweight Access Points G-3

GLOSSARY**INDEX**

CISCO CONFIDENTIAL - Draft A1



CISCO CONFIDENTIAL - Draft A1

Preface

Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1250 Series Access Point. The 1250 series access point is available in autonomous and lightweight configurations.

To use this guide with autonomous access points, you should have experience working with Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

To use this guide with lightweight access points, 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 autonomous or lightweight access point.

For detailed information about Cisco IOS commands used with autonomous access points, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS Release 12.4 commands, refer to the Cisco IOS documentation set available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline**.

For information about 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.

CISCO CONFIDENTIAL - Draft A1

Chapter 3, “Troubleshooting 1250 Series Autonomous Access Points,” provides troubleshooting procedures for basic problems with the autonomous access point.

Chapter 4, “Troubleshooting 1250 Series Lightweight Access Points” provides troubleshooting procedures for basic problems with the lightweight access point.

Appendix A, “Translated Safety Warnings,” provides instructions for locating 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,” provides instructions for locating the autonomous and lightweight access point radio channels and the maximum power levels supported by the world’s regulatory domains.

Appendix E, “Console Cable Pinouts,” identifies the pinouts for the serial console cable that connects to the access point’s serial console port.

Appendix F, “Priming Lightweight Access Points Prior to Deployment,” describes the procedure to prime access points with controller information.

Appendix G, “Configuring DHCP Option 43 for Lightweight Access Points,” describes the procedure to configure DHCP Option 43 for lightweight access points.

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.

CISCO CONFIDENTIAL - Draft A1**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 Körperverschüttung 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].)

CISCO CONFIDENTIAL - Draft A1

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”).
¡Advertencia!	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.”)
Varning!	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].)

Related Publications

These documents provide information about the autonomous access point:

- *Release Notes for Cisco Aironet 1250 Series Access Point*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*

These documents provide information about the lightweight access point and the controller:

- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*
- *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

To browse to the 1250 series access point documentation, click **Cisco Aironet 1250 Series** listed under Access Points.

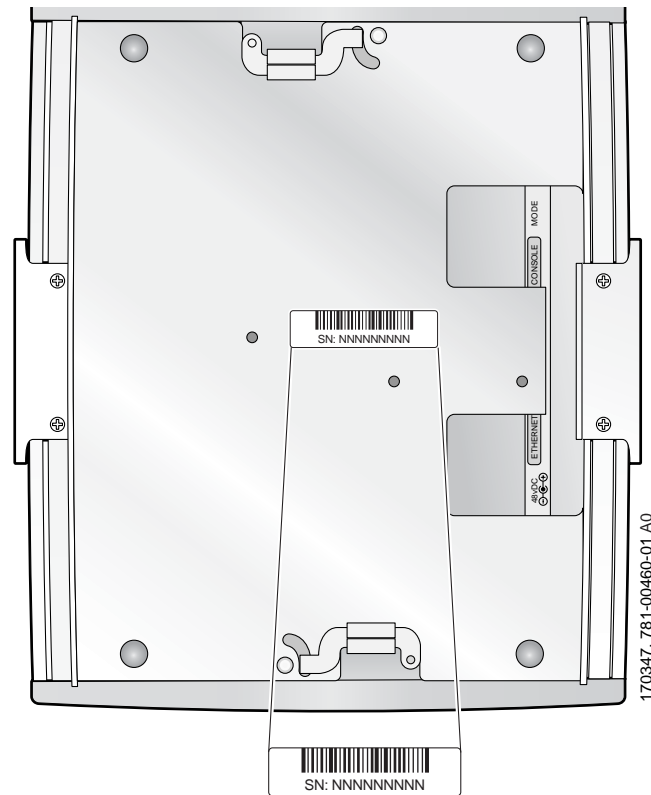
To browse to the Cisco Wireless LAN Controller documentation, click **Cisco 4400 Series Wireless LAN Controllers** or **Cisco 2000 Series Wireless LAN Controllers** listed under Wireless LAN Controllers.

CISCO CONFIDENTIAL - Draft A1

Locating the Product Serial Number

The access point serial number is located on the bottom of the access point case (see [Figure 1](#)).

Figure 1 **Location of Serial Number Label**



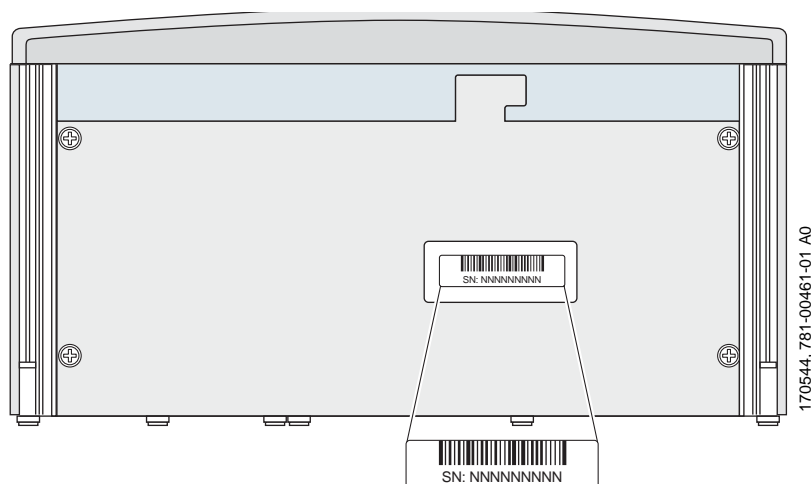
The access point serial number label contains the following information:

- Model number, such as *AIR-API251AG-A-k9* or *AIR-LAP1251AG-A-k9*
- Serial number, such as *VDF06367ABC* (11 alphanumeric digits)
- Ethernet MAC address, such as *00abc65094f3* (12 hexadecimal digits)
- Location of manufacture, such as *Made in Singapore*

CISCO CONFIDENTIAL - Draft A1

The radio module serial number is located on the bottom of the radio module case (see [Figure 2](#)).

Figure 2 **Location of Radio Module Serial Number Label**



The radio module serial number label contains the following information:

- Model number, such as AIR-RM1252A-A-K9 or AIR-RM1252G-A-K9
- Serial number, such as *VDF06367ABC* (11 alphanumeric digits)
- Radio 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>



CISCO CONFIDENTIAL - Draft A1

CHAPTER 1

Overview

The Cisco Aironet 1250 Series Access Point is available in autonomous and lightweight configurations. The autonomous access points can support standalone network configurations with all configuration settings maintained within the access points. The lightweight access points operate in conjunction with a Cisco wireless LAN controller with all configuration information maintained within the controller.

The 1250 series access point is a Wi-Fi certified, wireless LAN transceiver. The access point supports two (draft IEEE 802.11n version 2.0) radio modules: a 2.4-GHz radio and a 5-GHz radio.

You can configure the radios separately, using different settings on each. The access point connects wireless and wired networks or is the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless access to the network.

Product Terminology

The following terms refer to the autonomous and lightweight products:

- The term *access point* describes both autonomous and lightweight products.
- The term *autonomous access point* describes only the autonomous product.
- The term *lightweight access point* describes only the lightweight product.
- The term *access point* describes the product when configured to operate as an access point.
- The term *bridge* describes the product when configured to operate as a bridge.

Autonomous Access Points

The autonomous access point (model: AIR-AP1252) supports a management system based on Cisco IOS software. The access point serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless access to the network. You can configure and monitor the access point using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

CISCO CONFIDENTIAL - Draft A1

Lightweight Access Points

The lightweight access point (model: AIR-LAP1252) is part of the Cisco Integrated Wireless Network Solution and requires no manual configuration before being mounted. The lightweight access point is automatically configured by a Cisco wireless LAN controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

In the Cisco Centralized Wireless LAN architecture, access points operate in lightweight mode (as opposed to autonomous mode). The lightweight access points associate to a controller. The controller manages the configuration, firmware, and controls 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 lightweight access point an LWAPP join response allowing the access point to join the controller. When the access point is joined, the access point downloads its software if the versions on the access point and controller do not match. After an access point joins a controller, you can reassign it to any controller on your network.

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

This chapter provides information on the following topics:

- [Guidelines for Using Cisco Aironet Lightweight Access Points, page 1-2](#)
- [Hardware Features, page 1-3](#)
- [Network Examples with Autonomous Access Points, page 1-11](#)

Guidelines for Using Cisco Aironet Lightweight Access Points

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

- Lightweight access points can communicate only with Cisco 2006 series wireless LAN controllers or 4400 series controllers. Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series controllers are not supported because they lack the memory required to support access points running Cisco IOS software.
- Lightweight access points do not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- Lightweight access points support eight BSSIDs per radio and a total of eight wireless LANs per access point. When a lightweight access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- Lightweight access points do not support Layer 2 LWAPP. They must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- The lightweight access point console port is enabled for monitoring and debugging purposes (all configuration commands are disabled when the access point is associated to a controller).

CISCO CONFIDENTIAL - Draft A1

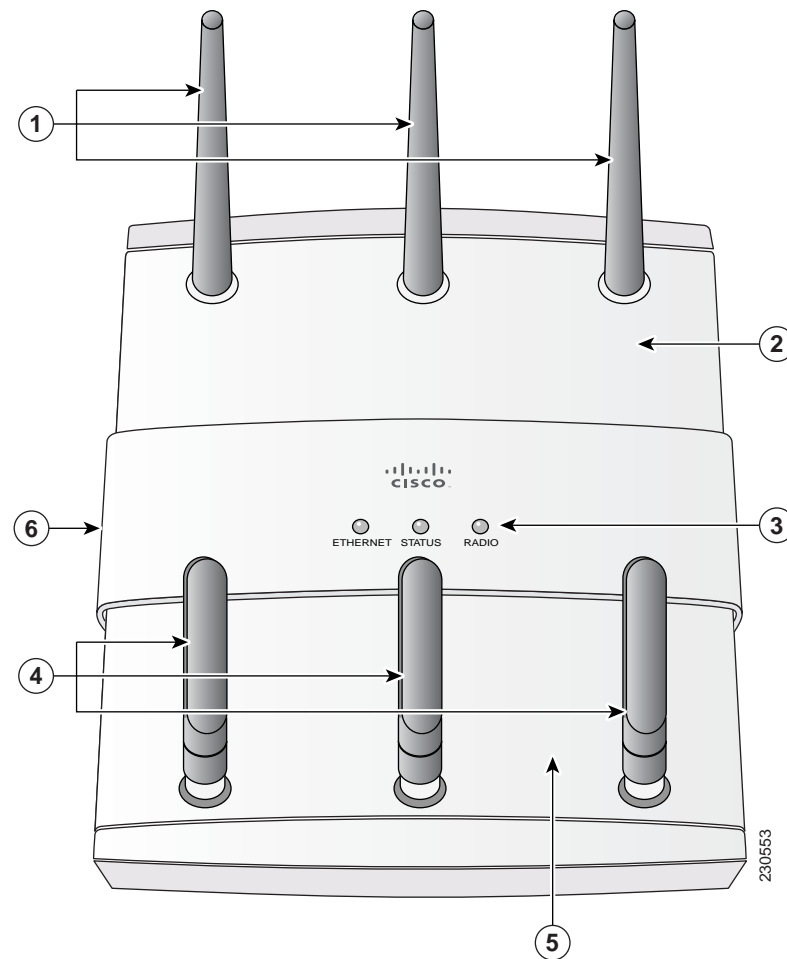
Hardware Features

Key hardware features of the access point include:

- Two radio module slots for single or dual-radio operation (see [page 1-5](#))
- Ethernet port (see [page 1-7](#)) and console port (see [page 1-8](#))
- LEDs, (see [page 1-8](#))
- Multiple power sources (see [page 1-8](#))
- UL 2043 compliance (see [page 1-9](#))
- Anti-theft features (see [page 1-10](#))

[Figure 1-1](#) shows the access point with two radio modules installed.

Figure 1-1 Access Point with 2.4-GHz and 5-GHz Radio Modules



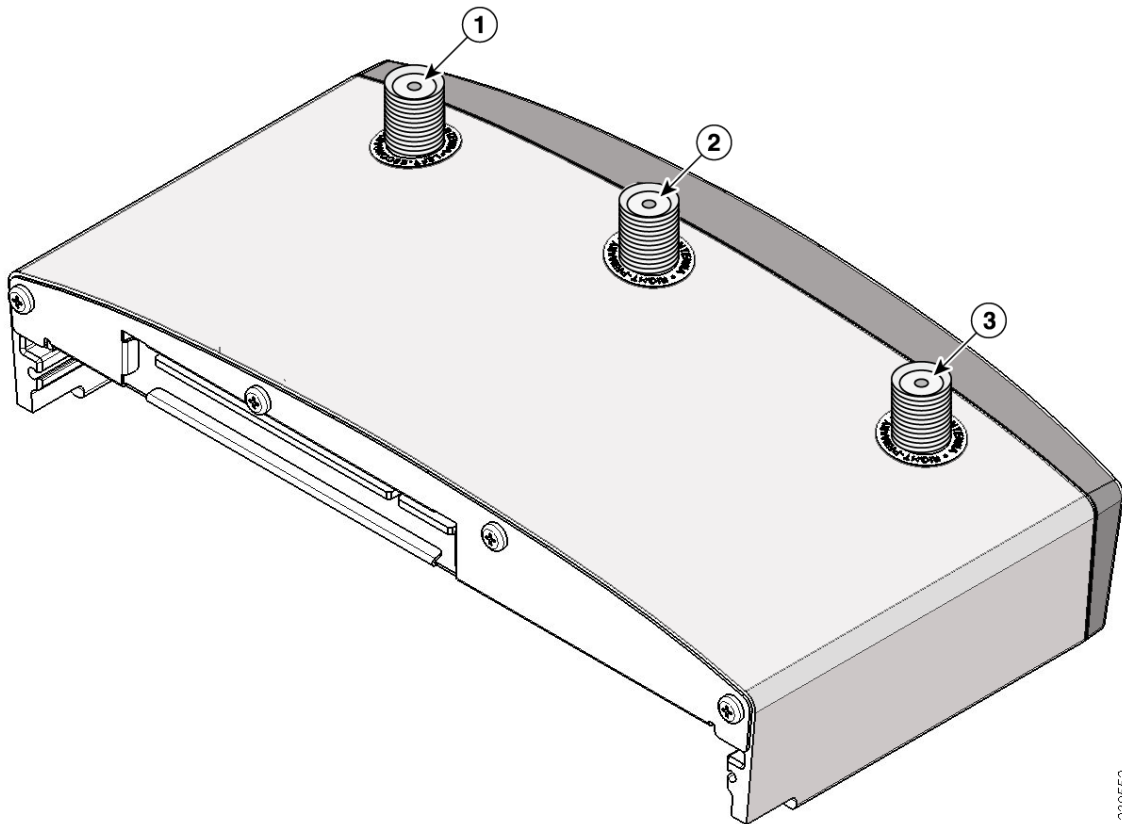
1	2.4-GHz radio antenna	4	5-GHz radio antenna
2	Module slot 0 (2.4-GHz radio module shown)	5	Module slot 1 (5-GHz radio module shown)
3	LEDs	6	PC cable security slot

CISCO CONFIDENTIAL - Draft A1

Figure 1-2 illustrates a radio module. The access point supports three types of modules:

- 2.4-GHz radio module—contains a 2.4-GHz (draft IEEE 802.11n version 2.0) radio and three radio connectors
- 5-GHz radio module—contains a 5-GHz (draft IEEE 802.11n version 2.0) radio and three radio connectors (identified with blue labels).
- Blank module—does not contain a radio or radio connectors.

Figure 1-2 Radio Module - new pic



1	Radio antenna connector (A-Tx/Rx)	3	Radio antenna connector (C-Rx)
2	Radio antenna connector (B-Tx/Rx)		


Note

The 5-GHz antennas have a blue dot or blue label to correspond to the blue labels around the antenna connectors on the 5-GHz radio module.

230552

CISCO CONFIDENTIAL - Draft A1

Radio Module Slots

The access point has two radio module slots: Slot 0 and Slot 1 (see [Figure 1-1](#)). The radio modules can be initially placed in any slot before the radios are configured with non-default parameters. New radio configuration changes are associated with the specific module slot in which the radio module is located.

When the default radio settings are changed, the radio modules should not be moved to a different slot. After configuration changes are made, moving the radio modules to a different modules slot requires that you re-configuring the radio settings for that slot.

Single or Dual-Radio Operation

The access point supports single or simultaneous dual radio (draft IEEE 802.11n version 2.0) operation using 2.4-GHz and 5-GHz radio modules. Each radio module contains an integrated radio with three antenna connectors. A blank module is supported for single radio access point configurations.

**Note**

The draft IEEE 802.11n version 2.0 radio modules support field upgrading to full 802.11n support when the standard is finalized.

The 2.4-GHz radio supports 802.11b, 802.11g, and 802.11n modes of operation. The 2.4-GHz radio also supports 1 or 2 transmitting antennas and up to 3 receiving antennas.

The 5-GHz radio supports 802.11a and 802.11n modes of operation. The radio supports the Unlicensed National Information Infrastructure (UNII-1, UNII-2, and UNII-3), and the European Telecommunications Standards Institute /industrial, scientific and medical (ETSI/ISM) frequency bands. The 5-GHz radio also supports 1 or 2 transmitting antennas and up to 3 receiving antennas.

Operating Modes

The 2.4 GHz radio module supports **six** operating modes:

- 802.11b single transmit antenna
- 802.11g single transmit antenna
- 802.11g dual transmit antennas
- 802.11g dual transmit antennas with beam forming??
- 802.11n HT-20 MHz with dual transmit antennas
- 802.11n HT-40 MHz with dual transmit antennas

The 5 GHz radio module supports **six** operating modes:

- 802.11a single transmit antenna
- 802.11a dual transmit antennas
- 802.11a dual transmit antennas with beam forming??
- 802.11n HT-20 MHz with dual transmit antennas
- 802.11n duplicate (2x20) HT-20 MHz with dual transmit antennas
- 802.11n HT-40 MHz with dual transmit antennas

CISCO CONFIDENTIAL - Draft A1**Spatial Multiplexing**

The radio modules can support two transmitters to achieve higher data rates for a given bandwidth. This technique is called multiple input multiple output (MIMO) and relies on the premise that, via multi-path, two transmitted signals take different paths to the receivers. Using special data packet features allows the receivers to distinguish between the two transmitted signals and increases the access point data rate.

Maximum Ratio Combining

The radio modules use three receivers to support maximum ratio combining (MRC) to enhance receiver performance. MRC is a technique that combines the signals from multiple receivers in a manner to optimize the signals. MRC can provide up to 3 dB of increased receive signal strength in all modes of operation.

Antennas Supported

Table 1-1 lists the supported access point antennas.

**Caution**

The access point, antennas, and all interconnected equipment must be located indoors within the same building, including the associated LAN connections.

**Note**

The access point has been designed to operate with the antennas listed below and having a maximum gain of 10 dBi for 2.4 GHz and 6 dBi for 5 GHz. Antennas not included in this list or having a higher gain are strictly prohibited for use with the access point. The required antenna impedance is 50 ohms.

**Note**

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the equivalent isotropically radiated power (e.i.r.p.) is not more than required for successful communication.

Table 1-1 Supported Antennas

2.4-GHz Antennas	Gain (dBi)	5-GHz Antennas	Gain (dBi)
AIR-ANT5959 ¹ diversity ceiling omnidirectional	2	AIR-ANT5135DG-R non-articulated omnidirectional	3.5
AIR-ANT2422DG-R non-articulated dipole	2.2	AIR-ANT5135D-R articulating dipole	3.5
AIR-ANT4941 articulating dipole	2.2	AIR-ANT5140V-R omnidirectional	4
AIR-ANT2430V-R omnidirectional	3	AIR-ANT5145V-R ¹ diversity ceiling omnidirectional	4.5
AIR-ANT1728 ceiling omnidirectional	5.2	AIR-ANT5160V-R ¹ omnidirectional	6

CISCO CONFIDENTIAL - Draft A1**Table 1-1 Supported Antennas (continued)**

2.4-GHz Antennas	Gain (dBi)	5-GHz Antennas	Gain (dBi)
AIR-ANT2506 mast mount omnidirectional	5.2		
AIR-ANT3213 diversity pillar omnidirectional	5.2		
AIR-ANT2460P-R ¹ ceiling omnidirectional	6		
AIR-ANT2465P-R ¹ diversity patch directional	6.5		
AIR-ANT2485P-R ¹ patch directional	8.5		
AIR-ANT2410Y-R yagi directional	10		

1. The antenna has an attached UL2043 rated antenna cable.

LEDs

The access point has three LEDs (see [Figure 1-1](#)) to indicate Ethernet activity, radio activity, and status indications (refer to the “[Checking the Autonomous Access Point LEDs](#)” section on page 3-2 or the “[Checking the Lightweight Access Point LEDs](#)” section on page 4-3 for additional information).

- The Status LED provides general operating status and error indications.
- The Ethernet LED signals Ethernet traffic on the wired Ethernet LAN and provides Ethernet error indications.
- The Radio LED signals that wireless packets are being transmitted or received over the radio interface and provides error indications.

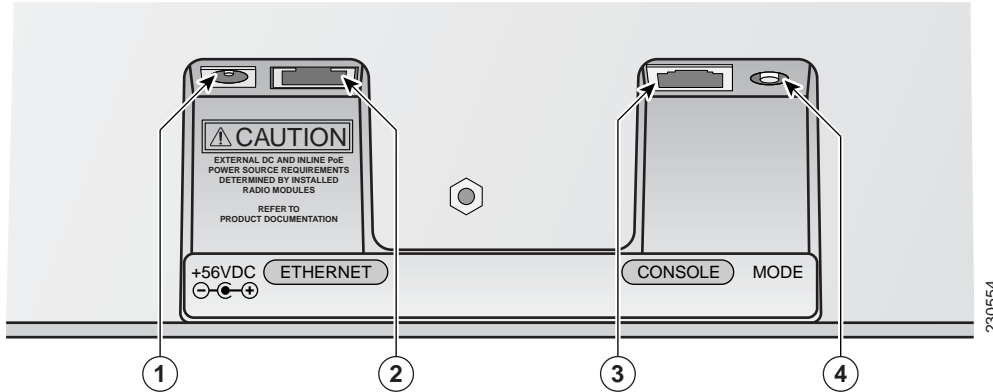
Ethernet Port

The Ethernet port is located on the bottom of the unit in the access point connector area (see [Figure 1-3](#)). The auto-sensing Ethernet port accepts an RJ-45 connector, linking the access point to your 10BASE-T, 100BASE-T, or 1000BASE-T Ethernet LAN. The Ethernet interface supports automatic media dependent interface crossover (MDIX) detection, which automatically senses cable type (straight-through or crossover) and adjusts the internal connections appropriately. Also the interface automatically senses the data rates being used over the connected cable.

The access point can receive power through the Ethernet cable from a 1250 series power injector. The Ethernet MAC address is printed on the label on the bottom of the access point.

CISCO CONFIDENTIAL - Draft A1

Figure 1-3 Access Point Connector Area



1	DC power connector (+56 VDC)	3	Console port (RJ-45)
2	Ethernet port (RJ-45)	4	MODE button

Console Port

The console port is located on the bottom of the unit in the access point connector area (see [Figure 1-3](#)). The console port provides access to the access point's command-line interface (CLI) using a terminal emulator program. Use an RJ-45 to DB-9 serial cable to connect your computer's COM port to the access point's serial console port. Assign the following port settings to a terminal emulator to open the management system pages: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.



Note

After completing your configuration changes, you must remove the serial cable from the access point.

The serial cable can be purchased from Cisco (part number AIR-CONCAB1200) or can be built using the pinouts in [Appendix E, "Console Cable Pinouts."](#)

Power Sources

The access point can receive power from a 1250 series DC power module or from inline power using the Ethernet cable. The access point supports the IEEE 802.3af inline power standard and Cisco CDP Power Negotiation. Using inline power, you do not need to run a power cord to the access point because power is supplied over the Ethernet cable.

The access point supports the following power sources:

- 23 W—Cisco Aironet 1250 series DC power module (AIR-PWR-SPLY1)
- Inline power:
 - 23W—Cisco Aironet 1250 series power injector (AIR-PWRINJ4)
 - 13W— IEEE 802.3af (with only one radio module installed)



Note

Current switches and patch panels do not provide enough power (23 W) to operate the access point with both 2.4-GHz and 5-GHz radios. 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

CISCO CONFIDENTIAL - Draft A1

over-current condition. The access point also activates a Status LED low power error indication and creates an error log entry (refer to the [“Checking the Autonomous Access Point LEDs”](#) section on page 3-2 or the [“Checking the Lightweight Access Point LEDs”](#) section on page 4-3).

UL 2043 Compliance

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

The 1250 series power injector (AIR-PWRINJ4), the 1250 series DC power module (AIR-PWR-SPLY1), and the antennas are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

CISCO CONFIDENTIAL - Draft A1**Anti-Theft Features**

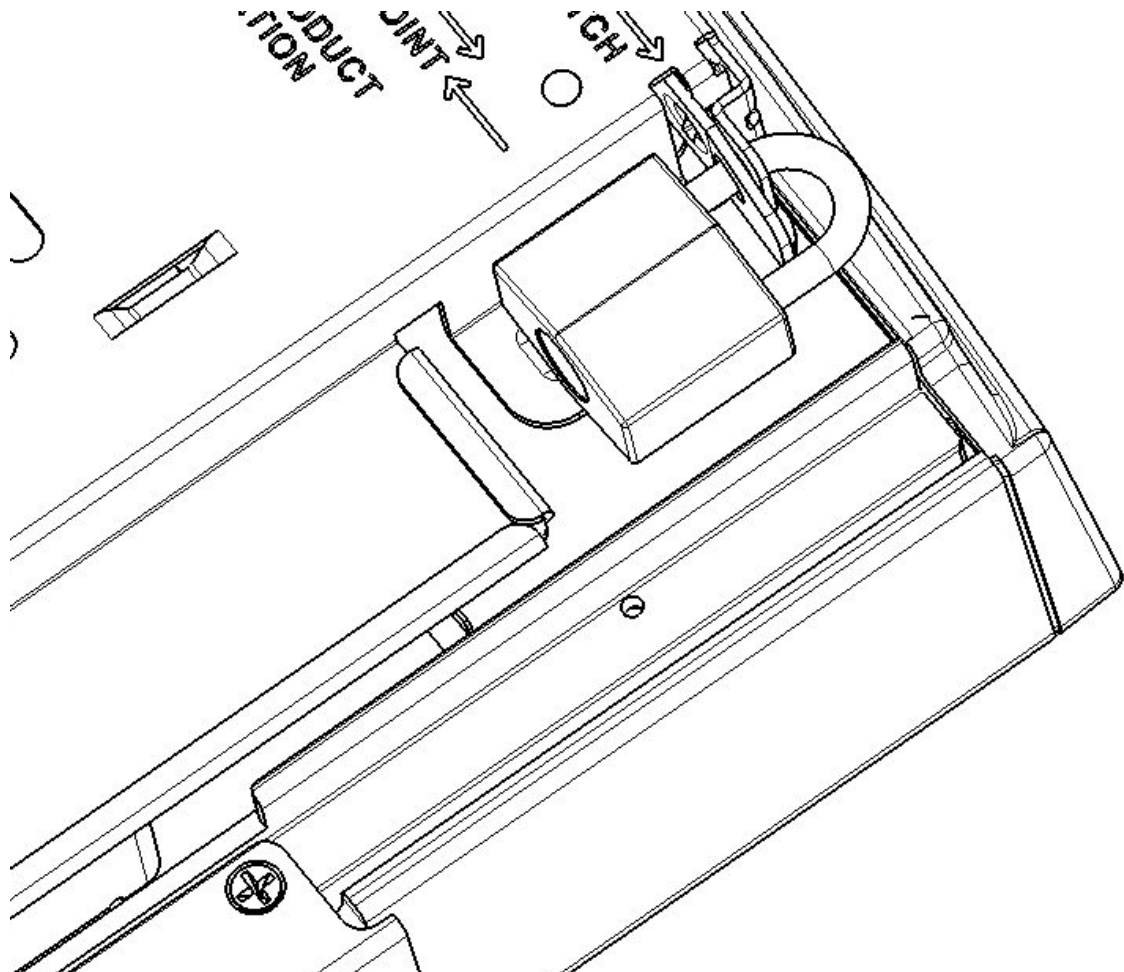
There are two methods of securing the access point:

- Padlock—You can lock the access point to the mounting plate with a padlock (see [Figure 1-4](#)). This prevents removing the radio modules and blocks access to the access point connector area. Compatible padlocks are Master Lock models 120T and 121T or equivalent. For additional information, refer to the [“Securing the Access Point”](#) section on page 2-22.
- Security cable keyhole—You can use the security cable slot (see [Figure 1-1](#)) to secure the access point using a standard security cable, like those used on laptop computers (refer to the [“Securing the Access Point”](#) section on page 2-22).

**Note**

The mounting plate and padlock are required to prevent removal of the radio modules.

Figure 1-4 Access Point with Padlock-



170349

CISCO CONFIDENTIAL - Draft A1

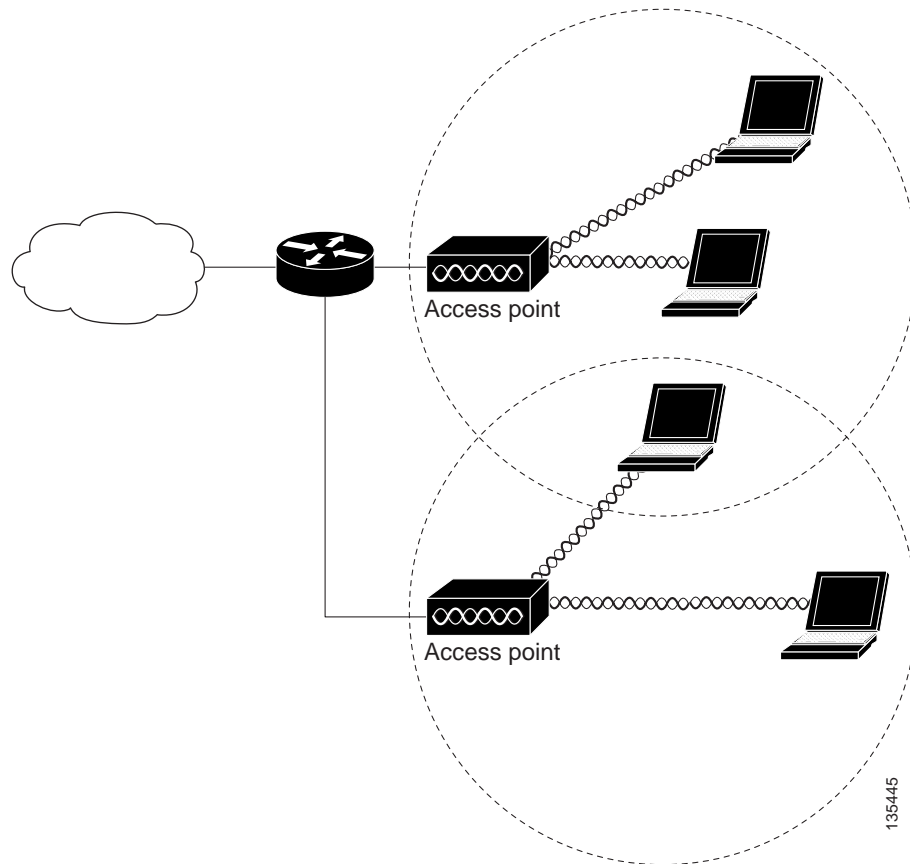
Network Examples with Autonomous Access Points

This section describes the access point's role in three common wireless network configurations. The access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. [Figure 1-5](#) shows access points acting as root units on a wired LAN.

Figure 1-5 Access Points as Root Units on a Wired LAN



CISCO CONFIDENTIAL - Draft A1

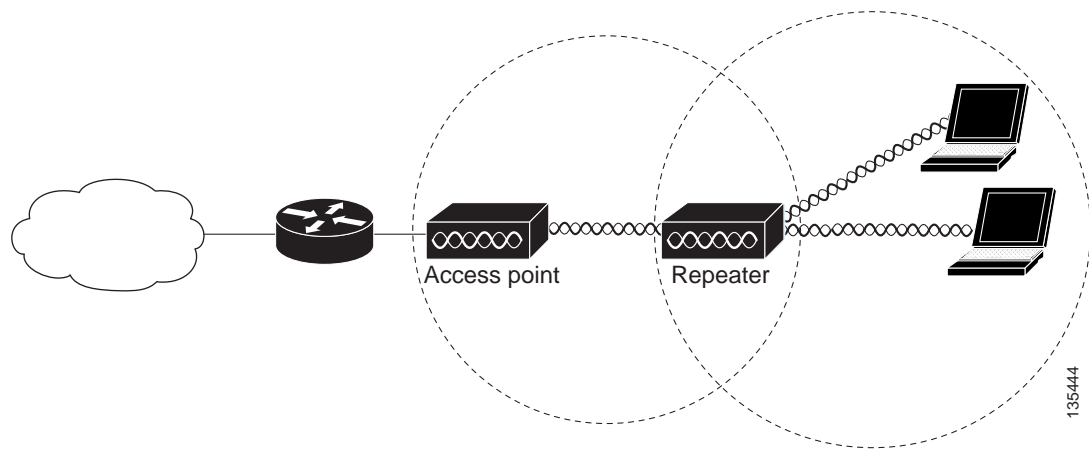
Repeater Unit that Extends Wireless Range

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. [Figure 1-6](#) shows an access point acting as a repeater. Consult the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting up the roles.

**Note**

Non-Cisco client devices might have difficulty communicating with repeater access points.

Figure 1-6 Access Point as Repeater



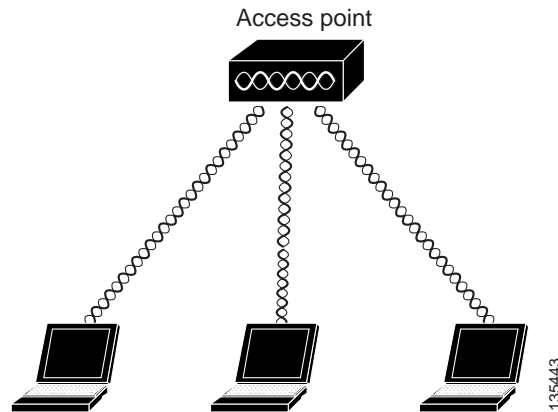
135/44

CISCO CONFIDENTIAL - Draft A1

Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. [Figure 1-7](#) shows an access point in an all-wireless network.

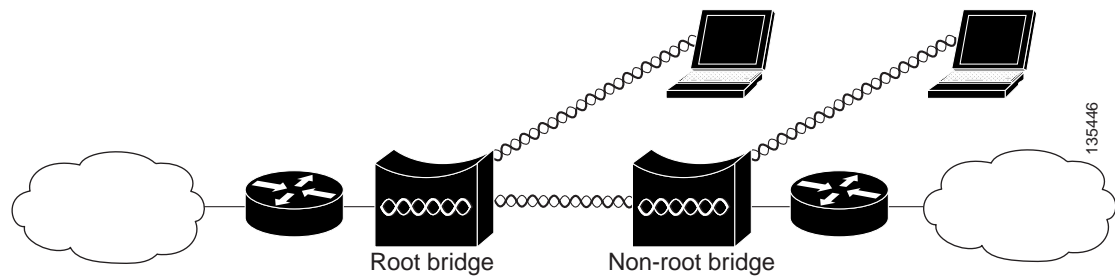
Figure 1-7 Access Point as Central Unit in All-Wireless Network



Bridge Network with Wireless Clients

The access point supports root bridge and non-root bridge roles used to interconnect a remote LAN to the main LAN (see [Figure 1-8](#)). The bridge units can also support wireless clients.

Figure 1-8 Root Bridge and Non-Root Bridge with Clients



CISCO CONFIDENTIAL - Draft A1

Workgroup Bridge Network

The access point supports a workgroup bridge role to interconnect remote Ethernet workstations to the main LAN. The workgroup bridge can communicate with an access point (see [Figure 1-9](#)) or with a bridge (see [Figure 1-10](#)).

Figure 1-9 Workgroup Bridge Communicating with an Access Point

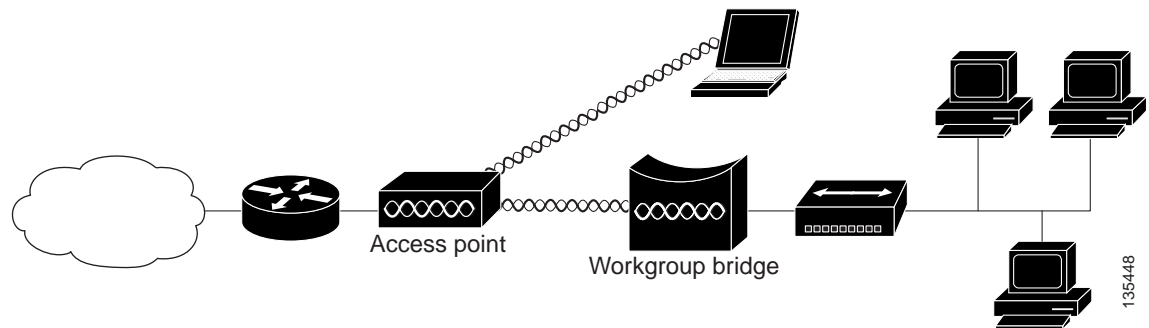
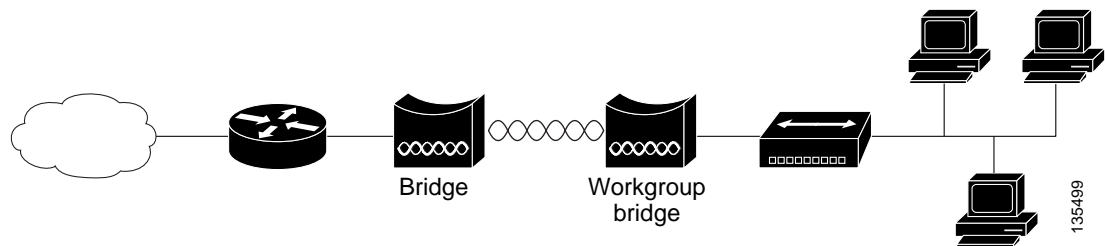


Figure 1-10 Workgroup Bridge Communicating with a Bridge

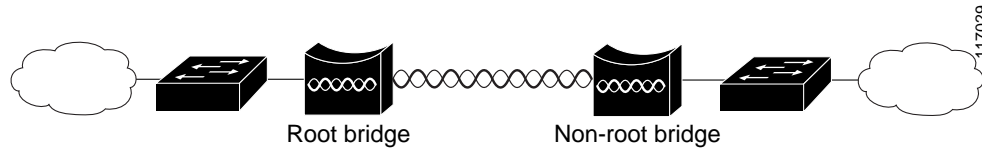


CISCO CONFIDENTIAL - Draft A1

Point-to-Point Bridge Configuration

In a point-to-point bridge configuration, two bridges interconnect two LAN networks using a wireless communication link (see [Figure 1-11](#)). The bridge connected to the main LAN network is classified as a root bridge and the other bridge is classified as a non-root bridge.

Figure 1-11 Point-to-Point Bridge Configuration

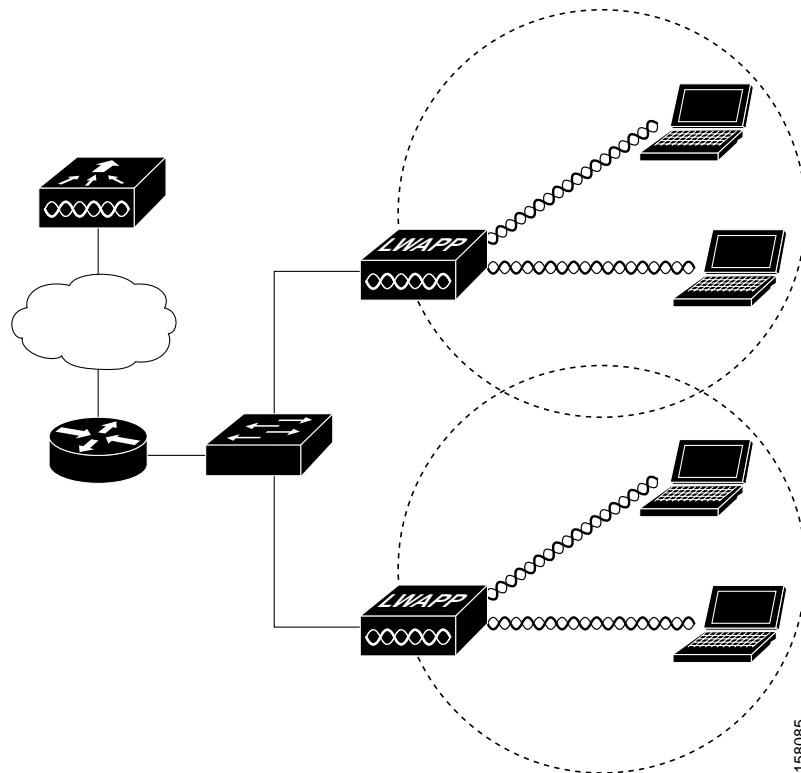


Network Example with Lightweight Access Points

The lightweight access points support Layer 3 network operation. Lightweight 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.

This section illustrates a typical wireless network configuration containing lightweight access points and a Cisco Wireless LAN Controller (see [Figure 1-5](#)). Consult the *Cisco Wireless LAN Controller Configuration Guide* for instructions on setting up the lightweight access points.

Figure 1-12 Typical Lightweight Access Point Network Configuration Example



CISCO CONFIDENTIAL - Draft A1



CISCO CONFIDENTIAL - Draft A1

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 2-4](#)
- [Before Beginning the Installation, page 2-4](#)
- [Installation Summary, page 2-5](#)
- [Mounting Overview, page 2-5](#)
- [Mounting on a Horizontal or Vertical Surface, page 2-7](#)
- [Mounting Below a Suspended Ceiling, page 2-9](#)
- [Mounting Above a Suspended Ceiling, page 2-11](#)
- [Mounting Access Point on a Desktop or Shelf, page 2-14](#)
- [Connecting the Ethernet and Power Cables, page 2-15](#)
- [Powering Up the Access Point, page 2-17](#)
- [Mounting Plate Not Attached to a Surface, page 2-19](#)
- [Mounting Plate Not Attached to a Surface, page 2-19](#)
- [Securing the Access Point, page 2-22](#)

CISCO CONFIDENTIAL - Draft A1

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 the following safety warnings are provided in [Appendix A, “Translated Safety Warnings.”](#)



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

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



Warning

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



Warning

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

Statement 245B



Warning

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

CISCO CONFIDENTIAL - Draft A1**Warning**

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

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

CISCO CONFIDENTIAL - Draft A1

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:

- Install the access point in an area where metal structures such as shelving units, bookcases, filing cabinets, and metal gridwork do not block the radio signals to and from the access point.
- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.

Before Beginning the Installation

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

- [Access Point Bottom Connector Access Openings, page 2-4](#)
- [Installation Summary, page 2-5](#)
- [Mounting Overview, page 2-5](#)

**Caution**

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

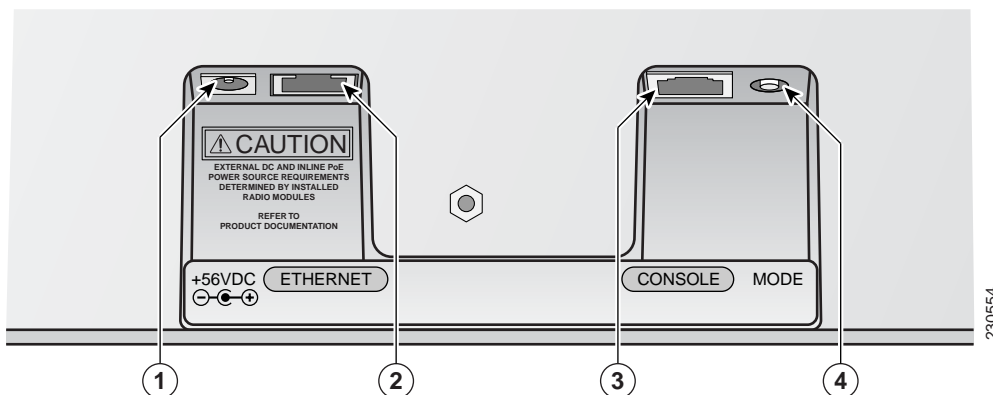
**Caution**

The access point and all interconnected equipment must be located indoors within the same building, including the associated LAN connections.

Access Point Bottom Connector Access Openings

Figure 2-1 illustrates the access point bottom connectors and MODE button.

Figure 2-1 Access Point Bottom Connectors



1	DC power connector (+56 VDC)	3	Console port (RJ-45)
2	Ethernet port (RJ-45)	4	MODE button

CISCO CONFIDENTIAL - Draft A1

Installation Summary

While installing the access point, you will perform these operations:

- Install the mounting plate on a convenient flat horizontal or vertical surface, such as a desktop, book shelf, file cabinet, wall, ceiling, or suspended ceiling T-rail (see the [“Mounting Overview” section on page 2-5](#))
- Connect Ethernet and power cables (see the [“Connecting the Ethernet and Power Cables” section on page 2-15](#)).
- Attach the access point to the mounting plate (see the [“Mounting Plate Attached to a Surface” section on page 2-21](#)).
- Secure the access point (see the [“Securing the Access Point” section on page 2-22](#)).
- Configure security and other access point options (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* or the *Cisco Wireless LAN Controller Configuration Guide*).

Mounting Overview

You can mount the access point on horizontal or vertical surfaces or on suspended ceilings (above or below). For additional information, see these sections:

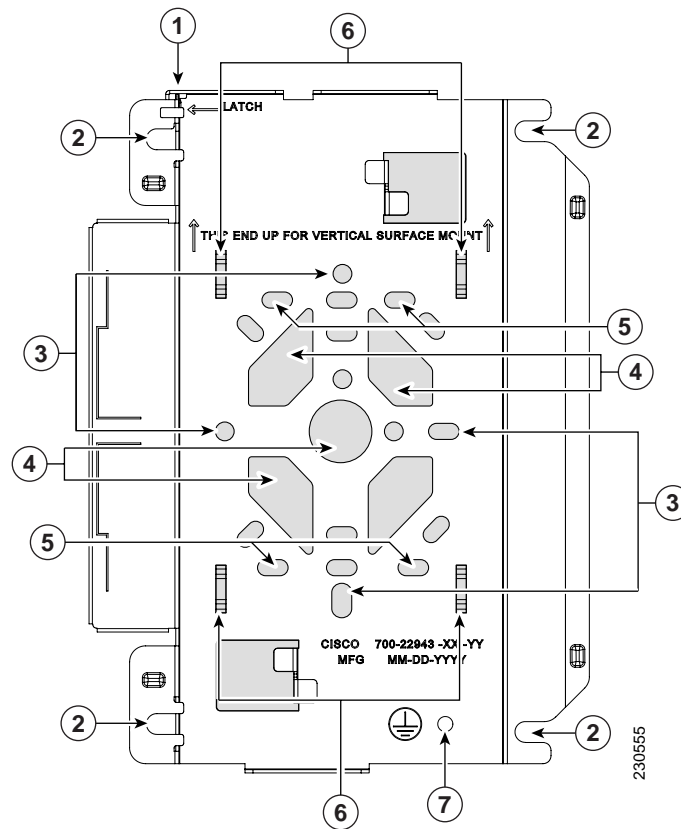
- [Mounting on a Horizontal or Vertical Surface, page 2-7](#)
- [Mounting Below a Suspended Ceiling, page 2-9](#)
- [Mounting Above a Suspended Ceiling, page 2-11](#)
- [Mounting Access Point on a Desktop or Shelf, page 2-14](#)).

The access point ships with an attached mounting plate and the mounting hardware. When you detach the mounting plate, you can use the mounting plate as a template to mark the positions of the mounting holes for your installation. You then install the mounting plate and attach the access point when you are ready.

CISCO CONFIDENTIAL - Draft A1

Figure 2-2 illustrates the various mounting holes on the mounting plate.

Figure 2-2 Mounting Plate



1	Mounting plate latch opening	5	Suspended ceiling mounting holes
2	Access point mounting slots	6	Cable tie points
3	Ceiling or wall mounting holes	7	Grounding stud
4	Cable access openings (also on both ends of the mounting plate)		



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).



Caution

The 1250 series power injector (AIR-PWRINJ4), 1250 series DC power module (AIR-PWR-SPLY1), and the antennas have not been tested to UL 2043 and they must not be placed in a building's environmental air space, such as above suspended ceilings.

CISCO CONFIDENTIAL - Draft A1**Note**

When mounting the access point in a building's environmental air space, you must use cables suitable for operation in environmental air space in accordance with Section 300-22(C) of the National Electrical Code (NEC) and Sections 2-128, 12-010(3), and 12-100 of the Canadian Electrical Code, Part 1, C22.1.

A mounting hardware kit is provided that contains the hardware and fasteners necessary to mount the access point. 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	In Kit
Horizontal or vertical surface	Four #8 x 1 in. (25.4 mm) screws	Yes
	Four wall anchors	Yes
	3/16 in. (4.7 mm) or 3/32 in. (2.3 mm) drill bit	No
	Electric drill and standard screwdriver	No
Suspended ceiling	Two T-rail clips with studs	Yes
	Two plastic spacers	Yes
	Two 1/4–20 Keps nuts with built-in washers	Yes
	Standard screwdriver, wrench, or pliers	No

Mounting on a Horizontal or Vertical Surface

**Caution**

When mounting on a vertical surface, you must position the mounting bracket latch opening on the top (see [Figure 2-2](#)). For a more secure installation, you should attach the mounting plate to a stud or major structural member and use the appropriate fasteners.

Follow these steps to mount the access point on a horizontal or vertical surface.

Step 1 Use the mounting plate as a template to mark the locations of four mounting holes.

**Note**

When mounting in a vertical location, ensure the mounting bracket latch opening is on top (see [Figure 2-2](#)).

- Step 2** Drill one of the following sized holes at the locations you marked:
- 3/16 in. (4.7 mm) if you are using wall anchors.
 - 1/8 in. (6.3 mm) if you are not using wall anchors, you must attach the mounting plate to a stud or major structural member and use appropriate length fasteners.
- Step 3** Install the anchors into the wall if you are using them. Otherwise, go to Step 4.
- Step 4** Secure the mounting plate to the surface using #8 fasteners.
- Step 5** Optionally, you can install a 10 AWG copper ground wire to the mounting plate ground stud (see [Figure 2-2](#)). The other end of the ground wire should be attached to a building ground connection point.
- Step 6** Route your cables through the mounting plate openings or through the ends of the mounting plate.
- Step 7** Optionally, you can secure your cables using the supplied tie-wraps and the mounting plate tie points.

CISCO CONFIDENTIAL - Draft A1

- Step 8** Connect your cables to the access point connectors (see [Figure 2-1](#)) before attaching the access point to the mounting plate (see the “[Connecting the Ethernet and Power Cables](#)” section on [page 2-15](#)).
- Step 9** Prior to attaching the access point to the mounting plate, ensure that the radio modules are completely inserted and both module latches are in the locked position (see [Figure 2-16](#)).
- Step 10** Attach the access point to the mounting plate (see “[Mounting Plate Attached to a Surface](#)” section on [page 2-21](#)).
- Step 11** If you need additional security, refer to the “[Securing the Access Point](#)” section on [page 2-22](#) for additional information.
- Step 12** Verify the access point is operating (see the “[Powering Up the Access Point](#)” section on [page 2-17](#)).
-

CISCO CONFIDENTIAL - Draft A1

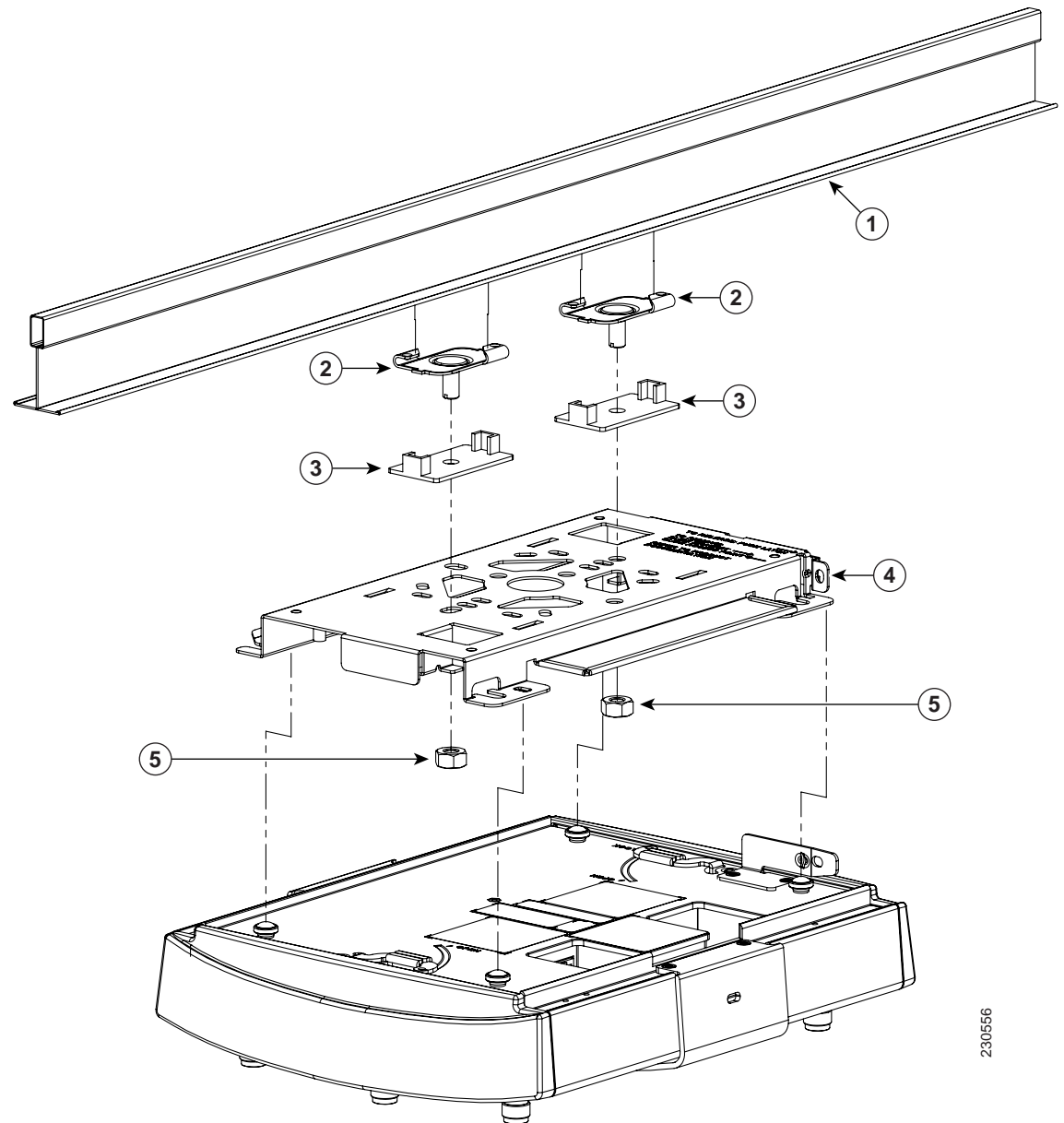
Mounting Below a Suspended Ceiling

**Note**

To comply with NEC code, a #10-24 grounding lug is provided on the mounting plate.

You should review [Figure 2-2](#) and [Figure 2-3](#) before beginning the mounting process.

Figure 2-3 T-Rail Mounting Parts



230556

1	Suspended ceiling T-rail	4	Mounting plate
2	T-rail clips	5	Keps nut (contains an attached lock washer)
3	Plastic spacer (used with recessed ceiling tiles)		

CISCO CONFIDENTIAL - Draft A1

Follow these steps to mount your access point on a suspended ceiling:

-
- Step 1** Decide where you want to mount the access point.
 - Step 2** Attach two T-rail clips to the suspended ceiling T-rail.
 - Step 3** Use the mounting plate to adjust the distance between the T-rail clips so that they align with the holes in the mounting plate.
 - Step 4** Use a standard screwdriver to tighten the T-rail clip studs in place on the suspended ceiling T-rail. Do not overtighten.
 - Step 5** If using recessed ceiling tiles, install a plastic spacer on each T-rail clip stud. The spacer's legs should contact the suspended ceiling T-rail.
 - Step 6** Attach the mounting plate to the T-rail clip studs and start a Keps nut on each stud.
 - Step 7** Use a wrench or pliers to tighten the Keps nuts. Do not overtighten.
 - Step 8** Optionally, you can install a 10 AWG copper ground wire to the mounting plate ground stud (see [Figure 2-2](#)). The other end of the ground wire should be attached to a building ground connection point.
 - Step 9** Route your cables through the mounting plate openings or through the ends of the mounting plate.
 - Step 10** Optionally, you can secure your cables using the supplied tie-wraps and the mounting plate cable tie points.
 - Step 11** Connect your cables to the access point connectors (see [Figure 2-1](#)) before attaching the access point to the mounting plate (see the [“Connecting the Ethernet and Power Cables”](#) section on page 2-15).
 - Step 12** Prior to attaching the access point to the mounting plate, ensure that the radio modules are completely inserted and both module latches are in the locked position (see [Figure 2-16](#)).
 - Step 13** Attach the access point to the mounting plate (see the [“Mounting Plate Attached to a Surface”](#) section on page 2-21).
 - Step 14** If you need additional security, refer to the [“Securing the Access Point”](#) section on page 2-22 for additional information.
 - Step 15** Verify the access point is operating (see the [“Powering Up the Access Point”](#) section on page 2-17).
-

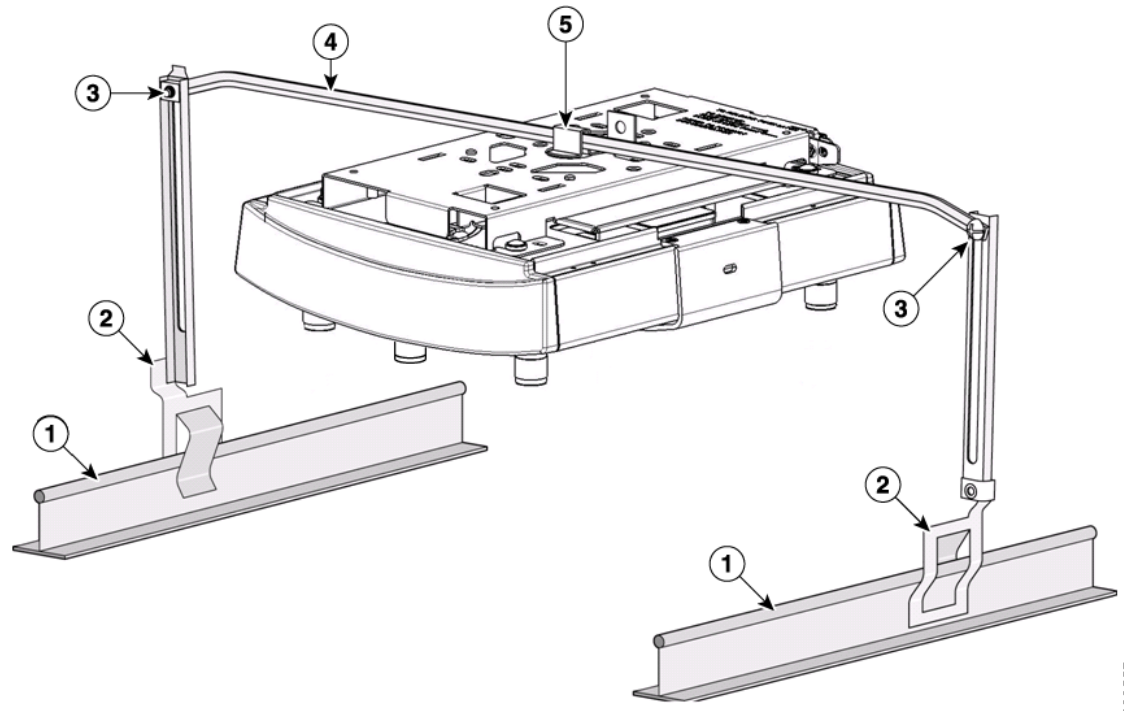
CISCO CONFIDENTIAL - Draft A1

Mounting Above a Suspended Ceiling

The access point mounting plate is designed to be integrated into the T-bar grid above the tiles of a suspended ceiling. Using a T-bar box hanger and bracket mounting clip (not supplied) such as the Erico 512A with BHC mounting clip, you orient the access point antenna just above the top surface of a standard ceiling tile. You may need to modify a thicker tile to allow room for the antenna.

It may be helpful to refer to [Figure 2-4](#) before proceeding.

Figure 2-4 Above Suspended Ceiling Parts



230557

1	Suspended ceiling T-rail	4	T-bar box hanger
2	T-rail clip	5	Bracket mounting clip
3	Height adjustment screw		

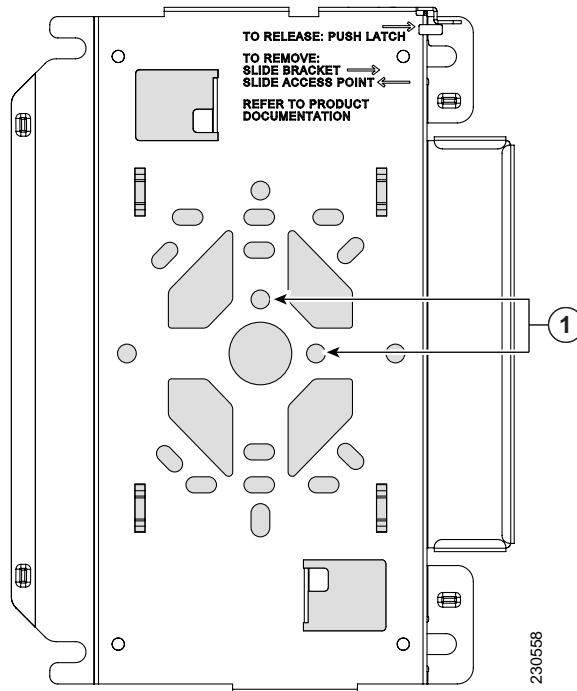
**Caution**

The 1250 series power injector (AIR-PWRINJ4), 1250 series DC power module (AIR-PWR-SPLY1), and the antennas 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.

CISCO CONFIDENTIAL - Draft A1

The bracket mounting clip requires the use of two mounting clip holes on the mounting plate (see [Figure 2-5](#)).

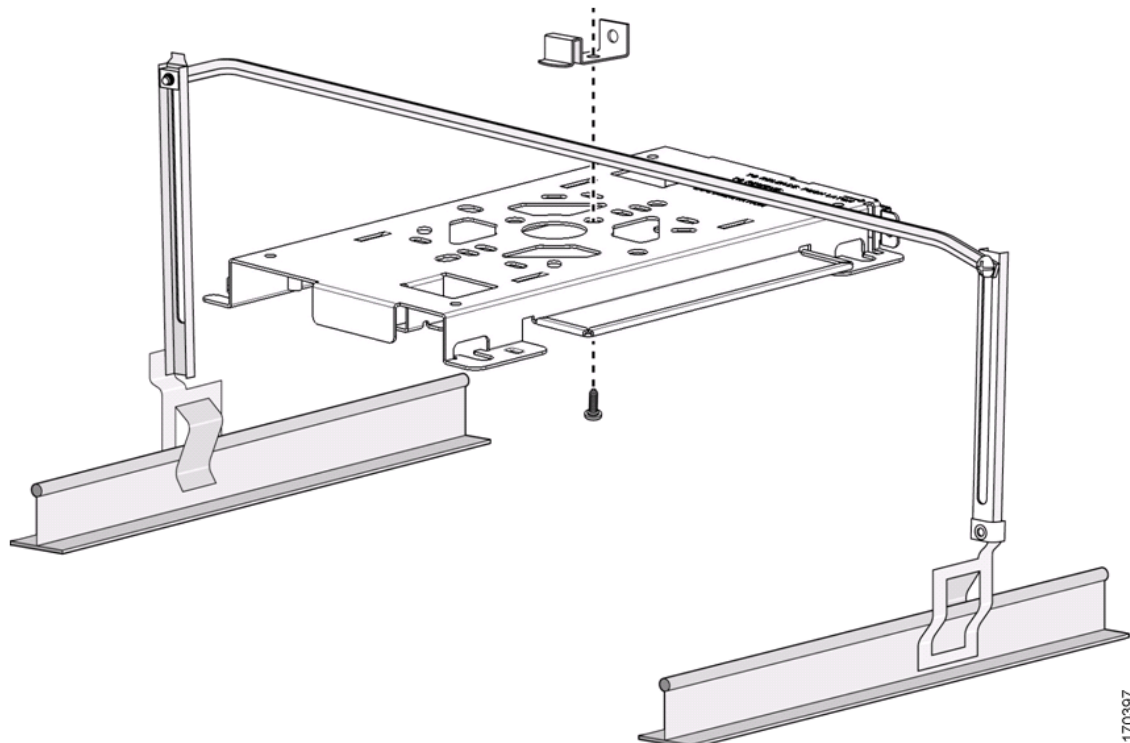
Figure 2-5 Mounting Clip Holes



1	Bracket mounting clip holes
----------	-----------------------------

Follow these steps to mount the access point above a suspended ceiling.

- Step 1** Insert the bracket mounting clip's tab into the large hole on the access point mounting plate.
- Step 2** Place the clip over the T-bar box hanger and secure it to the access point mounting plate (see [Figure 2-6](#)) with the 1/4-20 fastener (supplied with the T-bar hanger).

CISCO CONFIDENTIAL - Draft A1**Figure 2-6 Access Point Mounting Plate****Note**

The illustration shows the access point mounting plate mounted perpendicular to the T-bar box hanger. You can also mount the bracket parallel to the T-bar box hanger.

- Step 3** Determine the location in the ceiling where you will mount the access point and remove an adjacent ceiling tile.
- Step 4** Orient the access point 2-GHz and 5-GHz antennas so that they are pointing down when mounted on the T-bar Box hanger.
- Step 5** Adjust the height of the T-bar box hanger to provide antenna clearance above the ceiling tile using the height adjusting screws (refer to [Figure 2-4](#)).
- Step 6** Attach the T-rail clips on each end of the T-bar box hanger to the ceiling grid T-rails. Make sure the clips are securely attached to the T-rails.
- Step 7** Connect a drop wire to a building structural element and through the hole provided in the bracket mounting clip. This additional support is required in order to comply with the U.S. National Electrical Safety Code.
- Step 8** Optionally, you can install a 10 AWG copper ground wire to the mounting plate ground stud (see [Figure 2-2](#)). The other end of the ground wire should be attached to a building ground connection point.
- Step 9** Route your cables through the mounting plate openings or through the ends of the mounting plate.
- Step 10** Optionally, you can secure your cables using the supplied tie-wraps and the mounting plate cable tie points.
- Step 11** Connect your cables to the access point connectors (see [Figure 2-1](#)) before attaching the access point to the mounting plate (see the [“Connecting the Ethernet and Power Cables”](#) section on page 2-15).

CISCO CONFIDENTIAL - Draft A1

- Step 12** Prior to attaching the access point to the mounting plate, ensure that the radio modules are completely inserted and both module latches are in the locked position (see [Figure 2-16](#)).
- Step 13** Attach the access point to the mounting plate (see the “[Mounting Plate Attached to a Surface](#)” section on [page 2-21](#)).
- Step 14** Connect the antennas or antenna cables to the access point connectors and hand-tighten. Ensure the 2.4-GHz antennas or antenna cables are connected to the access point’s 2.4-GHz antenna connectors (see [Figure 1-1 on page 1-3](#)).



Note The access point 5-GHz antenna connectors have a blue label to correspond with the blue dot or label on the Cisco Aironet 5-GHz antennas or antenna cables.

- Step 15** If you need additional security, see the “[Securing the Access Point](#)” section on [page 2-22](#) for additional information.
- Step 16** Verify the access point is operating before replacing the ceiling tile (see the “[Powering Up the Access Point](#)” section on [page 2-17](#)).

Mounting Access Point on a Desktop or Shelf

When placing the access point on a desktop or shelf, the use of the mounting plate is optional. The access point is shipped with the mounting plate and the mounting plate latch installed. You can use a padlock and a PC type security cable to physically secure the access point (see the “[Securing the Access Point](#)” section on [page 2-22](#)).

If you do not need to secure the access point, you can remove the mounting plate and the mounting plate latch from the bottom of the access point (see the “[Removing the Access Point From the Mounting Plate](#)” section on [page 2-25](#) and “[Installing or Removing the Mounting Plate Latch](#)” section on [page 2-18](#)). The access point has four rubber pads on the bottom to help prevent sliding or scratching the surface of your desktop or shelf when the mounting plate is removed.

For information on connecting the access point cables, see the “[Connecting the Ethernet and Power Cables](#)” section on [page 2-15](#).

When connecting the antennas or antenna cables to the access point antenna connectors, only hand-tighten. Ensure the 2.4-GHz antennas or antenna cables are connected to the access point 2.4-GHz antenna connectors (see [Figure 1-1 on page 1-3](#)).



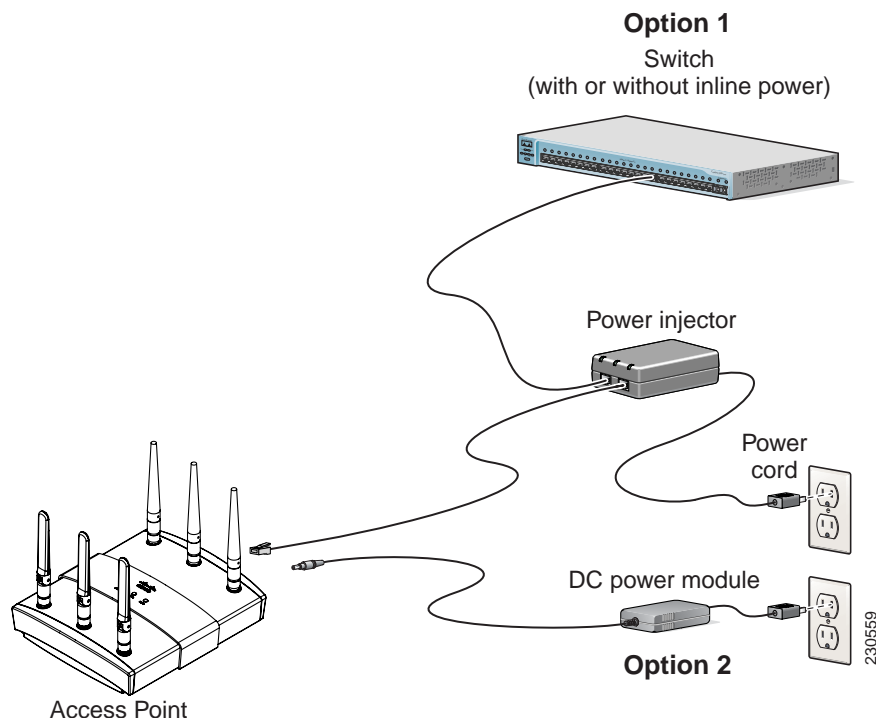
Note The access point 5-GHz antenna connectors have a blue label to correspond with the blue dot or label on the Cisco Aironet 5-GHz antennas or antenna cables.

CISCO CONFIDENTIAL - Draft A1

Connecting the Ethernet and Power Cables

The access point receives power through the Ethernet cable or an external power module. [Figure 2-7](#) shows the power options for the access point.

Figure 2-7 Access Point Power Options



Power options for access points with dual radio modules:

- Option 1—Switches without sufficient inline power can use the power injector:
 - 1250 series power injector (AIR-PWRINJ4)
- Option 2—Local power using the 1250 series DC power module (AIR-PWR-SPLY1)


**Note**

Current switches and patch panels do not provide enough power to operate the access point with dual radio modules. At power-up, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point Status LED turns amber and an error log entry is created (refer to the [“Checking the Autonomous Access Point LEDs”](#) section on page 3-2 and the [“Checking the Autonomous Access Point LEDs”](#) section on page 3-2) or the [“Checking the Lightweight Access Point LEDs”](#) section on page 4-3 and the [“Low Power Condition for Lightweight Access Points”](#) section on page 4-6).


**Note**

Access points with only a single radio module can be powered by IEEE 802.3af power sources, such as switches and power panels.

Connecting to an Ethernet Network with an Inline Power Source


Caution

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

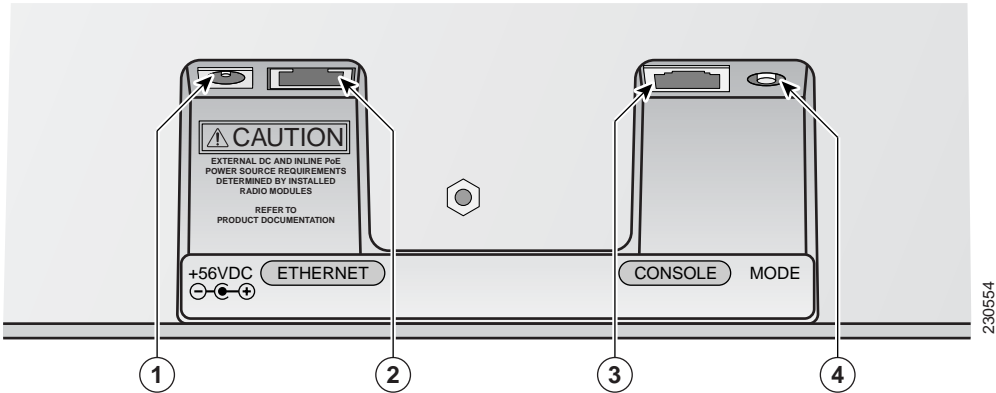

Note

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

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

- Step 1**
- Connect a Category 5E (or higher) Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point (see [Figure 2-8](#)).

Figure 2-8 Ethernet and Power Ports



1	DC power connector (DC-IN)	3	Console port (RJ-45)
2	Ethernet port (RJ-45)	4	MODE button

- Step 2**
- Connect the other end of the Ethernet cable to the Ethernet connector on the 1250 series power injector labeled *To AP*.
- Step 3**
- Connect a Category 5E (or higher) Ethernet cable from your your switch to the power injector connector labeled *To Switch*.
- Step 4**
- Connect an AC power cord to the power injector and the AC wall socket.

CISCO CONFIDENTIAL - Draft A1

Connecting to an Ethernet Network with Local Power

**Note**

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

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

-
- Step 1** Connect a Category 5E (or higher) Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point (see [Figure 2-8](#)).
- Step 2** Connect the 1250 series DC power module's output connector to the access point's DC-IN power connector (see [Figure 2-8](#)).
- Step 3** Plug the other end of the Ethernet cable into an unpowered Ethernet port on your LAN network.
- Step 4** Plug the 1250 series DC power module's AC power cord into an approved 100- to 240-VAC outlet.
- For information on securing your access point, see the [“Securing the Access Point”](#) section on page 2-22.
-

Powering Up the Access Point

When power is applied to the access point, it begins a routine power-up sequence that you can monitor by observing the three LEDs on the top of the access point. After you observe all three LEDs turning green to indicate the starting of the IOS operating system, the Status LED blinks green signifying that Cisco IOS is operational. When in an operational status, the Ethernet LED is steady green and blinking green when passing Ethernet traffic. The sequence takes about 1 minute to complete. Refer to [Chapter 3, “Checking the Autonomous Access Point LEDs,”](#) for LED descriptions.

When the sequence is complete, you are ready to obtain the access point's IP address and perform an initial configuration. Refer to *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on assigning basic settings to the access point.

**Caution**

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

**Note**

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

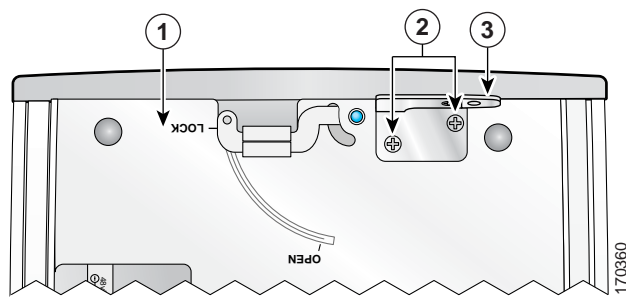


The 1250 series power injectors and 1250 series DC power modules are designed for an open-air environment. To avoid damaging the units, you must not bind together multiple power injectors or power modules.

Installing or Removing the Mounting Plate Latch

The mounting plate latch is located on the bottom of the access point (see [Figure 2-9](#)).

Figure 2-9 Mounting Plate Latch



1	Bottom of access point	3	Mounting plate latch
2	Mounting plate latch screws		

Installing the Mounting Plate Latch

Follow these steps to install the mounting plate latch:

- Step 1

Place the bottom of access point facing up and locate the two screw holes for the mounting plate latch (see [Figure 2-9](#)).
- Step 2

Place the mounting plate latch over the two screw holes.
- Step 3

Screw two 0.125 in (0.318 cm) 4x40 screws into the screw holes.

Removing the Mounting Plate Latch

Follow these steps to remove the mounting plate latch:

- Step 1

Place the bottom of access point facing up and locate the two screw holes for the mounting plate latch (see [Figure 2-9](#)).
- Step 2

Unscrew the two mounting plate screws and remove the mounting plate latch.

CISCO CONFIDENTIAL - Draft A1

Installing the Access Point to the Mounting Plate

There are two methods used to install the access point to the mounting plate:

- Attached to a surface
- Not attached to a surface

When the mounting plate is not attached to a wall or ceiling surface, the access point can be turned over to simplify the installation process.

The mounting plate latch must be on the access point bottom plate to enable the mounting plate to be installed (see the [“Installing the Mounting Plate Latch”](#) section on page 2-18).

**Note**

The access point is shipped with the mounting plate latch and the mounting plate installed.

Mounting Plate Not Attached to a Surface

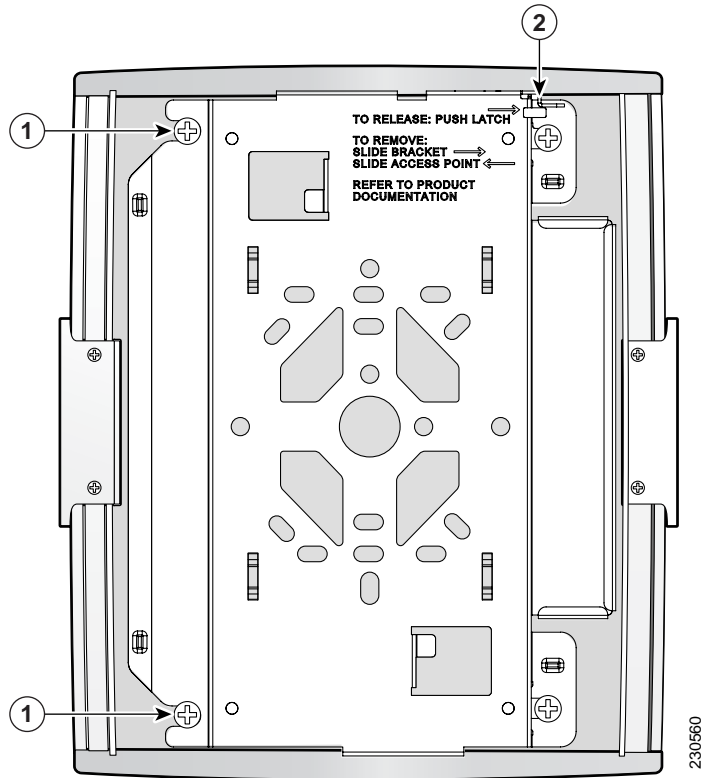
When the mounting plate is not attached to a wall or ceiling surface, follow these steps to attach the mounting plate on the access point:

-
- Step 1** Position your access point with the bottom plate facing you.
- Step 2** Prior to attaching the access point to the mounting plate, ensure that the radio modules are completely inserted and both module latches are in the locked position (see [Figure 2-16](#)).

CISCO CONFIDENTIAL - Draft A1

- Step 3** Line up the four slots on the mounting plate with the rubber feet on the access point. Ensure the mounting plate latch aligns with the mounting plate latch opening (see [Figure 2-10](#)).

Figure 2-10 *Aligning the Mounting Plate Slots with the Rubber Feet on the Access Point*



1	Access point rubber foot and mounting plate slot	2	Mounting plate latch opening
----------	--	----------	------------------------------

- Step 4** Slide the access point until the mounting plate latch clicks.
- Step 5** To secure your radio modules, see the [“Securing the Access Point to the Mounting Plate”](#) section on page 2-22.
- Step 6** To secure your access point with a PC type security cable, see the [“Using a Security Cable to Secure the Access Point”](#) section on page 2-24.

Mounting Plate Attached to a Surface

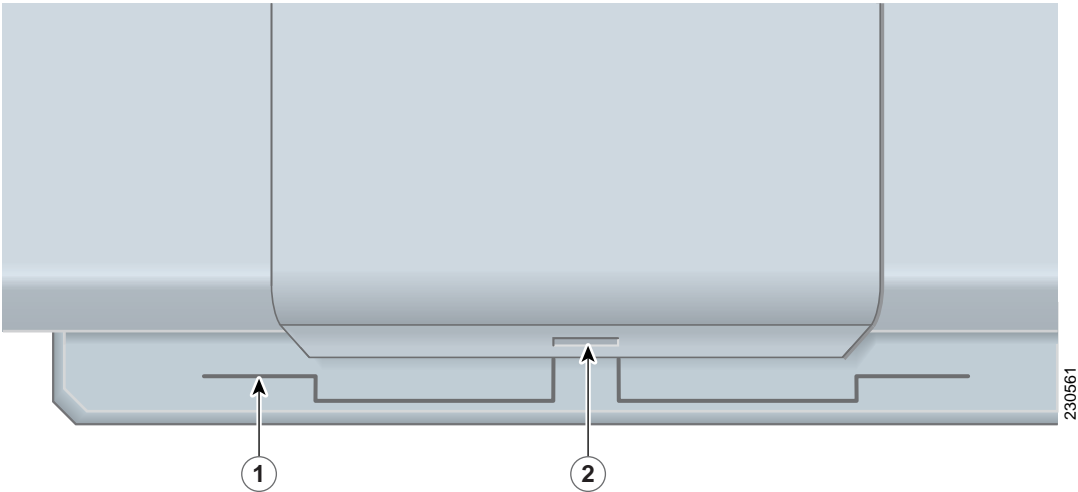


Note Your access point must have the mounting bracket latch attached to the bottom of the unit.

When the mounting plate is attached to a surface, such as a wall or ceiling, follow these steps to install the access point to the mounting plate:

- Step 1** Prior to attaching the access point to the mounting plate, ensure that the radio modules are completely inserted and both module latches are in the locked position (see [Figure 2-16](#)).
- Step 2** Locate the the mounting plate latch opening on your mounting plate (see [Figure 2-2](#)).
- Step 3** Position the end of the access point with the mounting plate latch (see [Figure 2-9](#)) towards the end of the mounting plate with the latch opening.
- Step 4** Place the access point on the mounting plate and align the access point side (with the security cable key slot) with the outline on the mounting plate (see [Figure 2-11](#)).

Figure 2-11 *Align Access Point to Mounting Plate Marking*



1	Outline on mounting plate	2	Security cable key slot side of access point
----------	---------------------------	----------	--

- Step 5** Slowly slide the access point over the outline on the mounting plate until the mounting plate latch clicks.
- Step 6** Visually verify that the four access point feet are securely held by the mounting plate slots.

Securing the Access Point

There are two ways to secure your access point:

- Securing the access point to the mounting plate with a padlock
- Using a security cable

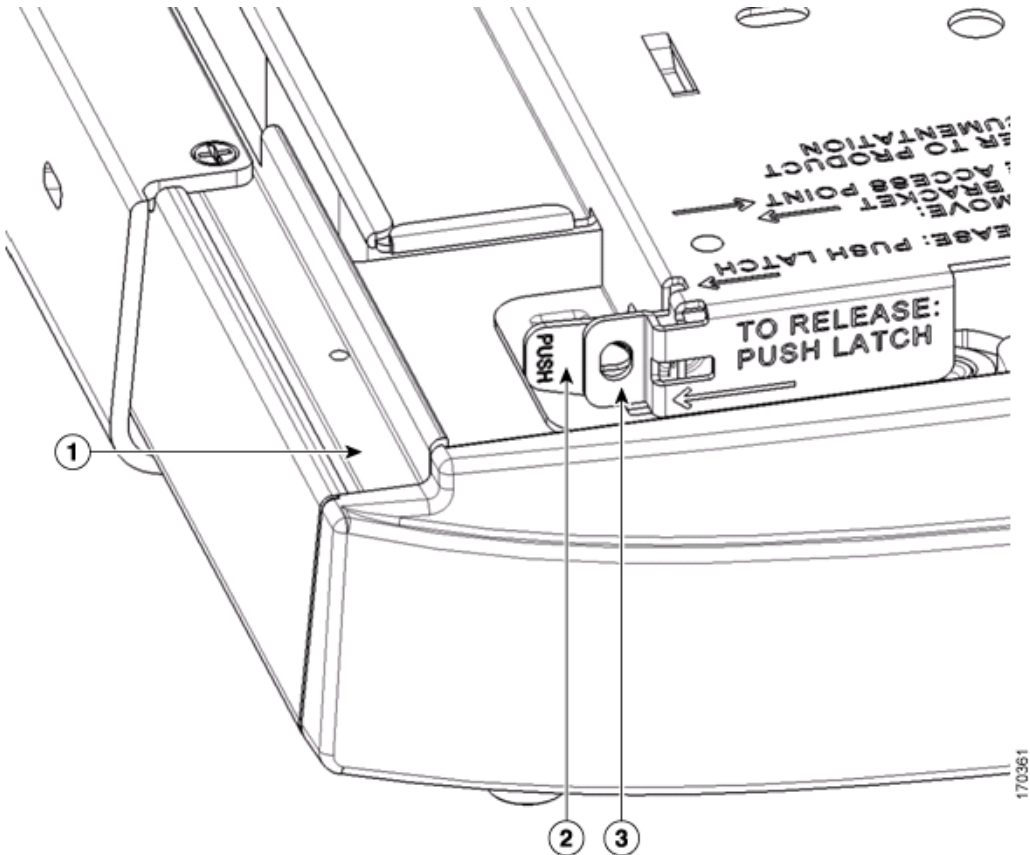
Securing the Access Point to the Mounting Plate

You can secure the access point to the mounting plate to prevent removal of the radio modules. Known compatible padlocks are Master Lock models 120T or 121T. [Figure 2-12](#) shows the padlock hole and the mounting plate latch from the bottom side of the access point for clarity.

 **Note**

The mounting plate latch must be installed on the access point to enable attachment of the mounting plate. The access point is shipped with the mounting plate latch and the mounting plate installed.

Figure 2-12 Security Padlock Hole as Viewed From the Bottom of the Access Point



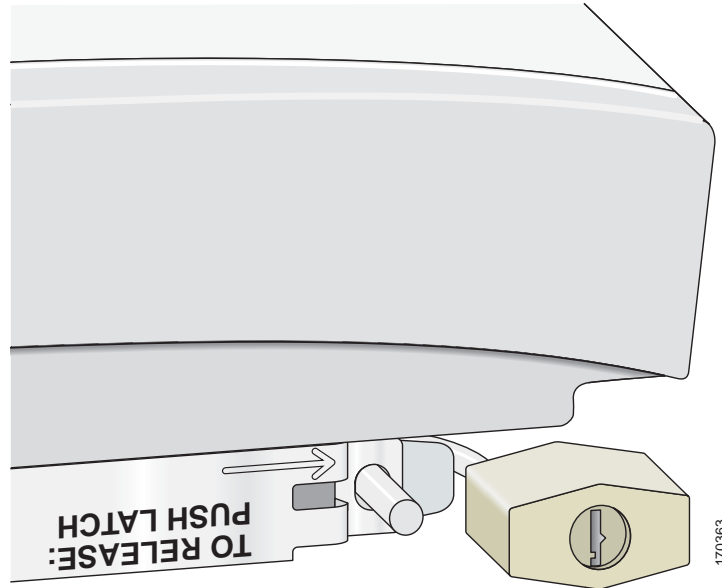
1	Access point	3	Security padlock hole
2	Mounting plate latch		

CISCO CONFIDENTIAL - Draft A1

To secure the access point to the mounting plate using a padlock, follow these steps:

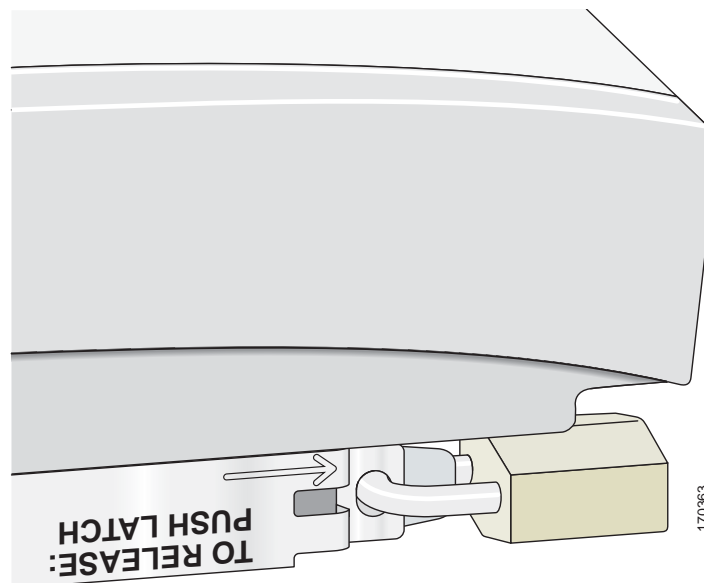
- Step 1** Insert the padlock into the padlock hole on the mounting plate (see [Figure 2-13](#)).

Figure 2-13 *Installing the Padlock*



- Step 2** Rotate the padlock to the lock position and then position the padlock to the side of the access point (see [Figure 2-14](#)).

Figure 2-14 *Position the Padlock for Locking*



- Step 3** Push the padlock against the side of the hole to lock the padlock.

CISCO CONFIDENTIAL - Draft A1

- Step 4** Rotate the padlock under the access point.
-

Using a Security Cable to Secure the Access Point

You can secure the access point by installing a standard security cable (such as the Kensington Notebook MicroSaver, model number 64068) into the access point security cable slot. The security cable can be used with any of the mounting methods described in this guide.

**Note**

To prevent the radio modules from being removed, you must install the mounting plate and a padlock.

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 side of the access point (see [Figure 2-11](#)).
- 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.
-

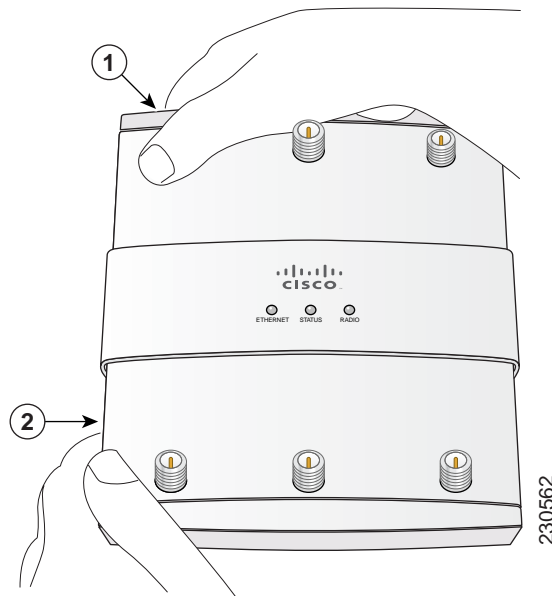
CISCO CONFIDENTIAL - Draft A1

Removing the Access Point From the Mounting Plate

To remove the access point from the mounting plate, follow these instructions:

- Step 1** Verify the location of the mounting plate latch (see [Figure 2-12](#)).
- Step 2** Push the mounting plate latch with your right index finger while gently sliding the access point to the right with your left hand (see [Figure 2-15](#)).

Figure 2-15 Pushing the Mounting Plate Latch



1	Mounting plate latch	2	Direction to slide the access point
----------	----------------------	----------	-------------------------------------

- Step 3** Continue sliding the access point to the right while lifting the edge of the access point with your left hand.
- Step 4** Disconnect the access point cables.

CISCO CONFIDENTIAL - Draft A1

Removing a Radio Module

The access point has two module latches (on the bottom of the access point) for securing or removing modules from the unit.



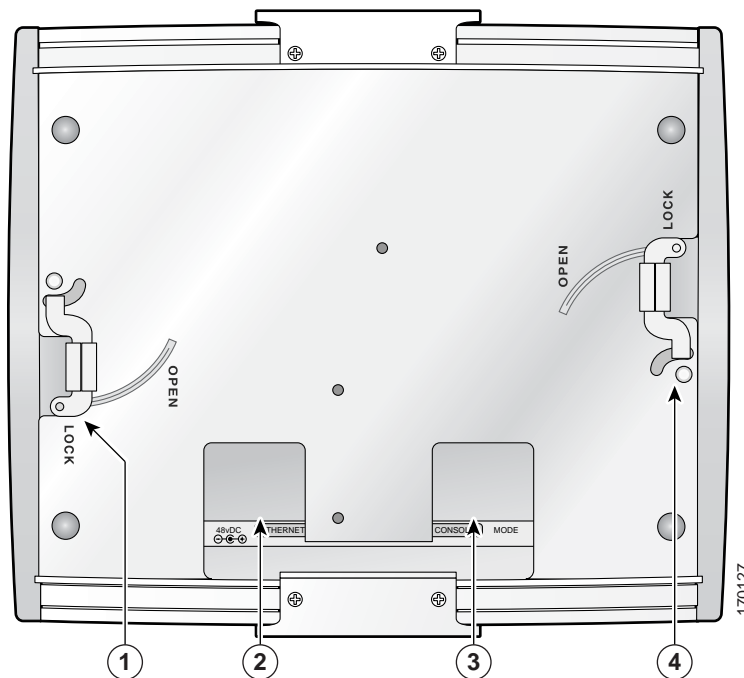
Note

To install or remove a radio module, the access point must be removed from the mounting plate.

To remove a module from the access point, follow these steps:

- Step 1** Place the access point, so that the bottom of the unit is facing up as shown in [Figure 2-16](#).

Figure 2-16 Access Point Module Latches

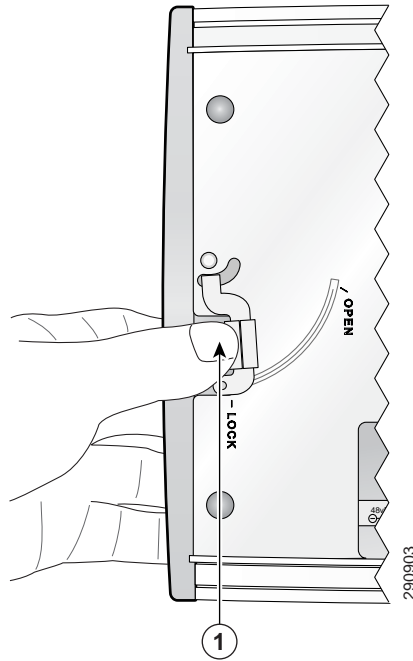


1	Slot 1 module latch	3	Console connector and MODE button
2	DC-IN and Ethernet connectors	4	Slot 1 module latch

CISCO CONFIDENTIAL - Draft A1

Step 2 Use your right or left thumb to push the module lever to the open position (see [Figure 2-17](#)).

Figure 2-17 Opening the Module Latch



1	Push module lever to open
----------	---------------------------

Step 3 When the module lever reaches the open position (see [Figure 2-16](#)), gently pull the radio module from the access point.

Inserting a Radio Module

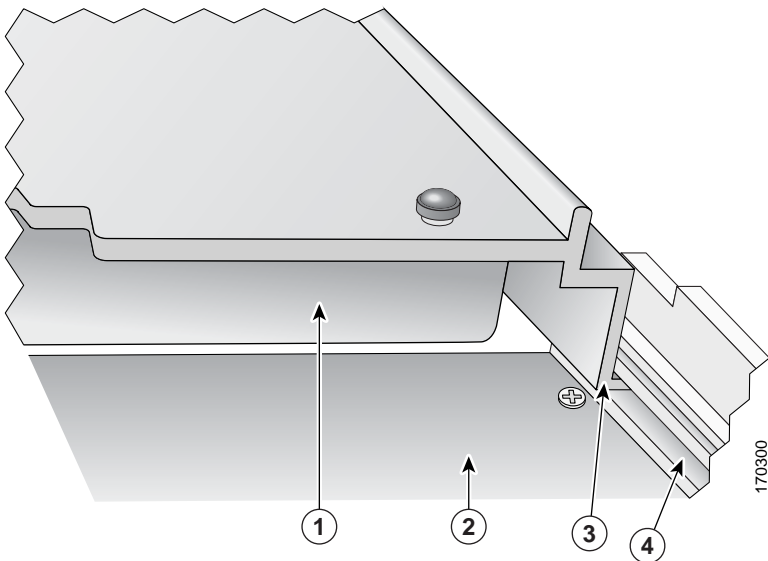

Note

To install or remove a radio module, the access point must be removed from the mounting plate.

Follow these steps to insert a radio module:

- Step 1** Carefully insert the access point module rails into the radio module slots (see [Figure 2-18](#)).

Figure 2-18 Inserting the Radio Module



1	Radio module slot on access point	3	Access point module rail
2	Radio module	4	Radio module slot

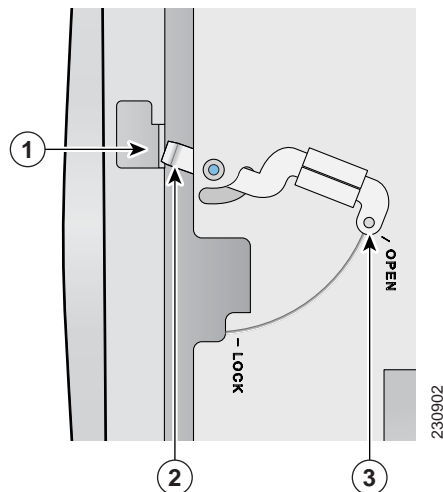
- Step 2** Slowly slide the radio module into the access point until you feel resistance.
- Step 3** Ensure the module latch is in the fully open position (see [Figure 2-19](#)).


Note

If the module latch is not in the open position, the latch will not allow the module to be closed.

CISCO CONFIDENTIAL - Draft A1

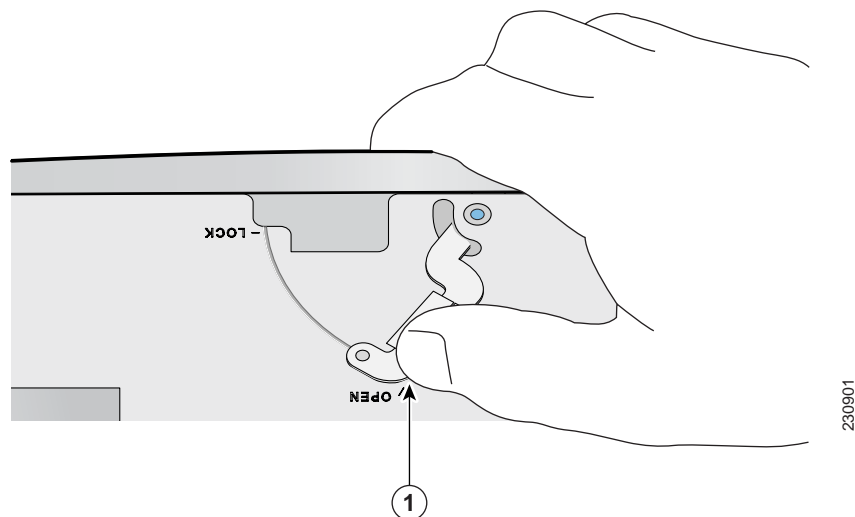
Figure 2-19 Module Latch Position During Module Installation



1	Radio module latch notch	3	Latch open position
2	Module latch		

Step 4 Use your thumb to push the module latch close while you are squeezing with your fingers (see [Figure 2-20](#)). Continue pushing until the module latch clicks.

Figure 2-20 Closing the Module Latch



1	Push module latch
---	-------------------

CISCO CONFIDENTIAL - Draft A1



CISCO CONFIDENTIAL - Draft A1

CHAPTER **3**

Troubleshooting 1250 Series Autonomous Access Points

This chapter provides troubleshooting procedures for basic problems with the 1250 series autonomous access point (model: AIR-AP1252). 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

Sections in this chapter include:

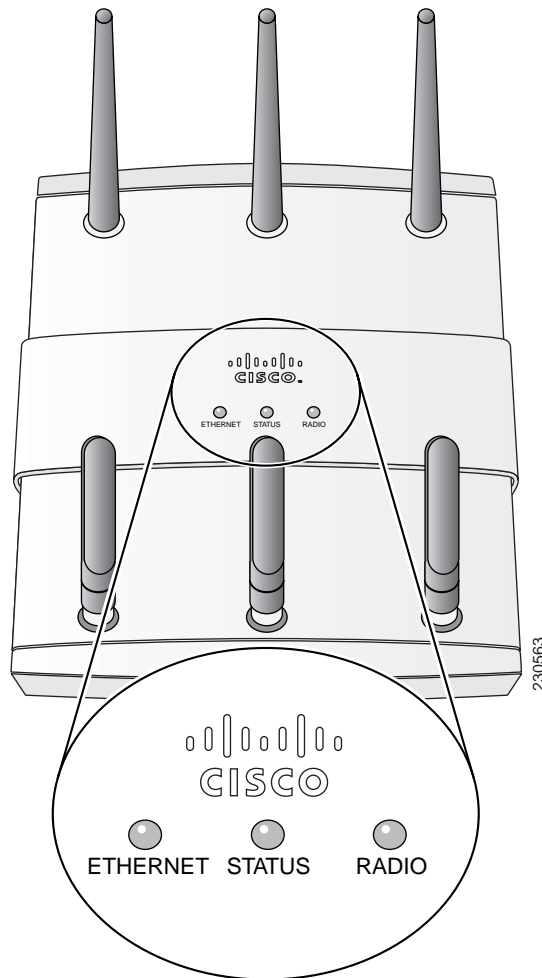
- [Checking the Autonomous Access Point LEDs, page 3-2](#)
- [Checking Basic Settings, page 3-5](#)
- [Low Power Condition on Autonomous Access Points, page 3-7](#)
- [Running the Carrier Busy Test, page 3-16](#)
- [Running the Ping Test, page 3-18](#)
- [Resetting to the Default Configuration, page 3-18](#)
- [Reloading the Access Point Image, page 3-19](#)
- [Obtaining the Access Point Image File, page 3-23](#)
- [Obtaining the TFTP Server Software, page 3-24](#)

CISCO CONFIDENTIAL - Draft A1

Checking the Autonomous Access Point LEDs

If your access point is not working properly, check the Status, Ethernet, and Radio 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



CISCO CONFIDENTIAL - Draft A1

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

Table 3-1 Autonomous Access Point LED Signals

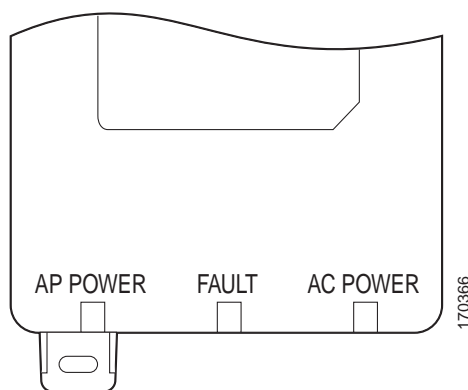
Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	Off	Amber	DRAM test in progress.
	Green	Green	Green	DRAM memory test ok.
	Off	Off	Red	Board initialization in progress.
	Off	Blinking green	Blinking green	Initialize Flash file system.
	Off	Green	Green	Flash memory test ok.
	Amber	White	Off	Initialize Ethernet.
	Green	Blinking blue	Off	Ethernet test ok.
	Green	Blinking green	Green	Starting Cisco IOS.
	Off	Off	Off	Initialization ok.
Association status	—	Green	—	Normal operating condition, but no wireless client devices are associated with the unit.
	—	Blue	—	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	—	—	Ethernet link is operational.
	Blinking green	—	—	Transmitting or receiving Ethernet packets.
	—	—	Blinking green	Transmitting or receiving radio packets.
	—	Blinking blue	—	Software upgrade in progress.
	Blinking green	Blinking green	Blinking green	Access point location command.
Boot loader warnings	Off	Blinking red	Off	Ethernet link not operational.
	Red	Red	Off	Ethernet failure.
	Amber	Blinking blue	Off	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Red	Image recovery (Mode button pressed for 20 to 30 seconds).
	Blinking green	Blinking green	Red	Image recovery in progress and Mode button is released.

CISCO CONFIDENTIAL - Draft A1**Table 3-1** Autonomous Access Point LED Signals (continued)

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Blinking red and blue	Red	Flash file system failure.
	Off	Alternating red and green	Amber	Environment variable (ENVAR) failure.
	Amber	Rapid blinking red	Off	Bad MAC address.
	Red	Blinking red and off	Off	Ethernet failure during image recovery.
	Amber	Blinking red and off	Amber	Boot environment error.
	Red	Blinking red and off	Amber	No Cisco IOS image file.
	Amber	Blinking red and off	Amber	Boot failure.
Cisco IOS errors	Blinking amber	—	—	Transmit or receive Ethernet errors.
	—	—	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Red	Off	Red	Software failure; try disconnecting and reconnecting unit power.
	—	Cycle through blue, green, red, and off	—	General warning, insufficient inline power (see the “Low Power Condition on Autonomous Access Points” section).

Checking the Power Injector LEDs

The power injector (model:AIR-PWRINJ4) has three LEDs on the top end of the case (see [Figure 3-2](#)).

Figure 3-2 Power Injector LEDs

CISCO CONFIDENTIAL - Draft A1

Table 3-2 lists the power injector LED indications.

Table 3-2 Power Injector LED Indications

LED	Color	Description
AP Power	Green	Indicates DC power is available to the access point.
Fault	Red	Indicates a short or overload condition. Check Ethernet cables and connections before contacting your support organization for assistance.
AC Power	Green	Indicates AC power is available at the power injector.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following areas.

Default IP Address Behavior

When you connect a 1250 series access point running Cisco IOS Release 12.4(1)JA or later software with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an IP address, continues to send requests indefinitely.

Enabling the Radio Interfaces

In Cisco IOS Release 12.4(1)JA or later, the access point radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radios before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on configuring the SSID.

To enable the radio interfaces, follow these instructions:

-
- Step 1** Use your web-browser to access your access point.
- Step 2** When the Summary Status page displays, click **Network Interfaces > Radio0-802.11N^{2.4GHZ} or Radio0-802.11N^{5GHZ}** and the radio status page displays



Note The module slot (slot 0 or slot 1) where the radio module is located defines the Radio0 or Radio1 designation. See [Figure 1-1 on page 1-3](#) for the location of the module slots.

- Step 3** Click **Settings** and the radio settings page displays.
- Step 4** Click **Enable** in the Enable Radio field.
- Step 5** Click **Apply**.
- Step 6** Click **Radio1-802.11N^{2.5GHZ} or Radio1-802.11N^{5GHZ}** and the radio status page displays.
- Step 7** Repeat Steps 3 to 5.

CISCO CONFIDENTIAL - Draft A1

Step 8 Close your web-browser.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device's SSID does not match the SSID of an access point in radio range, the client device will not associate.

**Note**

In Cisco IOS Release 12.4(1)JA and later, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must also set WEP Key 3 on the access point to exactly the same value. The access point does not need to use Key 3 as its transmit key, however.

Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting the access point's WEP keys.

Security Settings

Wireless clients attempting to authenticate with your access point must support the same security options configured in the access point, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a wireless client is unable to authenticate with your access point, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the access point settings.

**Note**

The access point MAC address that displays on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

CISCO CONFIDENTIAL - Draft A1

Low Power Condition on Autonomous Access Points

The access point can be powered from the 1250 DC power module or from the 1250 in-line power injector. The access point supports the Cisco Intelligent Power Management.

With only one radio module installed, the access point (powered device) requires 12.95 W (up to 15 W with 100 m of CAT 5E (or higher) Ethernet cable). When the access point is being used in a PoE configuration, the power drawn from the power sourcing equipment (PSE), such as a power injector, is higher by an amount dependent on the length of the interconnecting cable.

For full dual radio module operation, the access point requires 18.4 W (up to 21 W with 100 m CAT 5E (or higher) Ethernet cable).

**Caution**

Current switches, power patch pannels, and IEEE 802.3af compliant power sources are not able to provide sufficient power to the access point with both radio modules installed.

**Note**

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

On power up, the access point is placed into low power mode (both radios are disabled), Cisco IOS software loads and runs, and power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on; otherwise, the access point remains in low power mode with the radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication, displays a low power message on the browser and serial interfaces, and creates an event log entry (see the [“Checking the Autonomous Access Point LEDs”](#) section on page 3-2 and [“Inline Power Status Messages”](#) section on page 3-8).

Intelligent Power Management - need changes

The access point requires 18.4 W of power for dual radio operation or 12.95 W of power with a single radio module installed (needs ----TBD W of power when operating in low power mode with both radios disabled). To help avoid an over-current condition with low power sources and to optimize power usage on Cisco switches, Cisco developed Intelligent Power Management, which uses Cisco Discovery Protocol (CDP) to allow powered devices (such as your access point) to negotiate with a Cisco switch for sufficient power.

The access point supports Intelligent Power Management and as a result of the power negotiations, the access point will either enter full power mode or remain in low power mode with the radios disabled.

**Note**

Independent of the power negotiations, the access point hardware also uses the 802.3af classification scheme to indicate the power required from the power source. However, the power source cannot report the power available to the access point unless the power source also supports Intelligent Power Management.

CISCO CONFIDENTIAL - Draft A1

Some Cisco switches that are capable of supplying sufficient power to operate a single radio module require a software upgrade to support Intelligent Power Management. If the software upgrade is not desired, you can configure the access point to operate in pre-standard compatibility mode and the access point automatically enters full power mode (with a single radio module installed) if these Cisco switches are detected in the received CDP ID field.

When the access point determines that sufficient power is not available for full power operation, an error message is logged and the Status LED turns amber to indicate low power mode (see the “Checking the Autonomous Access Point LEDs” section on page 3-2 and the “Inline Power Status Messages” section on page 3-8).

**Tip**

If your switch is capable of supplying sufficient power for full operation (with a single radio module installed) but the access point remains in low-power mode, your access point or your switch (or both) might be misconfigured (see Table 3-3 and Table 3-5).

For full power operation with both radio modules installed, the access point can only be powered by these options :

- 1250 series power injector (AIR-PWRINJ4) on the switch port
- 1250 series DC power module (AIR-PWR-SPLY1) to locally power the access point

Inline Power Status Messages

These messages are logged on the console port by the access point to report the power condition:

- %CDP_PD-4-POWER_OK: Full Power - AC_ADAPTOR inline power source—This message indicates the access point is using the power module and can support full-power operation.
- %CDP_PD-4-POWER_OK: Full Power - NEGOTIATED inline power source—This message indicates the access point is operating at full power and has successfully negotiated for 12.95 W of power from a Cisco switch supporting Cisco Intelligent Power Management.
- %CDP_PD-4-POWER_OK: Full Power - HIGH_POWER_CLASSIC inline power source—This message indicates the access point is operating at full power because it has been configured for pre-standard compatibility mode and has detected a Cisco switch that does not support Intelligent Power Management but is able to supply sufficient power to the access point.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_CONFIGURED_ON_SOURCE inline power source—This message indicates the access point is operating at full power because it is connected to a Cisco switch that supports Intelligent Power Management and the switch has been configured with the *power inline never* command.
- %CDP_PD-4-POWER_OK: Full power - INJECTOR_CONFIGURED_ON_CURRENT_PORT inline power source—This message indicates the access point is operating at full power because it has been configured to expect a power injector on this port.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_PD inline power source—This message indicates the access point is operating at full power because it has detected a CDP packet from another Cisco powerable device (PD). The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not transmit this type of CDP packet.

CISCO CONFIDENTIAL - Draft A1

- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_MULTIPLE_MACS_ON_HUB inline power source—This message indicates the access point is operating at full power because it has detected multiple Cisco devices. The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not forward CDP packets.
- %CDP_PD-4-POWER_OK: Full Power - NON_CISCO-NO_CDP_RECEIVED inline power source—This message indicates the access point is operating at full power because it has not received any CDP packets within the timeout period. This condition indicates your access point is connected to a non-Cisco power source.
- %CDP_PD-4-POWER_OK: Full power - INJECTOR_DETECTED inline power source—This message indicates that the access point has detected the 1250 series power injector (AIR-PWINJ4) and is operating at full power with both radios enabled. The **power inline negotiation injector installed** command does not have to be used to specify that the power injector is installed.



Note To prevent possible over-current conditions, the power source must be an IEC60950 compliant limited power source.

- %CDP_PD-4-POWER_OK: Full power - INJECTOR_CONFIGURED_OVERRIDE_SAFETY inline power source —This message indicates the access point has been configured to override the inline power checks and a power injector is installed.

**Caution**

When using the *power inline negotiation injector override* command, a power injector must always be installed to prevent a possible overload condition with an underpowered power source.

- %CDP_PD-2-POWER_LOW: All radios disabled - NEGOTIATED inline power source—This message indicates the access point is in low power mode with all radios disabled because the Cisco power source has indicated it is not capable of supplying sufficient power to the access point.



Note A Cisco 1250 power injector might be required.

- %CDP_PD-2-POWER_LOW: All radios disabled - LOW_POWER_CLASSIC_NO_INJECTOR_CONFIGURED <platform name> (<MAC address>). —This message indicates the access point is in low power mode with all radios disabled and has detected a CDP device that is unable to supply sufficient power to the access point.

The <platform name> indicates the CDP device detected by the access point. The <MAC address> indicates the MAC address of the CDP device, typically, the switch port.



Note A Cisco power injector might be required.

Following the low power status message, two extra messages are displayed on the console port or when using a Telnet session that identify the actions needed to resolve this low power problem:

- Verify the required power injector is installed on this port: <platform name> (<Ethernet port>).
(where <platform name> indicates the CDP device detected by the access point and <Ethernet port> indicates the Ethernet port of the CDP device.
- If a power injector is installed, issue the command: *power inline negotiation injector installed*.

CISCO CONFIDENTIAL - Draft A1

- %CDP_PD-2-POWER_LOW: All radios disabled- LOW_POWER_CLASSIC_INJECTOR_CONFIGURED_ON_ANOTHER_PORT *<platform name>* (*<MAC address>*)—This message indicates the access point is in low power mode with all radios disabled and has detected a CDP device that is unable to supply sufficient power to the access point. A power injector has been configured, but it is for another port. It is likely that the access point has been relocated and has not been reconfigured for a new power injector.

The *<platform name>* indicates the CDP device detected by the access point. The *<MAC address>* indicates the MAC address of the CDP device, typically, the switch port.



Note A Cisco 1250 power injector might be required.

Following the low power status message, two extra messages are displayed when using the console port or a Telnet session that identify the actions needed to resolve this low power problem:

1. Verify the required power injector is installed on the new port: *<platform name>* (*<Ethernet port>*).
- (where *<platform name>* indicates the CDP device detected by the access point and *<Ethernet port>* indicates the Ethernet port of the CDP device.)
2. If a power injector is installed, issue the command: power inline negotiation injector installed.
- %CDP_PD-2-POWER_LOW: All radios disabled- HIGH_POWER_CLASSIC_NOT_CONFIGURED inline power source *<platform name>* (*<MAC address>*)—This message indicates the access point is in low power mode with all radios disabled and has detected a Cisco switch that does not support Intelligent Power Management, but should be able to supply sufficient power. The access point must be configured for pre-standard compatibility.

The *<platform name>* indicates the Cisco platform detected by the access point. The *<MAC address>* indicates the MAC address of the switch port.



Note You need to upgrade the software on the Cisco switch to support Intelligent Power Management or configure the access point for pre-standard compatibility.

- %CDP_PD-2-POWER_LOW: All radios disabled-INJECTOR_CONFIGURED_BUT_FAILS_VERIFICATION *<platform name>* (*<MAC address>*)—This message indicates the access point is in low power mode with all radios disabled and a power injector has been configured but has not been detected by the access point.

The *<platform name>* indicates the Cisco platform detected by the access point. The *<MAC address>* indicates the MAC address of the switch port.

CISCO CONFIDENTIAL - Draft A1

Configuring Power Using the CLI

Intelligent Power Management support is dependent on the version of software resident in the Cisco switch that is providing power to the access point. Each Cisco switch should be upgraded to support Intelligent Power Management. Until the software is upgraded, you can configure the access point to operate with older switch software using the following Cisco IOS CLI command:

```
[no] power inline negotiation {prestandard source |injector {installed | override | H.H.H} }
```

Where:

- **prestandard source** indicates the Cisco switch does not support Intelligent Power Management.
- **injector installed** indicates a power injector is installed on the current switch port.
- **injector override** indicates a power injector is installed and the access point is configured to override the inline power checks. When you move the access point, *H.H.H* is used to specify the MAC address of the new switch port where the access point was moved. A MAC address of 0.0.0 is invalid.)

**Caution**

When you are using the **power inline negotiation injector override** command, a power injector must always be installed to prevent a possible overload condition with an underpowered power source.

**Note**

The **power inline negotiation injector installed** command will fail if CDP is disabled.

When using the power inline negotiation injector override command, you must use a power injector to prevent possibly overloading underpowered power sources.

You can use this Cisco IOS CLI command to inform the access point of the following:

- The Cisco switch does not support Intelligent Power Management but should be able to supply sufficient power.
- A 1250 power injector is being used to supply sufficient power and the Cisco switch does not support Intelligent Power Management.
- The access point was moved to a new Cisco switch port and a 1250 power injector is being used to supply sufficient power.

**Caution**

If the access point receives power through PoE, the output current of the power sourcing equipment (PSE) cannot exceed 400 mA per port. The power source must comply with IEEE802.3af.

**Note**

After completing your configuration changes, you must remove the serial console cable from the access point.

CISCO CONFIDENTIAL - Draft A1**Table 3-3 Using Cisco IOS Commands For Access Points with One Radio Module Installed**

Power Source	Cisco IOS Commands	
	Access Point	Cisco Switch
AC power module	None required	power inline never
Cisco switch that supports Intelligent Power Management ¹	no power inline negotiation prestandard source no power inline negotiation injector	power inline auto
Cisco switch that does not support Intelligent Power Management ¹	power inline negotiation prestandard source no power inline negotiation injector	power inline auto
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	None required ³	power inline never⁴
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	None required ⁵	power inline never
Power injector used with a non-Cisco switch	None required	—

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.
2. Power injector must be AIR-PWRINJ4.
3. The Cisco switch uses Intelligent Power Management to inform the access point of the power injector being used.
4. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.
5. The access point detects the power injector (AIR-PWRINJ4).

Table 3-4 Using Cisco IOS Commands For Access Points with Two Radio Modules Installed

Power Source	Cisco IOS Commands	
	Access Point	Cisco Switch
AC power module	None required	power inline never
Cisco switch that supports Intelligent Power Management ¹	no power inline negotiation prestandard source power inline negotiation injector	power inline never
Cisco switch that does not support Intelligent Power Management ¹	power inline negotiation prestandard source power inline negotiation injector	power inline never
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	None required ³	power inline never⁴
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	None required ⁵	power inline never
Power injector ² used with a non-Cisco switch	None required ⁵	—

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.
2. Power injector must be AIR-PWRINJ4.
3. The Cisco switch uses Intelligent Power Management to inform the access point of the power injector being used.
4. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.
5. The access point detects the power injector (AIR-PWRINJ4).

CISCO CONFIDENTIAL - Draft A1**Issuing the Cisco IOS Command Using the CLI**

Follow these steps to issue the Cisco IOS command for your power scenario:

-
- Step 1** Connect a PC to the access point console port and use a terminal emulator to establish a session with the access point (refer to the [“Connecting to the Access Point Locally”](#) section on page 3-23).
- Step 2** From the global configuration mode (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*), enter the command below that applies to your power configuration (see [Table 3-3](#) and [Table 3-4](#)):
- **power inline negotiation injector installed**
 - **no power inline negotiation injector**
 - **power inline negotiation prestandard source**
 - **no power inline negotiation prestandard source**
- Step 3** Enter the **write memory** command to save the setting to the access point memory.
- Step 4** Enter the **quit** command to exit the terminal session.
-

Configuring the Access Point System Power Settings Using a Browser - TBD

You can also use your browser to set the access point system power settings.


Note

The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.


Note

When using the access point browser interface, you should disable your browser pop-up blocker.

Figure 3-3 shows the system power setting options and indicates the access point power status (1250 series power injector detected).

Figure 3-3 System Power Settings

System Power Settings	
Power State:	FULL POWER
Power Source:	INJECTOR_DETECTED
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)

Table 3-5 and Table 3-6 lists the access point system power settings and the Cisco switch power commands for several power options.

Table 3-5 System Power Settings and Cisco Switch Commands for Access Points with a Single Radio Module ??

Power Source	Access Point System Power Settings	Cisco Switch Power Command
AC power module	Configuration changes are not required	power inline never
Cisco switch that supports Intelligent Power Management ¹	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (unchecked)	power inline auto
Cisco switch that does not support Intelligent Power Management ¹	Power Settings: Pre-standard Compatibility (selected) Power Injector: Installed on Port with MAC Address (unchecked)	power inline auto
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (unchecked)	power inline never

CISCO CONFIDENTIAL - Draft A1**Table 3-5 System Power Settings and Cisco Switch Commands for Access Points with a Single Radio Module**

Power Source	Access Point System Power Settings	Cisco Switch Power Command
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (checked)	power inline never
Power injector used with a non-Cisco switch	Configuration changes are not required	—

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.
2. Power injector must be AIR-PWRINJ4.

Table 3-6 System Power Settings and Cisco Switch Commands for Access Points with Dual Radio Modules ??

Power Source	Access Point System Power Settings	Cisco Switch Power Command
AC power module	Configuration changes are not required	power inline never
Power injector ¹ used with a Cisco switch that supports Intelligent Power Management ²	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (checked)	power inline never
Power injector used with a Cisco switch that does not support Intelligent Power Management ²	Power Settings: Pre-standard Compatibility (selected) Power Injector: Installed on Port with MAC Address (checked)	power inline never
Power injector used with a non-Cisco switch	Configuration changes are not required	—

1. Power injector must be AIR-PWRINJ4.
2. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.

Follow these steps to configure your access point power settings using the browser interface:

-
- Step 1** Obtain the access point IP address and browse to your access point.
- Step 2** Perform one of these operations:
- a. When you browse to your access point operating in low-power mode, a Warning message displays indicating that all radios are disabled due to insufficient power. Click **OK** to jump to the System Power Settings located on the System Software > System Configuration page.
 - b. When you browse to your access point operating in full-power mode, choose **System Software > System Configuration**.

CISCO CONFIDENTIAL - Draft A1

- Step 3** Choose one of these Power Settings options (see [Figure 3-3](#)):
- If your Cisco switch supports Intelligent Power Management negotiations, choose **Power Negotiation**.
 - If your Cisco switch does not support Intelligent Power Management negotiations, choose **Pre-standard Compatibility**.
 - If you are using a non-Cisco switch, changes to the power settings are not required.
- Step 4** If you are using a power injector with a Cisco switch, choose one of these Power setting options (see [Figure 3-3](#)):
- If your Cisco switch supports Intelligent Power Management negotiations, uncheck **Installed on Port with MAC address**.
 - If your Cisco switch does not support Intelligent Power Management, check **Installed on Port with MAC address** and ensure the MAC address for your switch port is displayed in the MAC address field. The HHHH.HHHH.HHHH indicates the MAC address contains 12 hexadecimal digits.



Note The MAC address field is not case-sensitive.

- Step 5** Click **Apply** and a message displays indicating that you should disable pop-up blockers before proceeding.
- Step 6** Click **OK** to continue. Your access point reboots and your power settings are configured in the access point.



Note You might have to refresh your browser page to obtain the latest browser page that indicates your radios are enabled.

Running the Carrier Busy Test

You can use the carrier busy test to determine the least congested channel for a radio interface (2.4-GHz or 5-GHz radio module). You should typically run the test several times over several days to obtain the best results and to avoid temporary activity spikes.



Note The carrier busy test is primarily used for single access points or bridge environments. For sites with multiple access points, a site survey is typically performed to determine the best operation location and operating frequency for the access points.



Note All associated clients on the selected radio will be deassociated during the 6 to 8 seconds needed for the carrier busy test.

Follow these steps to activate the carrier busy test:

- Step 1** Use your web browser to access the access point browser interface.

CISCO CONFIDENTIAL - Draft A1

- Step 2** When the Summary Status page displays, click **Network Interfaces > Radio0-802.11N^{2.4GHZ}** or **Radio0-802.11N^{5GHZ}** and the radio status page displays



Note The module slot (slot 0 or slot 1) where the radio module is located defines the Radio0 or Radio1 designation. See [Figure 1-1 on page 1-3](#) for the location of the module slots.

- Step 3** Click the **Carrier Busy Test** tab and the Carrier Busy Test page displays

- Step 4** Click **Start** to begin the carrier busy test.

When the test completes, the results are displayed on the page. For each of the channel center frequencies, the test produces a value indicating the percentage of time that the channel is busy.

- Step 5** To perform a link test on the second radio module, repeat steps 2 through 4 for the Radio1-802.11N^{2.4GHZ} or Radio1-802.11N^{5GHZ} radio interfaces.

When the test completes, the results are displayed on the page. For each of the channel center frequencies, the test produces a value indicating the percentage of time that the channel is busy.

- Step 6** Close your browser.

CISCO CONFIDENTIAL - Draft A1

Running the Ping Test

You can use the ping test to evaluate the link to and from an associated wireless device. The ping test provides two modes of operation:

- a. Performs a test using a specified number of packets and then displays the test results.
- b. Performs a test that continuously operates until you stop the test and then displays the test results.

Follow these steps to activate the ping test:

-
- Step 1** Use your web browser to access the access point browser interface.
 - Step 2** Click **Association** and the main association page displays.
 - Step 3** Click the MAC address of an associated wireless device and the Statistics page for that device displays.
 - Step 4** Click the **Ping/Link Test** tab and the Ping/Link Test page displays.
 - Step 5** If you want to specify the number of packets to use in the test, follow these steps:
 - a. Enter the number of packets in the Number of Packets field
 - b. Enter the packet size in the Packet Size field.
 - c. Click **Start**.
 - Step 6** If you want to use a continuous test, follow these steps:
 - a. Enter the packet size in the Packet Size field.
 - b. Click **Start** to activate the test.
 - c. Click **Stop** to stop the test.

When the test has completed, the test results are displayed at the bottom of the page. You should check for any lost packets that can indicate a problem with the wireless link. For best results, you should also perform this test several times.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you may need to completely reset the configuration. You can use the MODE button on the access point or the web-browser interface.

**Note**

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

Using the MODE Button

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

-
- Step 1** Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

CISCO CONFIDENTIAL - Draft A1

- Step 2** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 3** Hold the **MODE** button until the Ethernet LED turns an amber color (approximately 2 to 3 seconds), and release the button.
- Step 4** After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.



Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP).

Using the Web Browser Interface

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

- Step 1** Open your Internet browser.



Note When using the access point browser interface, you should disable your browser pop-up blocker.

- Step 2** Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password page displays.
- Step 3** Enter your username in the User Name field.
- Step 4** Enter the access point password in the Password field and press **Enter**. The Summary Status page displays.
- Step 5** Click **System Software** and the System Software page displays.
- Step 6** Click **System Configuration** and the System Configuration page displays.
- Step 7** Click the **Reset to Defaults** button.



Note If the access point is configured with a static IP address, the IP address does not change.

- Step 8** After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.

Reloading the Access Point Image

If your access point has a firmware failure, you must reload the complete access point image file using the Web browser interface or by using the MODE button (see [Figure 3-4](#)). You can use the browser interface if the access point firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image.

CISCO CONFIDENTIAL - Draft A1

Using the MODE Button

You can use the MODE button on the access point to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

**Note**

If your access point experiences a firmware failure or a corrupt firmware image, indicated by the Status LED turning an amber color, you must reload the image from a connected TFTP server.

**Note**

This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the access point IP address, and SSIDs.

Follow these steps to reload the access point image file:

- Step 1** The PC you intend to use must be configured with a static IP address in the same subnet as the access point.
- Step 2** Place a copy of the access point image file (such as c1250-k9w7-tar.123-11.JA.tar) into the TFTP server folder on your PC. For additional information, refer to the [“Obtaining the Access Point Image File”](#) and [“Obtaining the TFTP Server Software”](#) sections.
- Step 3** Rename the access point image file in the TFTP server folder to **c1250-k9w7-tar.default**.
- Step 4** Activate the TFTP server.
- Step 5** If using in-line power, use a Category 5E (or higher) Ethernet cable to connect your PC to the **To Network** Ethernet connector on the power injector.
- Step 6** Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.
- Step 7** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 8** Hold the **MODE** button until the Radio LED turns a red color (approximately 20 to 30 seconds), and release the **MODE** button.
- Step 9** After the access point reboots, you must reconfigure the access point by using the Web interface, the Telnet interface, or Cisco IOS commands.

Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

**Note**

Your access point configuration is not changed when using the browser to reload the image file.

CISCO CONFIDENTIAL - Draft A1**Browser HTTP Interface**

The HTTP interface enables you to browse to the access point image file on your PC and download the image to the access point. Follow these instructions to use the HTTP interface:

Step 1 Open your Internet browser.



Note The access point web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.



Note When using the access point browser interface, you should disable your browser pop-up blocker.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password page displays.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page displays.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade page displays.

Step 6 Click the **Browse** button to locate the access point image file (such as **c1250-k9w7-tar.124-1.JA.tar**) on your PC.

Step 7 Click **Upload**.

For additional information, click the **Help** icon on the Software Upgrade page.

CISCO CONFIDENTIAL - Draft A1**Browser TFTP Interface**

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow these instructions to use a TFTP server:

Step 1 Open your Internet browser.



Note When using the access point browser interface, you should disable your browser pop-up blocker.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password page displays.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page displays.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade page displays.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point image file (such as **c1250-k9w7-tar.124-1.JA.tar**) in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click the **Upload** button.

Step 10 When a message displays that indicates the upgrade is complete, click **OK**.

For additional information click the **Help** icon on the Software Upgrade page.

CISCO CONFIDENTIAL - Draft A1

Obtaining the Access Point Image File

The access point image file can be obtained from the Cisco.com software center using these steps:

-
- Step 1** Use your Internet browser to access the Cisco Software Center at the following URL:
<http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>
 - Step 2** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
 - Step 3** Click **Access Points > Cisco Aironet 1250 Series**.
 - Step 4** Click **Cisco Aironet 1250 Access Point**.
 - Step 5** Click **IOS**.
 - Step 6** Choose the Cisco IOS release desired, such as 12.4.1-JA.
 - Step 7** Click **Wireless LAN** for an access point image file, such as c1250-k9w7-tar.123-11.JA.tar.
 - Step 8** Click **DOWNLOAD**.
 - Step 9** Read and accept the terms and conditions of the Software Download Rules.
 - Step 10** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
 - Step 11** Click **Save** to download your image file to your hard disk.
 - Step 12** Select the desired download location on your hard disk and click **Save**.
 - Step 13** When the download completes, click **Close**.
 - Step 14** Close your browser.
-

Connecting to the Access Point Locally

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

**Caution**

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

**Note**

After completing your configuration changes, you must remove the serial cable from the access point.

CISCO CONFIDENTIAL - Draft A1

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

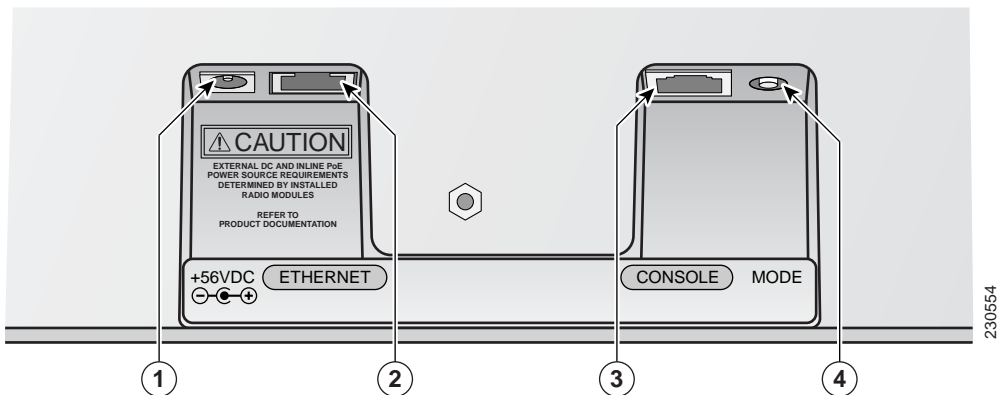
- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 console port on the access point and to the COM port on a computer.



Tip Bend the RJ-45 connector end of the cable approximately 90 degrees before attempting to connect to the access point console port.

Figure 3-4 shows the console port and MODE button locations.

Figure 3-4 Console Port and MODE Button Locations



1	DC power connector (56 VDC)	3	Console port (RJ-45)
2	Ethernet port connector (RJ-45)	4	MODE button



Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/go/marketplace> to order a serial cable.

- Step 2** Set up a terminal emulator on your PC to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Obtaining the TFTP Server Software

You can download TFTP server software from several web sites. Cisco recommends the shareware TFTP utility available at this URL:

<http://tftpd32.jounin.net>

Follow the instructions on the website for installing and using the utility.



CISCO CONFIDENTIAL - Draft A1

CHAPTER 4

Troubleshooting 1250 Series Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the 1250 series lightweight access point (model: AIR-LAP1252). 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

Sections in this chapter include:

- [Guidelines for Using Cisco Aironet Lightweight Access Points, page 4-2](#)
- [Checking the Lightweight Access Point LEDs, page 4-3](#)
- [Low Power Condition for Lightweight Access Points, page 4-6](#)
- [Manually Configuring Controller Information Using the Access Point CLI, page 4-11](#)
- [Obtaining the Autonomous Access Point Image File, page 4-14](#)
- [Obtaining the TFTP Server Software, page 4-16](#)

CISCO CONFIDENTIAL - Draft A1

Guidelines for Using Cisco Aironet Lightweight Access Points

Keep these guidelines in mind when you use a 1250 series lightweight access point:

- The access points can only communicate with Cisco 2006 series wireless LAN controllers or 4400 series controllers.

**Note**

Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series wireless LAN controllers are not supported because they lack the memory required to support access points running Cisco IOS software.

- The access points do not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support eight Basic Service Set Identifiers (BSSIDs) per radio and a total of eight wireless LANs per access point. When an access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- The access points do not support Layer 2 LWAPP. They must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes (all configuration commands are disabled when connected to a controller).

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 for Lightweight Access Points”](#) section on page G-1.

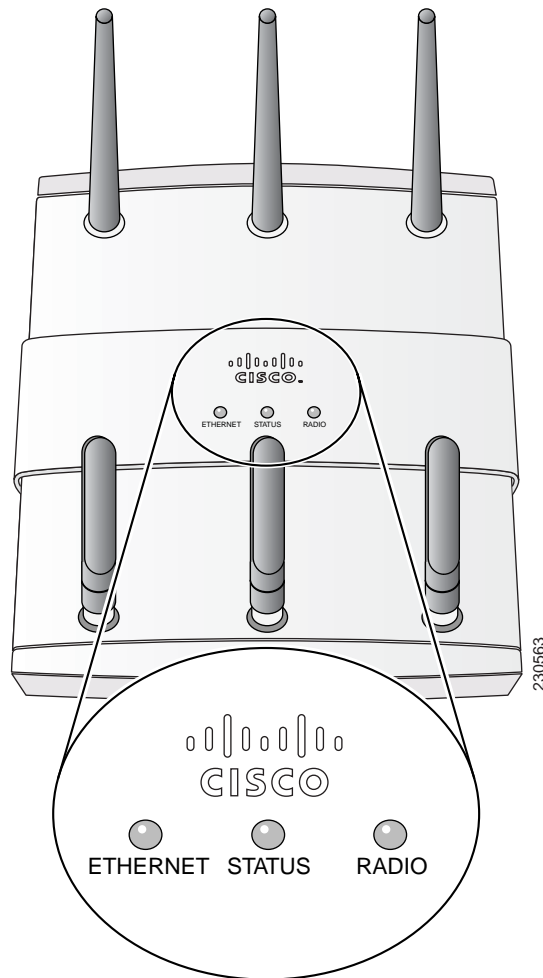
CISCO CONFIDENTIAL - Draft A1

Checking the Lightweight Access Point LEDs

If your lightweight access point is not working properly, check the Status, Ethernet, and Radio LEDs on the 2.4 GHz end of the unit. You can use the LED indications to quickly assess the unit's status.

Figure 4-1 shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

Figure 4-1 Access Point LEDs - Need New Picture



CISCO CONFIDENTIAL - Draft A1

The LED signals for lightweight access points are listed in [Table 4-1](#).

Table 4-1 *LED Signals for Lightweight Access Points*

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	Off	Amber	DRAM test in progress.
	Green	Green	Green	DRAM memory test ok.
	Off	Off	Red	Board initialization in progress.
	Off	Blinking green	Blinking green	Initialize Flash file system.
	Off	Green	Green	Flash memory test ok.
	Amber	White	Off	Initialize Ethernet.
	Green	Blinking blue	Off	Ethernet test ok.
	Green	Blinking green	Green	Starting Cisco IOS.
	Off	Off	Off	Initialization ok.
Association status	—	Green	—	Normal operating condition, but no wireless client devices are associated with the unit.
	—	Blue	—	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	—	—	Ethernet link is operational.
	Blinking green	—	—	Transmitting or receiving Ethernet packets.
	—	—	Blinking green	Transmitting or receiving radio packets.
	—	Blinking blue	—	Software upgrade in progress.
	Blinking green	Blinking green	Blinking green	Access point location command.
	Slow blinking green	—	—	Hybrid-REAP standalone mode.
Boot loader warnings	Off	Blinking red	Off	Ethernet link not operational.
	Red	Red	Off	Ethernet failure.
	Amber	Blinking blue	Off	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Red	Image recovery (Mode button pressed for 20 to 30 seconds).
	Blinking green	Blinking green	Red	Image recovery in progress and Mode button is released.

CISCO CONFIDENTIAL - Draft A1**Table 4-1 LED Signals for Lightweight Access Points (continued)**

Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Blinking red and blue	Red	Flash file system failure.
	Off	Alternating red and green	Amber	Environment variable (ENVAR) failure.
	Amber	Rapid blinking red	Off	Bad MAC address.
	Red	Blinking red and off	Off	Ethernet failure during image recovery.
	Amber	Blinking red and off	Amber	Boot environment error.
	Red	Blinking red and off	Amber	No Cisco IOS image file.
	Amber	Blinking red and off	Amber	Boot failure.
Cisco IOS errors	Blinking amber	—	—	Transmit or receive Ethernet errors.
	—	—	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Red	Off	Red	Software failure; try disconnecting and reconnecting unit power.
	—	Alternating blue, green, red, and off	—	General warning, insufficient inline power (see the “Low Power Condition for Lightweight Access Points” section).
Controller status	Alternating green, red , and amber ¹			Connecting to the controller. Note If the access point remains in this mode for more than five minutes, the access point is unable to find the controller. Ensure a DHCP server is available or that controller information is configured on the access point.
	Green	Blinking blue	Green	Loading the access point image file.

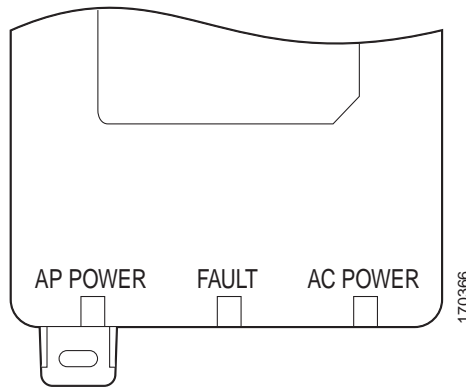
1. This status indication has the highest priority and overrides other status indications.

CISCO CONFIDENTIAL - Draft A1

Checking the Power Injector LEDs

The power injector (model:AIR-PWRINJ4) has three LEDs on the top end of the case (see [Figure 4-2](#)).

Figure 4-2 Power Injector LEDs



[Table 4-2](#) lists the power injector LED indications.

Table 4-2 Power Injector LED Indications

LED	Color	Description
AP Power	Green	Indicates DC power is available to the access point.
Fault	Red	Indicates a short or overload condition. Check Ethernet cables and connections before contacting your support organization for assistance.
AC Power	Green	Indicates AC power is available at the power injector.

Low Power Condition for Lightweight Access Points

The access point can be powered from the 1250 DC power module or from the 1250 in-line power injector. The access point supports the Cisco Intelligent Power Management.

For full operation, the access point (powered device) **requires xx W (up to yy W with 100 m CAT 5E (or higher) Ethernet cable**. When the access point is being used in a PoE configuration, the power drawn from the power sourcing equipment (PSE), such as a power injector, is higher by an amount dependent on the length of the interconnecting cable.



Note

Current switches, power patch pannels, and IEEE 802.3af compliant power sources are not able to provide sufficient power to the access point.



Note

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

CISCO CONFIDENTIAL - Draft A1

On power up, the access point is placed into low power mode (both radios are disabled), Cisco IOS software loads and runs, and power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on; otherwise, the access point remains in low power mode with the radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication (see the [“Checking the Lightweight Access Point LEDs”](#) section on page 4-3).

Intelligent Power Management - need changes

The access point requires **xx W of power** (needs **zz W of power** when operating in low power mode with both radios disabled. To help avoid an over-current condition with low power sources and to optimize power usage on Cisco switches, Cisco developed Intelligent Power Management, which uses Cisco Discovery Protocol (CDP) to allow powered devices (such as your access point) to negotiate with a Cisco switch for sufficient power.

The access point supports Intelligent Power Management and as a result of the power negotiations, the access point will either enter full power mode or remain in low power mode with the radios disabled.



Note

Independent of the power negotiations, the access point hardware also uses the 802.3af classification scheme to indicate the power required from the power source. However, the power source cannot report the power available to the access point unless the power source also supports Intelligent Power Management.

Some Cisco switches that are capable of supplying sufficient power require a software upgrade to support Intelligent Power Management. If the software upgrade is not desired, you can configure the access point to operate in pre-standard compatibility mode and the access point automatically enters full power mode if these Cisco switches are detected in the received CDP ID field.

When the access point determines that sufficient power is not available for full power operation, an error message is logged and the Status LED turns amber to indicate low power mode (see the [“Checking the Lightweight Access Point LEDs”](#) section on page 4-3 and the [“Inline Power Status Messages”](#) section on page 4-7).



Tip

If your switch is capable of supplying sufficient power for full operation but the access point remains in low-power mode, your access point or your switch (or both) might be misconfigured (see [Table 4-3](#)).

The access point can be powered by these options:

- Use the 1250 series power injector (AIR-PWRINJ4) on the switch port
- Use the 1250 series DC power module (AIR-PWR-SPLY1) to locally power the access point

Inline Power Status Messages

These messages are logged on the console port by the access point to report the power condition:

- %CDP_PD-4-POWER_OK: Full Power - AC_ADAPTOR inline power source—This message indicates the access point is using the power module and can support full-power operation.
- %CDP_PD-4-POWER_OK: Full Power - NEGOTIATED inline power source—This message indicates the access point is operating at full power and has successfully negotiated for 12.95 W of power from a Cisco switch supporting Cisco Intelligent Power Management.

CISCO CONFIDENTIAL - Draft A1

- %CDP_PD-4-POWER_OK: Full Power - HIGH_POWER_CLASSIC inline power source—This message indicates the access point is operating at full power because it has been configured for pre-standard compatibility mode and has detected a Cisco switch that does not support Intelligent Power Management but is able to supply sufficient power to the access point.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_CONFIGURED_ON_SOURCE inline power source—This message indicates the access point is operating at full power because it is connected to a Cisco switch that supports Intelligent Power Management and the switch has been configured with the *power inline never* command.
- %CDP_PD-4-POWER_OK: Full power - INJECTOR_CONFIGURED_ON_CURRENT_PORT inline power source—This message indicates the access point is operating at full power because it has been configured to expect a power injector on this port.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_PD inline power source—This message indicates the access point is operating at full power because it has detected a CDP packet from another Cisco powerable device (PD). The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not transmit this type of CDP packet.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_MULTIPLE_MACS_ON_HUB inline power source—This message indicates the access point is operating at full power because it has detected multiple Cisco devices. The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not forward CDP packets.
- %CDP_PD-4-POWER_OK: Full Power - NON_CISCO-NO_CDP_RECEIVED inline power source—This message indicates the access point is operating at full power because it has not received any CDP packets within the timeout period. This condition indicates your access point is connected to a non-Cisco power source.
- %CDP_PD-4-POWER_OK: Full power - INJECTOR_DETECTED inline power source—This message indicates that the access point has detected the 1250 series power injector (AIR-PWINJ4) and is operating at full power with both radios enabled. The **power inline negotiation injector installed** command does not have to be used to specify that the power injector is installed.

**Note**

To prevent possible over-current conditions, the power source must be an IEC60950 compliant limited power source.

- %CDP_PD-4-POWER_OK: Full power - INJECTOR_CONFIGURED_OVERRIDE_SAFETY inline power source —This message indicates the access point has been configured to override the inline power checks and a power injector is installed.

**Caution**

When using the *power inline negotiation injector override* command, a power injector must always be installed to prevent a possible overload condition with an underpowered power source.

- %CDP_PD-2-POWER_LOW: All radios disabled - NEGOTIATED inline power source—This message indicates the access point is in low power mode with all radios disabled because the Cisco power source has indicated it is not capable of supplying sufficient power to the access point.

**Note**

A Cisco power injector might be required.

CISCO CONFIDENTIAL - Draft A1

- %CDP_PD-2-POWER_LOW: All radios disabled - LOW_POWER_CLASSIC_NO_INJECTOR_CONFIGURED <platform name> (<MAC address>). —This message indicates the access point is in low power mode with all radios disabled and has detected a CDP device that is unable to supply sufficient power to the access point.

The <platform name> indicates the CDP device detected by the access point. The <MAC address> indicates the MAC address of the CDP device, typically, the switch port.



Note A Cisco power injector might be required.

Following the low power status message, two extra messages are displayed on the console port or when using a Telnet session that identify the actions needed to resolve this low power problem:

- Verify the required power injector is installed on this port: <platform name> (<Ethernet port>).
(where <platform name> indicates the CDP device detected by the access point and <Ethernet port> indicates the Ethernet port of the CDP device.
 - If a power injector is installed, issue the command: power inline negotiation injector installed.
- %CDP_PD-2-POWER_LOW: All radios disabled- LOW_POWER_CLASSIC_INJECTOR_CONFIGURED_ON_ANOTHER_PORT <platform name> (<MAC address>)—This message indicates the access point is in low power mode with all radios disabled and has detected a CDP device that is unable to supply sufficient power to the access point. A power injector has been configured, but it is for another port. It is likely that the access point has been relocated and has not been reconfigured for a new power injector.

The <platform name> indicates the CDP device detected by the access point. The <MAC address> indicates the MAC address of the CDP device, typically, the switch port.



Note A Cisco power injector might be required.

Following the low power status message, two extra messages are displayed when using the console port or a Telnet session that identify the actions needed to resolve this low power problem:

1. Verify the required power injector is installed on the new port: <platform name> (<Ethernet port>).
(where <platform name> indicates the CDP device detected by the access point and <Ethernet port> indicates the Ethernet port of the CDP device.
 2. If a power injector is installed, issue the command: power inline negotiation injector installed.
- %CDP_PD-2-POWER_LOW: All radios disabled- HIGH_POWER_CLASSIC_NOT_CONFIGURED inline power source <platform name> (<MAC address>)—This message indicates the access point is in low power mode with all radios disabled and has detected a Cisco switch that does not support Intelligent Power Management, but should be able to supply sufficient power. The access point must be configured for pre-standard compatibility.

The <platform name> indicates the Cisco platform detected by the access point. The <MAC address> indicates the MAC address of the switch port.



Note You need to upgrade the software on the Cisco switch to support Intelligent Power Management or configure the access point for pre-standard compatibility.

CISCO CONFIDENTIAL - Draft A1

- %CDP_PD-2-POWER_LOW: All radios disabled-INJECTOR_CONFIGURED_BUT_FAILS_VERIFICATION *<platform name>* (*<MAC address>*)—This message indicates the access point is in low power mode with all radios disabled and a power injector has been configured but has not been detected by the access point.

The *<platform name>* indicates the Cisco platform detected by the access point. The *<MAC address>* indicates the MAC address of the switch port.

Configuring Power Using Controller CLI Commands

Intelligent Power Management support is dependent on the version of software resident in the Cisco switch that is providing power to the access point. Each Cisco switch should be upgraded to support Intelligent Power Management. Until the software is upgraded, you can use your controller to configure the access point to operate with older switch software using these controller CLI commands:

- 1) **config ap power pre-standard enable** *<ap>*
where *<ap>* is the access point name on the controller
- 2) **config ap power injector enable** *<ap>* *<switch port MAC address>*
(where *<ap>* is the access point name on the controller
and *<switch port MAC address>* is the MAC address of the switch port to which the access point is connected)

**Note**

Refer to your controller documentation for instructions on using these commands.

You can use these controller CLI commands to inform the access point of the following:

- The Cisco switch does not support Intelligent Power Management but should be able to supply sufficient power.
- A power injector is being used to supply sufficient power and the Cisco switch does not support Intelligent Power Management.

CISCO CONFIDENTIAL - Draft A1

Refer to [Table 4-3](#) for information on when to use these special CLI controller commands and the corresponding Cisco switch power command.

**Caution**

If the access point receives power through PoE, the output current of the power sourcing equipment (PSE) cannot exceed 400 mA per port. The power source must comply with IEEE 802.3af.

Table 4-3 **Using CLI Power Commands - Changes Needed ???**

Power Source	CLI Commands	
	Cisco Wireless LAN Controller	Cisco Switch
AC power module	None required	power inline never
Cisco switch that supports Intelligent Power Management ¹	None required	power inline auto
Cisco switch that does not support Intelligent Power Management ¹	config ap power pre-standard enable	power inline auto
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	None required	power inline never³
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	None required ⁴	power inline never
Power injector used with a non-Cisco switch	None required	—
802.3af compliant non-Cisco switches	A 1250 power injector is required	—

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.
2. Power injector must be AIR-PWRINJ4.
3. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.
4. The access point detects the power injector (AIR-PWRINJ4).

Manually Configuring Controller Information Using the Access Point CLI

In a new installation, when your access point is unable to reach a DHCP server, you can manually configure needed controller information using the access point CLI. For information on how to connect to the console port, see the [“Connecting to the Access Point Locally”](#) section on [page 4-15](#).

**Note**

The CLI commands in this section can be used only on an access point that is not associated to a controller.

The static information configured with the CLI commands are used by the access point to connect with a controller. After connecting with the controller, the controller reconfigures the access point with new controller settings, but the static IP addresses for the access point and the default gateway are not changed.

CISCO CONFIDENTIAL - Draft A1

Configuring Controller Information

To manually configure controller information on a new (out-of-the-box) access point using the access point CLI interface, you can use these EXEC mode CLI commands:

```
AP# lwapp ap ip address <IP address> <subnet mask>
AP# lwapp ip default-gateway IP-address
AP# lwapp controller ip address IP-address
AP# lwapp ap hostname name
```

Where *name* is the access point name on the controller.

**Note**

The default (out-of-box) Enable password is *Cisco*.

Clearing Manually Entered Controller Information

When you move your access point to a different location in your network, you must clear the manually entered controller information to allow your access point to associate with a different controller.

**Note**

This command requires the controller configured Enable password to enter the CLI EXEC mode.

To clear or remove the manually entered controller information, you can use these EXEC mode CLI commands:

```
clear lwapp ap ip address
clear lwapp ip default-gateway
clear lwapp controller ip address
clear lwapp ap hostname
```

Manually Resetting the Access Point to Defaults

You can manually reset your access point to default settings using this EXEC mode CLI command:

**Note**

This command requires the controller configured Enable password to enter the CLI EXEC mode.

```
clear lwapp private-config
```

Returning the Lightweight Access Point to Autonomous Mode

You can return a lightweight access point to autonomous mode by loading a Cisco IOS release that supports autonomous mode (such as Cisco IOS Release 12.3(11)JA). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release (refer to your controller documentation). If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP.

CISCO CONFIDENTIAL - Draft A1

Using a Controller to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using a controller:

-
- Step 1** Log into the CLI on the controller to which the access point is associated and enter this command:
- ```
config ap tftp-downgrade tftp-server-ip-address filename access-point-name
```
- (where:
- a) *tftp-server-ip-address* is the IP address of the TFTP server
  - b) *filename* is the full path and filename of the access point image file, such as `D:/Images/c1250-k9w7-tar.123-11.JA.tar`
  - c) *access-point-name* is the name that identifies the access point on the controller.)
- Step 2** Wait until the access point reboots, as indicated by all LEDs turning green followed by the Status LED blinking green.
- Step 3** After the access point reboots, reconfigure it using the access point GUI or the CLI.
- 

## Using the MODE Button to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using the access point MODE button and a TFTP server:

**Note**

The access point MODE button is enabled by default, but you need to verify that the MODE button is enabled (see the [“MODE Button Setting” section on page 4-14](#)).

- 
- Step 1** Set the static IP address of the PC on which your TFTP server software runs to an address between 10.0.0.2 and 10.0.0.30.
- Step 2** Make sure that the PC contains the access point image file (such as *c1250-k9w7-tar.123-11.JA.tar* for a 1250 series access point) in the TFTP server folder and that the TFTP server is activated.
- Step 3** Rename the access point image file in the TFTP server folder to **c1250-k9w7-tar.default**.
- Step 4** Connect the PC to the access point using a Category 5E (or higher) Ethernet cable.
- Step 5** Disconnect power from the access point.
- Step 6** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 7** Hold the **MODE** button until the Radio LED turns red (approximately 20 to 30 seconds) and then release.
- Step 8** Wait until the access point reboots, as indicated by all LEDs turning green followed by the Status LED blinking green.
- Step 9** After the access point reboots, reconfigure it using the access point GUI or the CLI.
-

**CISCO CONFIDENTIAL - Draft A1**

## MODE Button Setting

The lightweight access point MODE button is configured from your Cisco Wireless LAN Controller. Use these controller CLI commands to view and configure the MODE button:

- 1) `config ap rst-button enable <access-point-name>/all`
- 2) `config ap rst-button disable <access-point-name>/all`
- 3) `show ap config general <access-point-name>`  
(Where *access-point-name* is the name that identifies the access point on the ocontroller.)

## Obtaining the Autonomous Access Point Image File

The autonomous access point image file can be obtained from the Cisco.com software center using these steps:

**Note**

To download software from the Cisco.com software center, you must be a registered user. You can register from the main Cisco.com web page at this URL: <http://cisco.com>.

- Step 1** Use your Internet browser to access the Cisco Software Center at the following URL:  
<http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>
- Step 2** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
- Step 3** Click **Access Points > Aironet Access Points > Cisco Aironet 1250 Series**.
- Step 4** Click **Cisco Aironet 1250 Access Point**.
- Step 5** Click **IOS**.
- Step 6** Choose the Cisco IOS release desired, such as 12.3.11.JA.
- Step 7** Click **Wireless LAN** for an access point image file, such as c1250-k9w7-tar.123-11.JA.tar.
- Step 8** Click **DOWNLOAD**.
- Step 9** Read and accept the terms and conditions of the Software Download Rules.
- Step 10** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
- Step 11** Click **Save** to download your image file to your hard disk.
- Step 12** Select the desired download location on your hard disk and click **Save**.
- Step 13** When the download completes, click **Close**.
- Step 14** Close your browser.

CISCO CONFIDENTIAL - Draft A1

# Connecting to the Access Point Locally

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

  
**Caution**

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

  
**Note**

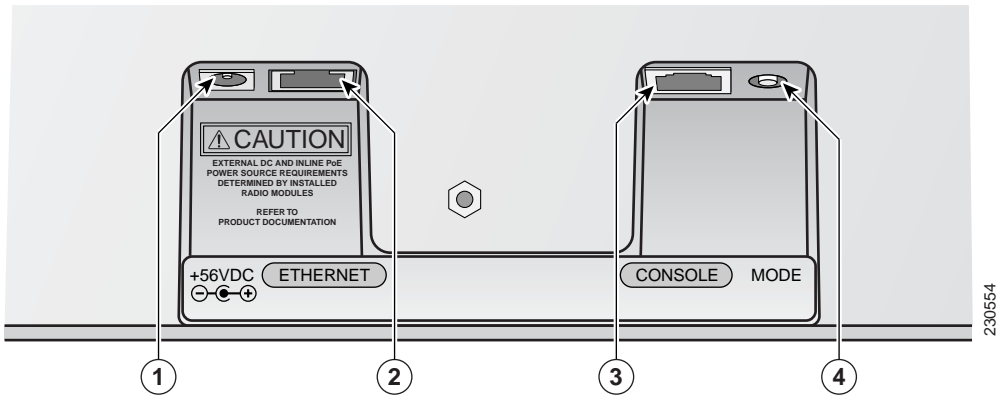
After completing your configuration changes, you must remove the serial cable from the access point.

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

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

Figure 4-3 shows the console port location.

Figure 4-3 Console Port Location



|   |                             |   |                      |
|---|-----------------------------|---|----------------------|
| 1 | DC power connector (56 VDC) | 3 | Console port (RJ-45) |
| 2 | Ethernet port (RJ-45)       | 4 | MODE button          |



**Note** The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/go/marketplace> to order a serial cable.

**Step 2** Set up a terminal emulator on your PC to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

***CISCO CONFIDENTIAL - Draft A1***

## Obtaining the TFTP Server Software

You can download TFTP server software from several web sites. Cisco recommends the shareware TFTP utility available at this URL:

<http://tftpd32.jounin.net>

Follow the instructions on the website for installing and using the utility.



**CISCO CONFIDENTIAL - Draft A1**

## 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 1250 Series** listed under Access Points.
  - Step 3** Click **Install and Upgrade Guides**.
  - Step 4** Click **Translated Safety Warnings for Cisco Aironet 1000, 1100, 1130AG, 1200, 1240AG, and 1250 Series Access Points**.
-

***CISCO CONFIDENTIAL - Draft A1***



**CISCO CONFIDENTIAL - Draft A1**

## **APPENDIX B**

# **Declarations of Conformity and Regulatory Information**

---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1250 Series Autonomous Access Point and the Cisco Aironet 1250 Series Lightweight Access Point.

This appendix contains the following sections:

- [Manufacturers Federal Communication Commission Declaration of Conformity Statement, page B-2](#)
- [Department of Communications—Canada, page B-4](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page B-4](#)
- [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](#)

**CISCO CONFIDENTIAL - Draft A1**

# Manufacturers Federal Communication Commission Declaration of Conformity Statement

**Models**

AIR-RM1252A-A-K9

AIR-RM1252G-A-K9

**Certification Numbers**

LDK102061

LDK102062

**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.



**CISCO CONFIDENTIAL - Draft A1****Caution**

Within the 5.15 to 5.25 GHz band (5 GHz radio channels 34 to 48) the UNII 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。

**CISCO CONFIDENTIAL - Draft A1**

# Department of Communications—Canada

**Certification Numbers**

2461B-102061

2461B-102062

## 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. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

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

**Models:**

AIR-RM1252A-E-K9

AIR-RM1252G-E-K9

**CISCO CONFIDENTIAL - Draft A1****Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC**

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

142729

**CISCO CONFIDENTIAL - Draft A1**

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

142730

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 60950-1

**Note**

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

**CISCO CONFIDENTIAL - Draft A1**

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 60950-1

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.

---

**CISCO CONFIDENTIAL - Draft A1**

# Guidelines for Operating Cisco Aironet Access Points in Japan

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

## Japanese Translation

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

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

連絡先 : 03-5549-6500

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

**CISCO CONFIDENTIAL - Draft A1**

# 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.

**CISCO CONFIDENTIAL - Draft A1****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.



***CISCO CONFIDENTIAL - Draft A1***

## 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 below:

***CISCO CONFIDENTIAL - Draft A1***



**CISCO CONFIDENTIAL - Draft A1**

# APPENDIX **C**


## Access Point Specifications

Table C-1 lists the technical specifications for the Cisco Aironet 1250 Series Access Point.

**Table C-1**      **Access Point Specifications**

| Category              | 2.4 GHz Radio Specifications                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5 GHz Radio Specifications |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Size                  | 8.1 in W x 9.5 in D x 2.3 in H<br>20.6 cm W x 24.1 cm D x 5.8 cm H                                                                                                                                                                                                                                                                                                                                                                                           |                            |
| Weight                | Base access point (without modules): 2.1 lbs (0.78 kg)<br>2.4- GHz radio module: 1.4 lbs (0.52 kg)<br>5-GHz radio module: 1.4 lbs (0.52 kg)<br>Blank radio module: 1.1 lbs (0.41 kg)                                                                                                                                                                                                                                                                         |                            |
| Indicators            | Three indicators on top of unit: Ethernet traffic, status, and radio traffic.                                                                                                                                                                                                                                                                                                                                                                                |                            |
| Connectors            | Base unit (bottom of access point):<br><br>DC power connector (for plug-in power module); RJ-45 connector for 10BASE-T or 100BASE-T or 1000BASE-T Ethernet connections; RJ-45 connector for serial console port connections.<br><br>2.4 GHz radio module (left to right) RP-TNC antenna connectors:<br><br>Left (A-Tx/Rx); middle (C-Rx), right (B-Tx/Rx).<br><br>5-GHz radio module (left to right):<br><br>Left (A-Tx/Rx); middle (C-Rx), right (B-Tx/Rx). |                            |
| Input voltage         | 44 to 57 VDC (56 VDC nominal)                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| Input power           | Single radio module—13 W (up to 15.4 W with a 100 m CAT 5E Ethernet cable)—maximum<br>Dual radio modules —23W (up to TBD W with a 100 m CAT 5E Ethernet cable)—maximum                                                                                                                                                                                                                                                                                       |                            |
| Operating temperature | Access point, DC power module, and power injector:<br><br>–4 to 131°F (–20 to 55°C)                                                                                                                                                                                                                                                                                                                                                                          |                            |
| Storage temperature   | –40 to 185°F (–40 to 85°C)                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| Humidity              | 10 to 90% non-condensing                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
| Operating altitude    | 10,000 ft (3048 m) maximum                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |

**CISCO CONFIDENTIAL - Draft A1****Table C-1 Access Point Specifications (continued)**

| Category          | 2.4 GHz Radio Specifications                                                                                                                                                                                                                                                                                                         |                                                                             |                                                                                                                                                                                                                                                         | 5 GHz Radio Specifications                                                                                                                                         |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power output      | 802.11b                                                                                                                                                                                                                                                                                                                              | 802.11g and 802.11n                                                         |                                                                                                                                                                                                                                                         | 802.11a and 802.11n                                                                                                                                                |
|                   | 23 dBm                                                                                                                                                                                                                                                                                                                               | 17 dBm                                                                      |                                                                                                                                                                                                                                                         | 50 mW (17 dBm)                                                                                                                                                     |
|                   | 20 dBm                                                                                                                                                                                                                                                                                                                               | 14 dBm                                                                      |                                                                                                                                                                                                                                                         | 25 mW (14 dBm)                                                                                                                                                     |
|                   | 17 dBm                                                                                                                                                                                                                                                                                                                               | 11 dBm                                                                      |                                                                                                                                                                                                                                                         | 12 mW (11 dBm)                                                                                                                                                     |
|                   | 14 dBm)                                                                                                                                                                                                                                                                                                                              | 8 dBm                                                                       |                                                                                                                                                                                                                                                         | 6 mW (8 dBm)                                                                                                                                                       |
|                   | 11 dBm                                                                                                                                                                                                                                                                                                                               | 5 dBm                                                                       |                                                                                                                                                                                                                                                         | 3 mW (5 dBm)                                                                                                                                                       |
|                   | 8 dBm                                                                                                                                                                                                                                                                                                                                | 2 dBm                                                                       |                                                                                                                                                                                                                                                         | 2 mW (2 dBm)                                                                                                                                                       |
|                   | 5 dBm                                                                                                                                                                                                                                                                                                                                | -1 dBm                                                                      |                                                                                                                                                                                                                                                         | 1 mW (-1 dBm)                                                                                                                                                      |
|                   | 2 dBm                                                                                                                                                                                                                                                                                                                                | (Depending on the regulatory domain in which the access point is installed) |                                                                                                                                                                                                                                                         | (Depending on the regulatory domain in which the access point is installed)                                                                                        |
|                   | -1 dBm                                                                                                                                                                                                                                                                                                                               |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |
|                   | (Depending on the regulatory domain in which the access point is installed)                                                                                                                                                                                                                                                          |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |
|                   | <b>Note</b> For the maximum power and the channels allowed in your regulatory domain, refer to the <i>Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges</i> or the <i>Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points</i> .                                 |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |
| Antenna           | Three external antenna connectors on each radio module.                                                                                                                                                                                                                                                                              |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |
| Frequency         | 2.400 to 2.497 GHz<br>(Depending on the regulatory domain in which the access point is installed)                                                                                                                                                                                                                                    |                                                                             |                                                                                                                                                                                                                                                         | 5.15 to 5.25 GHz<br>5.25 to 5.35 GHz<br>5.470 to 5.725 GHz<br>5.725 to 5.85 GHz<br><br>(Depending on the regulatory domain in which the access point is installed) |
| Data Rates (Mbps) | 802.11b                                                                                                                                                                                                                                                                                                                              | 802.11g                                                                     | 802.11n                                                                                                                                                                                                                                                 | 802.11n                                                                                                                                                            |
|                   | 1, 2, 5.5, and 11                                                                                                                                                                                                                                                                                                                    | 6, 9, 12, 18, 24, 36, 48, and 54                                            | 6.5, 7.22, 13, 13.5, 14.44, 15, 19.5, 21.67, 26, 27, 28.89, 30, 39, 40.5, 43.33, 45, 52, 54, 57.78, 58.5, 60, 65, 72.22, 78, 81, 86.67, 90, 104, 108, 115.56, 117, 120, 121.5, 130, 135, 144.44, 157.5, 162, 180, 216, 180, 216, 240, 243, 270, and 300 |                                                                                                                                                                    |
| Compliance        | The 1250 series access point complies with UL 2043 for products installed in a building’s environmental air handling spaces, such as above suspended ceilings.                                                                                                                                                                       |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |
|                   | <div><div></div><div><b>Caution</b> The 1250 power injector (AIR-PWRINJ4), the 1250 DC power module (AIR-PWR-SPLY1), and the antennas should not be placed in a building’s environmental air space, such as above suspended ceilings.</div></div> |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |
| Safety            | IEC60950-1<br>UL60950-1<br>CAN/CSA C22.2 Number 60950-1-03<br>EN60950-1<br>UL 2043                                                                                                                                                                                                                                                   |                                                                             |                                                                                                                                                                                                                                                         |                                                                                                                                                                    |

**CISCO CONFIDENTIAL - Draft A1****Table C-1** Access Point Specifications (continued)

| Category               | 2.4 GHz Radio Specifications                                                                                                           | 5 GHz Radio Specifications |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Radio approvals        | FCC Parts 15.401 -15.407<br>FCC Bulletin OET-65C<br>RSS-210 and RSS-102<br>EN 301.893<br>AS 4268.2<br>ARIB STD-T71<br>Telec 33B        |                            |
| EMI and susceptibility | FCC Part 15.107 and 15.109 Class B<br>ICES-003 Class B (Canada)<br>EN 55022 Class B<br>EN 55024<br>AS/NZS 3548 Class B<br>VCCI Class B |                            |
| RF exposure            | OET-65C<br>RSS-102<br>ANSI C95.1                                                                                                       |                            |

***CISCO CONFIDENTIAL - Draft A1***



**CISCO CONFIDENTIAL - Draft A1**

## APPENDIX **D**

# Channels and Power Levels

---

For channel and maximum power level settings, refer to *Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges* or 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 1250 Series** listed under Access Points.
  - Step 3** Click **Install and Upgrade Guides**.
  - Step 4** Click **Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges**, or **Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges**.
-

***CISCO CONFIDENTIAL - Draft A1***





**CISCO CONFIDENTIAL - Draft A1**

## APPENDIX **E**

# Console Cable Pinouts

---

This appendix identifies the pinouts for the serial console cable that connects to the access point's serial console port. The appendix contains the following sections:

- [Overview, page E-2](#)
- [Console Port Signals and Pinouts, page E-2](#)

**CISCO CONFIDENTIAL - Draft A1**

# Overview

The access point requires a special serial cable that connects the access point serial console port (RJ-45 connector) to your PC's COM port (DB-9 connector). This cable can be purchased from Cisco (part number AIR-CONCAB1200) or can be built using the pinouts in this appendix.

## Console Port Signals and Pinouts

Use the console RJ-45 to DB-9 serial cable to connect the access point's console port to the COM port of your PC running a terminal emulation program.

**Note**

Both the Ethernet and console ports use RJ-45 connectors. Be careful to avoid accidentally connecting the serial cable to the Ethernet port connector.

**Note**

After completing your configuration changes, you must remove the serial console cable from the access point.

[Table E-1](#) lists the signals and pinouts for the console RJ-45 to DB-9 serial cable.

**Table E-1** *Signals and Pinouts for a Console RJ-45 to DB-9 Serial Cable*

| Console Port |                  | PC COM Port |                  |
|--------------|------------------|-------------|------------------|
| RJ-45        |                  | DB-9        |                  |
| Pins         | Signals          | Pins        | Signals          |
| 1            | NC <sup>1</sup>  | —           | —                |
| 2            | NC <sup>1</sup>  | —           | —                |
| 3            | TXD <sup>2</sup> | 2           | RXD <sup>3</sup> |
| 4            | GND <sup>4</sup> | 5           | GND <sup>4</sup> |
| 5            | GND <sup>3</sup> | 5           | GND <sup>4</sup> |
| 6            | RXD <sup>5</sup> | 3           | TXD <sup>2</sup> |
| 7            | NC <sup>1</sup>  | —           | —                |
| 8            | NC <sup>1</sup>  | —           | —                |

1. NC indicates not connected.
2. TXD indicates transmit data.
3. RXD indicates receive data.
4. GND indicates ground.



**CISCO CONFIDENTIAL - Draft A1**

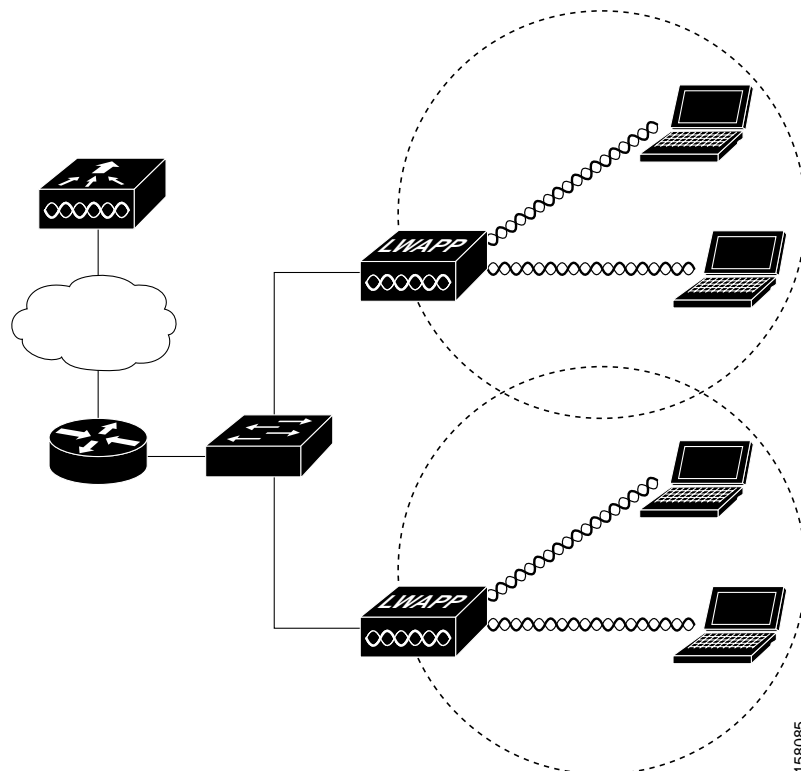
## APPENDIX **F**

# Priming Lightweight Access Points Prior to Deployment

This section describes an optional procedure designed to prime or stage your lightweight access points in a convenient location rather than after they are installed in possibly difficult to reach locations. This process can be used when a DHCP server is not reachable by your deployed access point and it helps limit potential installation problems to primarily Ethernet and power areas.

Figure F-1 illustrates a typical priming configuration for your lightweight access points.

**Figure F-1**      *Typical Lightweight Access Point Priming Configuration*



**CISCO CONFIDENTIAL - Draft A1**

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

- Step 1** In a Layer 2 environment, where the lightweight 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 lightweight access points. The access points will receive its IP address and controller information using DHCP Option 43.

The lightweight 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 more information, refer to the [“Configuring DHCP Option 43 for Lightweight Access Points” section on page G-1](#).



**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 that 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 lightweight access points:

- a.** Connect your lightweight access points to untagged access ports on your POE capable switch. You can optionally use power modules or power injectors to power your access points.
- b.** After you power up the lightweight access point, it begins a power-up sequence that you can check by observing the access point LEDs. All LEDs blink sequentially back and forth, indicating that the access point is trying to find a controller.



**Note** If the lightweight 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 lightweight access point shuts down (all LEDs off), check to ensure that sufficient power is available.

**CISCO CONFIDENTIAL - Draft A1**

- d. When the lightweight 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 lightweight access point reboots. Normal operation is indicated when the radio LED is blinking to indicate radio activity.
- Step 7** Use the controller CLI, controller GUI, or Cisco WCS to configure the lightweight access point with primary, secondary, and tertiary controller names.
- Step 8** If the lightweight 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 radio LED is 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 lightweight access points, ensure that the Master setting is disabled on your controller. Also you can begin deploying the access points to their final destinations.

---

***CISCO CONFIDENTIAL - Draft A1***



**CISCO CONFIDENTIAL - Draft A1**

## APPENDIX **G**

# Configuring DHCP Option 43 for Lightweight Access Points

---

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 Cisco Aironet lightweight access points. This appendix contains these sections:

- [Overview, page G-2](#)
- [Configuring Option 43 for 1000 Series Access Points, page G-2](#)
- [Configuring Option 43 for 1100, 1130, 1200, 1240, 1250, and 1300 Series Lightweight Access Points, page G-3](#)

**CISCO CONFIDENTIAL - Draft A1**

# 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 their product 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 and 1500 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 G-1](#):

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

| Access Point              | Vendor Class Identifier (VCI)                |
|---------------------------|----------------------------------------------|
| Cisco Aironet 1000 series | A 1respace A P1200                           |
| Cisco Aironet 1100 series | C 1sco A P c1100                             |
| Cisco Aironet 1130 series | C 1sco A P c1130                             |
| Cisco Aironet 1200 series | C 1sco A P c1200                             |
| Cisco Aironet 1240 series | C 1sco A P c1240                             |
| Cisco Aironet 1250 series | C 1sco A P c1250                             |
| Cisco Aironet 1300 series | C 1sco A P c1300                             |
| Cisco Aironet 1500 series | C 1sco A P L A P1510 or C 1sco A P L A P1505 |

The format of the TLV block for 1100, 1130, 1200, 1240, 1250, 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>
```



**CISCO CONFIDENTIAL - Draft A1**

```
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, 1250, and 1300 Series Lightweight Access Points

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, 1250, 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 G-1](#). The quotation marks must be included.

**CISCO CONFIDENTIAL - Draft A1**

**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
```

---



**CISCO CONFIDENTIAL - Draft A1**

## **GLOSSARY**

- 802.3af** The IEEE standard that describes a mechanism for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling.
- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
- 802.11a** The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 6, 9, 12, 18, 24, 36, 48, and 54 Mbps wireless LANs operating in the 2.4-GHz frequency band.

## **A**

- access point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- ad hoc network** A wireless network composed of stations without Access Points.
- antenna gain** The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High gain antennas have a more focused radiation pattern in a specific direction.
- associated** A station is configured properly to allow it to wirelessly communicate with an Access Point.

**CISCO CONFIDENTIAL - Draft A1****B**

|                         |                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>beacon</b>           | A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode. |
| <b>BOOTP</b>            | Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.                                                                                                                                                 |
| <b>BPSK</b>             | Binary phase shift keying is a modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.                                                                                                                        |
| <b>broadcast packet</b> | A single data message (packet) sent to all addresses on the same subnet.                                                                                                                                                                            |

**C**

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CCK</b>    | Complementary Code Keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>CCKM</b>   | Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. |
| <b>cell</b>   | The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.                                                                                                                                                                                                                                                     |
| <b>client</b> | A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>CSMA</b>   | Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.                                                                                                                                                                                                                                                                                                                                                                                                   |

**D**

|                   |                                                                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>data rates</b> | The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).                                                                   |
| <b>dBi</b>        | A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage. |
| <b>DFS</b>        | Dynamic Frequency Selection. In some regulatory domains, 5-GHz radios are required to use DFS to avoid interfering with radar signals.                                               |

**CISCO CONFIDENTIAL - Draft A1**

|                    |                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DHCP</b>        | Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.                          |
| <b>dipole</b>      | A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.                                                                                                                                                                                                              |
| <b>domain name</b> | The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on. |
| <b>DNS</b>         | Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.                                                                                                             |
| <b>DSSS</b>        | Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.                                                                                                                                                 |

**E**

|                 |                                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>EAP</b>      | Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server. |
| <b>Ethernet</b> | The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used. |

**F**

|                    |                                                                                          |
|--------------------|------------------------------------------------------------------------------------------|
| <b>file server</b> | A repository for files so that a local area network can share files, mail, and programs. |
| <b>firmware</b>    | Software that is programmed on a memory chip.                                            |

**G**

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| <b>gateway</b> | A device that connects two otherwise incompatible networks together.       |
| <b>GHz</b>     | Gigahertz. One billion cycles per second. A unit of measure for frequency. |

**CISCO CONFIDENTIAL - Draft A1****I**

|                       |                                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IEEE</b>           | Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications. |
| <b>infrastructure</b> | The wired Ethernet network.                                                                                                                                                                                                                                            |
| <b>IP Address</b>     | The Internet Protocol (IP) address of a station.                                                                                                                                                                                                                       |
| <b>IP subnet mask</b> | The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.                     |
| <b>isotropic</b>      | An antenna that radiates its signal in a spherical pattern.                                                                                                                                                                                                            |

**M**

|                         |                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MAC</b>              | Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.                                             |
| <b>MBSSID</b>           | Multiple basic SSID. Each multiple basic SSID is assigned a unique MAC address. You use multiple BSSIDs to assign a unique DTIM setting for each SSID and to broadcast SSIDs in beacons (one SSID per beacon). |
| <b>modulation</b>       | Any of several techniques for combining user information with a transmitter's carrier signal.                                                                                                                  |
| <b>multipath</b>        | The echoes created as a radio signal bounces off of physical objects.                                                                                                                                          |
| <b>multicast packet</b> | A single data message (packet) sent to multiple addresses.                                                                                                                                                     |

**O**

|                         |                                                                                                                                                                           |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>omni-directional</b> | This typically refers to a primarily circular antenna radiation pattern.                                                                                                  |
| <b>OFDM</b>             | Orthogonal frequency division multiplex is a modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. |

**P**

|               |                                                                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>packet</b> | A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information. |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

**CISCO CONFIDENTIAL - Draft A1****Q****QPSK**

Quadruple phase shift keying is a modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

**R****range**

A linear measure of the distance that a transmitter can send a signal.

**receiver sensitivity**

A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

**RF**

Radio frequency. A generic term for radio-based technology.

**roaming**

A feature of some Access Points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

**RP-TNC**

A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

**S****spread spectrum**

A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

**SSID**

Service set identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

**T****transmit power**

The power level of radio transmission.

**CISCO CONFIDENTIAL - Draft A1****U**

|                       |                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>UNII</b>           | Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands. |
| <b>UNII-1</b>         | Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.                                                                        |
| <b>UNII-2</b>         | Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.                                                                        |
| <b>UNII-3</b>         | Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.                                                                      |
| <b>unicast packet</b> | A single data message (packet) sent to a specific IP address.                                                                                         |

**W**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WDS</b>         | Wireless Domain Services. An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. |
| <b>WEP</b>         | Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.                                                                                                                                                                                                                                                                               |
| <b>WLSE</b>        | Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco Aironet wireless LAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations. WLSE's centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity.                 |
| <b>WNM</b>         | Wireless Network Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>workstation</b> | A computing device with an installed client adapter.                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>WPA</b>         | Wi-Fi Protected Access is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.                                      |





**CISCO CONFIDENTIAL - Draft A1**

## INDEX

---

### Numerics

2.4-GHz radio module [1-4](#)

5-GHz radio module [1-4](#)

---

### A

access point

image [3-17](#)

module rail [2-26](#)

size [C-1](#)

types [1-1](#)

antenna connectors [C-2](#)

antennas [1-6](#)

autonomous access point [1-1](#)

---

### B

basic settings, checking [3-5](#)

blank module [1-4](#)

box hanger [2-9](#)

bridge configuration [1-1](#)

---

### C

cables, connecting [2-14](#)

central unit [1-12](#)

CLI

terminal emulator settings [3-21, 4-15](#)

connectors [C-1, C-2](#)

console port [1-2, 1-7, E-2](#)

controller [1-2](#)

---

### D

DC power module [1-8, 2-14](#)

declarations of conformity [B-1](#)

default, configuration, resetting [3-16](#)

DHCP Option 43 [4-2, G-1](#)

DHCP pool [G-2](#)

---

### E

Ethernet

LED [1-6](#)

MAC address [1-7](#)

port [1-7](#)

extended temperature range [2-3, 2-4](#)

---

### F

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

FCC Safety Compliance [2-2](#)

frequency range [C-2](#)

---

### G

ground wire [2-7, 2-9](#)

guidelines, installation [2-4](#)

---

### I

indicators [3-2, 4-3](#)

input power [C-1](#)

installation guidelines [2-4](#)

**CISCO CONFIDENTIAL - Draft A1**

---

**K**

key features [1-3](#)

---

**L**

latch, radio module [2-24](#)  
layer 3 network [1-14](#)  
LEDs [1-6](#)  
lightweight access point [1-1](#)  
local power [2-16](#)  
LWAPP [1-2](#)

---

**M**

MAC address, Ethernet [1-7](#)  
Mode button [3-17](#)  
modules [1-4](#)  
mounting  
    above a suspended ceiling [2-9](#)  
    below a suspended ceiling [2-8](#)  
    bracket clip [2-9](#)  
    clip holes [2-11](#)  
    desktop or shelf [2-13](#)  
    hardware kit [2-3](#)  
    horizontal or vertical [2-7](#)  
    orientations [2-5](#)  
mounting plate  
    holes [2-6](#)  
    installation [2-18](#)  
    latch [2-17, 2-20, 2-24](#)  
    marking [2-19](#)

---

**N**

needed material [2-7](#)  
network examples [1-10](#)  
non-root bridge [1-12](#)

---

---

**O**

operating temperature [C-1](#)  
outline, on mounting plate [2-19](#)

---

**P**

package contents [2-3](#)  
padlock [2-21](#)  
padlock hole [2-20](#)  
padlock security [1-9](#)  
password reset [3-16](#)  
pinouts, serial cable [E-2](#)  
point-to-point bridge configuration [1-14](#)  
power  
    connecting [2-14](#)  
    input [C-1](#)  
    output [C-2](#)  
power cables [2-14](#)  
power injector [1-8, 2-14](#)  
power options [2-14](#)  
power sources [1-8](#)  
priming access points [F-1](#)

---

**R**

Radio LED [1-6](#)  
radio module  
    2.4 GHz [1-4](#)  
    5 GHz [1-4](#)  
    blank [1-4](#)  
    inserting [2-26](#)  
    latch  
        closing [2-27](#)  
        opening [2-25](#)  
    slot [1-5, 2-26](#)  
radios supported [1-1](#)  
range, radio [C-2](#)  
regulatory information [B-1](#)

---

**CISCO CONFIDENTIAL - Draft A1**

reloading access point image [3-17](#)  
 repeater operation [1-11](#)  
 RF exposure [B-7](#)  
 root bridge [1-12](#)  
 root unit [1-10](#)

---

**S**

safety warnings, translated [A-1](#)  
 security cable [2-22](#)  
 security cable key slot [1-9, 2-19](#)  
 security padlock hole [2-20](#)  
 serial  
     cable [E-2](#)  
     Cisco cable [1-7, E-2](#)  
 serial number  
     access point [xiii](#)  
     radio module [xiv](#)  
 size, access point [C-1](#)  
 slot 1 [2-24](#)  
 slot 2 [2-24](#)  
 status indicators [C-1](#)  
 Status LED [1-6](#)

---

**T**

T-bar box hanger [2-9](#)  
 T-bar grid [2-9](#)  
 temperature  
     operating [C-1](#)  
     storage [C-1](#)  
 terminal emulator [3-21, 4-15](#)  
 terminal emulator settings [1-7](#)  
 TFTP server [3-17](#)  
 T-rail clip studs [2-9](#)  
 troubleshooting [3-1, 4-1](#)  
 type-length-value (TLV) [G-2](#)

---

**U**

UL2043 compliance [1-8](#)  
 Unlicensed National Information Infrastructure (UNII) [1-5](#)  
 unpacking [2-3](#)

---

**V**

vendor class identifier (VCI) [G-2](#)  
 voltage range [C-1](#)

---

**W**

warnings [2-2, A-1](#)  
 web site, Cisco Software Center [3-20, 4-14](#)  
 weight [C-1](#)  
 WEP key [3-6](#)  
 Wi-Fi [1-1](#)  
 Wireless Domain Services (WDS) [1-2](#)  
 workgroup bridge [1-13](#)

---

**X**

X.509 certificate [1-2](#)

***CISCO CONFIDENTIAL - Draft A1***