CISCO SYSTEMS

CISCO CONFIDENTIAL - Draft 2

Cisco Aironet 1200 Series Access Point Hardware Installation Guide

September 2004

Corporate 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: 408 526-4100

Customer Order Number:
Text Part Number: OL-4310-03

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.

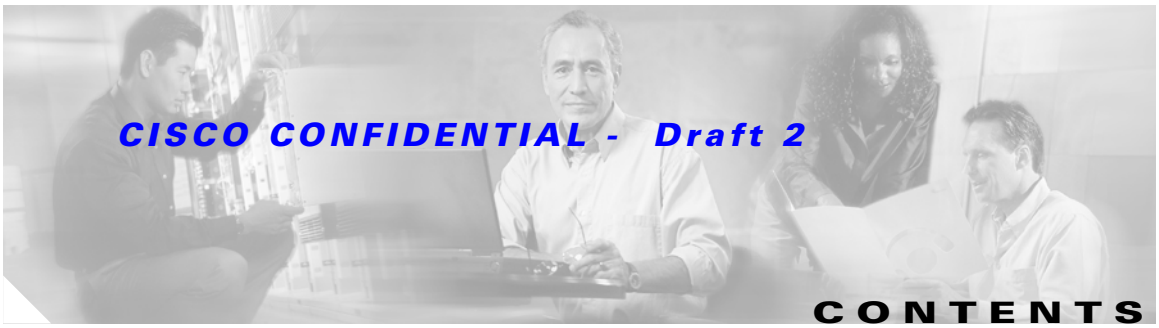
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0406R)

Cisco Aironet 1200 Series Access Point Hardware Installation Guide
Copyright © 2004 Cisco Systems, Inc. All rights reserved.



Preface ix

Audience ix

Purpose ix

Organization ix

Conventions x

Related Publications xii

Obtaining Documentation xii

Cisco.com xii

Documentation CD-ROM xiii

Ordering Documentation xiii

Documentation Feedback xiii

Obtaining Technical Assistance xiv

Cisco.com xiv

Technical Assistance Center xiv

Locating the Product Serial Number xv

Cisco TAC Website xv

Cisco TAC Escalation Center xvi

Obtaining Additional Publications and Information xvi

CHAPTER 1 **Overview** 1-1

Hardware Features 1-2

Dual-Radio Operation 1-2

Ethernet Port 1-2

Console Port 1-3

LEDs 1-3

Power Sources 1-4

UL 2043 Certification 1-4

Anti-Theft Features 1-4

Network Configuration Examples 1-5

Root Unit on a Wired LAN 1-5

Repeater Unit that Extends Wireless Range 1-6

Central Unit in an All-Wireless Network 1-7

CISCO CONFIDENTIAL - Draft 2

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

Safety Information 2-2

FCC Safety Compliance Statement 2-2

General Safety Guidelines 2-2

Warnings 2-2

Unpacking the Access Point 2-3

Package Contents 2-3

Basic Installation Guidelines 2-3

Installation Above Suspended Ceilings 2-3

Before Beginning the Installation 2-4

Installation Summary 2-5

Connecting the 2.4-GHz Antennas 2-6

Connecting the 5-GHz External Antennas 2-6

Connecting the Ethernet and Power Cables 2-7

Connecting to an Ethernet Network with an Inline Power Source 2-8

Connecting to an Ethernet Network with Local Power 2-8

Powering Up the Access Point 2-9

CHAPTER 3 **Configuring the Access Point for the First Time** 3-1

Before You Start 3-2

Resetting the Access Point to Default Settings 3-2

Obtaining and Assigning an IP Address 3-3

Connecting to the Access Point Locally 3-3

Assigning Basic Settings 3-4

Default Settings on the Express Setup Page 3-8

Protecting Your Wireless LAN 3-8

Using the IP Setup Utility 3-9

Obtaining and Installing IPSU 3-9

Using IPSU to Find the Access Point's IP Address 3-10

Using IPSU to Set the Access Point's IP Address and SSID 3-11

Assigning an IP Address Using the CLI 3-12

Using a Telnet Session to Access the CLI 3-12

CISCO CONFIDENTIAL - Draft 2

CHAPTER 4 **Using the Web-Browser Interface** 4-1

Using the Web-Browser Interface for the First Time 4-2

Using the Management Pages in the Web-Browser Interface 4-2

Using Action Buttons 4-4

Character Restrictions in Entry Fields 4-5

Using Online Help 4-5

CHAPTER 5 **Using the Command-Line Interface** 5-1

IOS Command Modes 5-2

Getting Help 5-3

Abbreviating Commands 5-3

Using no and default Forms of Commands 5-3

Understanding CLI Messages 5-4

Using Command History 5-4

Changing the Command History Buffer Size 5-4

Recalling Commands 5-5

Disabling the Command History Feature 5-5

Using Editing Features 5-5

Enabling and Disabling Editing Features 5-6

Editing Commands Through Keystrokes 5-6

Editing Command Lines that Wrap 5-7

Searching and Filtering Output of show and more Commands 5-8

Accessing the CLI 5-8

Opening the CLI with Telnet 5-8

Opening the CLI with Secure Shell 5-9

CHAPTER 6 **Mounting Instructions** 6-1

Overview 6-2

Mounting on a Horizontal or Vertical Surface 6-3

Mounting Below a Suspended Ceiling 6-4

Mounting Above a Suspended Ceiling 6-5

Attaching the Access Point to the Mounting Bracket 6-7

Securing the Access Point to the Mounting Bracket 6-7

CISCO CONFIDENTIAL - Draft 2

CHAPTER 7 **2.4-GHz Radio Upgrade** 7-1

Upgrade Overview 7-2

Unpacking the Radio 7-2

Opening the Access Cover 7-3

Removing a Blank Spacer Card 7-4

Removing a 2.4-GHz Radio 7-5

Installing a 2.4-GHz Radio 7-7

Attaching the Compliance Labels 7-9

Placing the Labels 7-10

Finding the Software Version 7-10

CHAPTER 8 **5-GHz Radio Module Upgrade** 8-1

Upgrade Overview 8-2

Unpacking the Radio Module 8-2

Removing the 5-GHz Radio Access Cover 8-2

Removing a 5-GHz Radio Module 8-3

Installing a 5-GHz Radio Module 8-5

CHAPTER 9 **Troubleshooting** 9-1

Checking the Top Panel LEDs 9-2

Checking Basic Settings 9-4

SSID 9-4

WEP Keys 9-4

Security Settings 9-4

Resetting to the Default Configuration 9-4

Using the MODE Button 9-5

Using the Web Browser Interface 9-5

Reloading the Access Point Image 9-6

Using the MODE button 9-6

Web Browser Interface 9-7

Browser HTTP Interface 9-7

Browser TFTP Interface 9-7

Obtaining the Access Point Image File 9-8

Obtaining the TFTP Server Software 9-8

CISCO CONFIDENTIAL - Draft 2

APPENDIX A **Translated Safety Warnings** A-1
Dipole Antenna Installation Warning A-2
Explosive Device Proximity Warning A-3
Lightning Activity Warning A-4
Installation Warning A-5
Circuit Breaker (15A) Warning A-5

APPENDIX B **Declarations of Conformity and Regulatory Information** B-1
Manufacturers Federal Communication Commission Declaration of Conformity Statement B-2
Department of Communications—Canada B-3
Canadian Compliance Statement B-3
European Community, Switzerland, Norway, Iceland, and Liechtenstein B-4
Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC B-4
Declaration of Conformity for RF Exposure B-6
Guidelines for Operating Cisco Aironet Access Points in Japan B-6
Japanese Translation B-6
English Translation B-7
Administrative Rules for Cisco Aironet Access Points in Taiwan B-7
Access Points with IEEE 802.11a Radios B-7
Chinese Translation B-7
English Translation B-7
All Access Points B-8
Chinese Translation B-8
English Translation B-8
Declaration of Conformity Statements B-9
Declaration of Conformity Statements for European Union Countries B-9

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

APPENDIX D **Channels and Antenna Settings** D-1
Channels D-2
IEEE 802.11b (2.4-GHz Band) D-2
IEEE 802.11g (2.4-GHz Band) D-3
IEEE 802.11a (5-GHz Band) D-4

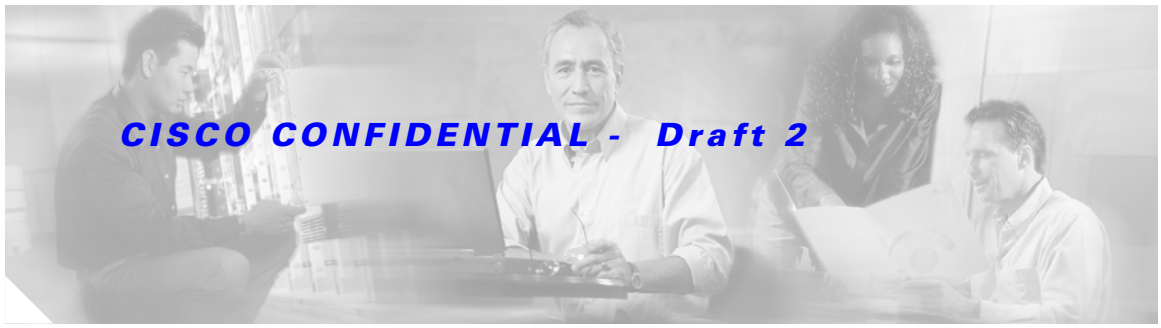
CISCO CONFIDENTIAL - Draft 2

Maximum Power Levels and Antenna Gains D-5
IEEE 802.11b (2.4-GHz Band) D-5
IEEE 802.11g (2.4-GHz Band) D-6
IEEE 802.11a (5-GHz Band) D-7

APPENDIX E
Console Cable Pinouts E-1
Overview E-2
Console Port Signals and Pinouts E-2

GLOSSARY

INDEX



Preface

Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1200 Series Access Point, hereafter referred to as the *access point*. To use this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

Purpose

This guide provides the information you need to install and configure basic settings for your access point. For information on using Cisco IOS commands to configure your access point, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. For detailed information about these IOS commands, refer to the *Cisco Aironet 1200 Series Access Point Command Reference* for this release. For information about the standard IOS Release 12.2 or 12.3 commands, refer to the IOS documentation set available from the Cisco.com home page at **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.2** or **Release 12.3** from the Cisco IOS Software drop-down menu.

This guide also includes an overview of the access point web-based interface (APWI) and the command line interface (CLI). This guide does not provide field-level descriptions of all APWI windows nor does it provide the procedures for completely configuring the access point using the APWI or the CLI. For all APWI window descriptions and procedures, refer to the access point online help, which is available from the Help buttons on the APWI pages. For configuration information refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

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 connect Ethernet and power cables and provides an installation summary, safety warnings, and general guidelines.

Chapter 3, "Configuring the Access Point for the First Time," describes how to configure basic settings on a new access point.

CISCO CONFIDENTIAL - Draft 2

Chapter 4, "Using the Web-Browser Interface," describes how to use the web-browser interface to configure the access point.

Chapter 5, "Using the Command-Line Interface," describes how to use the command-line interface (CLI) to configure the access point.

Chapter 6, "Mounting Instructions," describes how to mount the access point on a desktop, wall, or ceiling.

Chapter 7, "2.4-GHz Radio Upgrade," provides instructions for upgrading the access point 2.4-GHz radio.

Chapter 8, "5-GHz Radio Module Upgrade," provides instructions for upgrading the access point 5-GHz radio.

Chapter 9, "Troubleshooting," provides troubleshooting procedures for basic problems with the access point.

Appendix A, "Translated Safety Warnings," provides translations of the safety warnings that appear in this publication.

Appendix B, "Declarations of Conformity and Regulatory Information," provides declarations of conformity and regulatory information for the access point.

Appendix C, "Access Point Specifications," lists technical specifications for the access point.

Appendix D, "Channels and Antenna Settings," lists the 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.

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.

CISCO CONFIDENTIAL - Draft 2

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

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

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")**

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

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

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

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

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

CISCO CONFIDENTIAL - Draft 2

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

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. 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 complete information about the access point:

- *Release Notes for Cisco Aironet 1200 Series Access Point*
- *Cisco Aironet 1200 Series Access Point Command Reference*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*

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

http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm

To browse to the 1200 series access point documentation, select **Aironet 1200 Series Wireless LAN Products > Cisco Aironet 1200 Series Access Points**.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

CISCO CONFIDENTIAL - Draft 2

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

CISCO CONFIDENTIAL - Draft 2

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

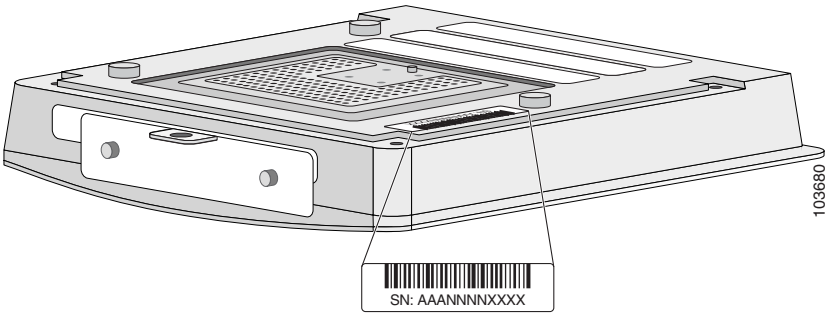
- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

CISCO CONFIDENTIAL - Draft 2

Locating the Product Serial Number

The access point serial number is located on the bottom of the cabinet (refer to Figure 1).

Figure 1 Location of Serial Number Label



The access point serial number label contains the following information:

- Model number, such as *AIR-AP1200*
- Serial number, such as S/N: *VDF0636XXXX* (11 alphanumeric digits)
- MAC address, such as MAC: *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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

CISCO CONFIDENTIAL - Draft 2

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Overview

Cisco Aironet 1200 Series Access Points provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, the 1200 series is a Wi-Fi certified, wireless LAN transceiver.

The 1200 series access point can contain two radios: a 2.4-GHz radio (IEEE 802.11b or IEEE 802.11g) in an internal mini-PCI slot and a 5-GHz radio module (IEEE 802.11a) in an external, modified cardbus slot. The access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios. You can configure the radios separately, using different settings on each radio.

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, uninterrupted 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).

This chapter provides information on the following topics:

- Hardware Features, page 1-2
- Network Configuration Examples, page 1-5

CISCO CONFIDENTIAL - Draft 2

Hardware Features

This section describes access point features. Refer to Appendix C, "Access Point Specifications," for a list of access point specifications.

Key hardware features of the 1200 series access point include:

- Dual-Radio Operation, page 1-2
- LEDs, page 1-3
- Ethernet Port, page 1-3
- Console Port, page 1-4
- Power Sources, page 1-4
- UL 2043 Certification, page 1-4
- Anti-Theft Features, page 1-4

Dual-Radio Operation

The 1200 series access point can be initially configured at the factory for single- or dual-radio operation. You can also upgrade an access point configured for single-radio operation to support dual-radio operation using a 5-GHz radio module or a 2.4-GHz mini-PCI radio card. The access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios.

The 2.4-GHz mini-PCI radio card connects to an internal mini-PCI slot and is available in two configurations:

- IEEE 802.11b mini-PCI radio card, hereafter called *802.11b radio*
- IEEE 802.11g mini-PCI radio card, herafter called *802.11g radio*
  - Requires Cisco IOS 12.2 (13)JA or later

The 5-GHz radio module connects to the access point's modified card bus connector and is available in three configurations:

- IEEE 802.11a radio module with integrated antenna (low power), hereafter called the *RM20A radio module*
- IEEE 802.11a radio module with integrated antenna, hereafter called the *RM21A radio module*
  - Requires Cisco IOS 12.3 (2)JA or later
- IEEE 802.11a radio module with external RP-TNC antenna connectors, hereafter called the *RM22A radio module*
  - Requires Cisco IOS 12.3 (2)JA or later

All 5-GHz radio modules incorporate an Unlicensed National Information Infrastructure (UNII) radio transceiver operating in the UNII 5-GHz frequency bands. The RM20A and the RM21A radio modules contain dual integrated omnidirectional antennas and directional antennas for diversity operation. The 802.11b or 802.11g radio is called *Radio0* and the 802.11a radio is called *Radio1*.

CISCO CONFIDENTIAL - Draft 2

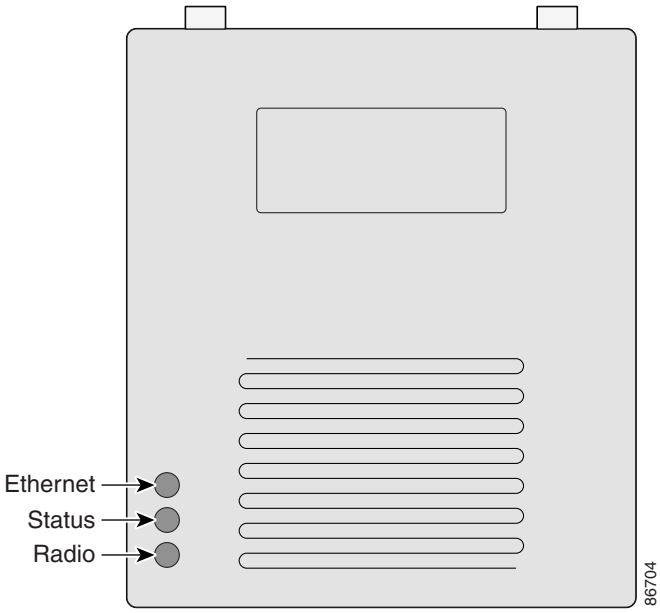
LEDs

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

- The Ethernet LED signals Ethernet traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED signals wireless traffic over the radio interface. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point radio.

Figure 1-1 shows the three status LEDs.

Figure 1-1 Access Point LEDs



Ethernet Port

The auto-sensing Ethernet port accepts an RJ-45 connector, linking the access point to your 10BASE-T or 100BASE-T Ethernet LAN. The access point can receive power through the Ethernet cable from a power injector, switch, or power patch panel. The Ethernet MAC address is printed on the label on the back of the access point.

CISCO CONFIDENTIAL - Draft 2

Console Port

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. (Refer to Appendix E, "Console Cable Pinouts," for a description of the console port pinouts.) 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.

Power Sources

The access point can receive power from an external power module or through inline power using the Ethernet cable. Using inline power, you do not need to run a power cord to the access point. The access point supports the following power sources:

- Power supply (input 100–240 VAC, 50–60 Hz, output 48 VDC, 0.2A minimum)
- Inline power from:
  - Cisco Aironet Power Injector for 1100 and 1200 series access points
  - A switch capable of providing inline power, such as Cisco Catalyst 3500XL, 3550, 4500, or 6500 switches
  - An inline power patch panel, such as the Cisco Catalyst Inline Power Patch Panel

Note The Catalyst 3550-24 PWR switch supports power for access points configured with both 2.4-GHz and 5-GHz radios. Other switches and patch panels might not provide enough power for both radios.

UL 2043 Certification

The access point is encased in a durable metal case having 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 Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space, all other power injectors and power modules are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

Anti-Theft Features

There are two methods of securing the access point to help prevent theft:

- Security cable keyhole—You can use the security cable slot to secure the access point using a standard security cable, such as those used on laptop computers.
- Security hasp—When you mount the access point on a wall or ceiling using the mounting bracket and the security hasp, you can lock the access point to the bracket with a padlock. Compatible padlocks are Master Lock models 120T and 121T or equivalent.

CISCO CONFIDENTIAL - Draft 2

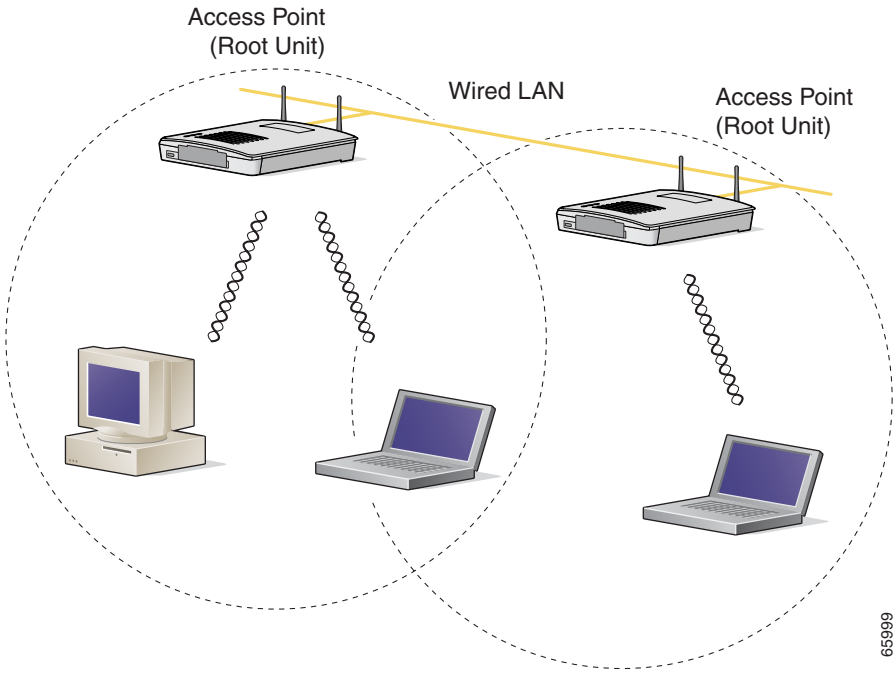
Network Configuration Examples

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. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-2 shows access points acting as root units on a wired LAN.

Figure 1-2 Access Points as Root Units on a Wired LAN



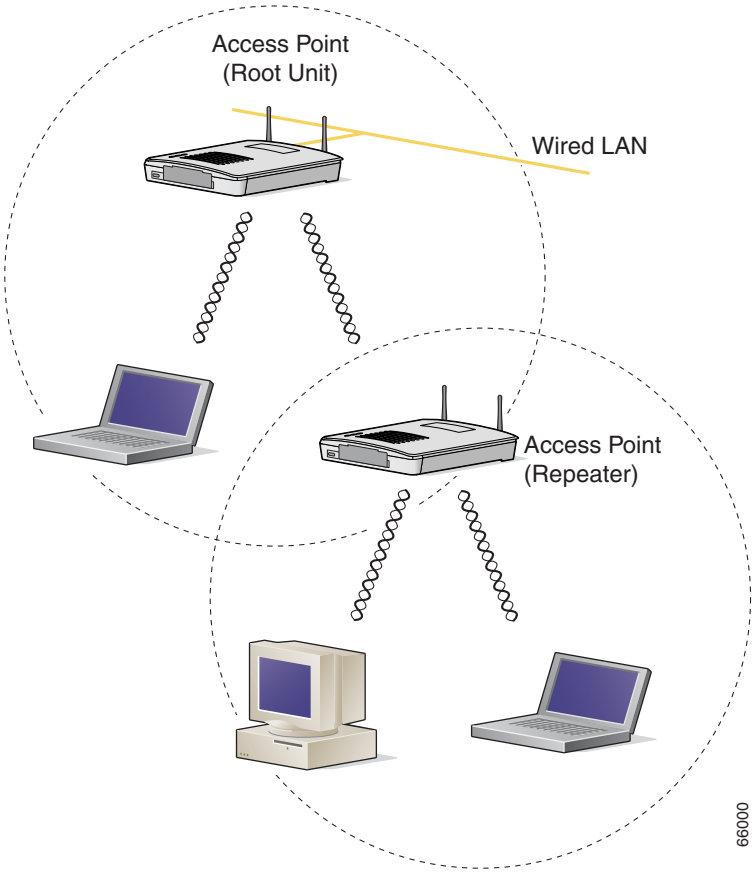
CISCO CONFIDENTIAL - Draft 2

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 1-3 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 an access point as a repeater.

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

Figure 1-3 Access Point as Repeater

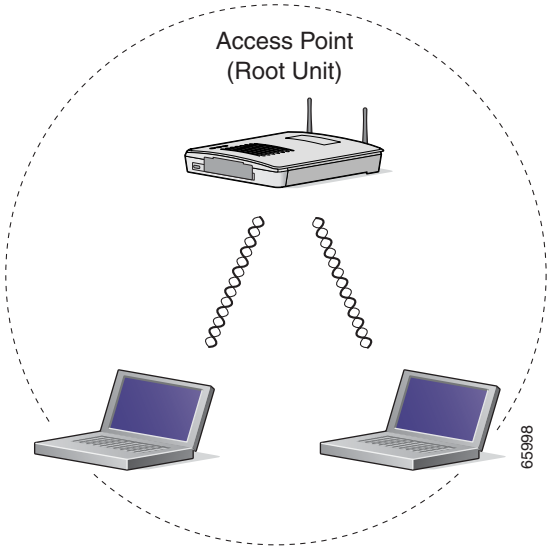


CISCO CONFIDENTIAL - Draft 2

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 1-4 shows an access point in an all-wireless network.

Figure 1-4 Access Point as Central Unit in All-Wireless Network



CISCO CONFIDENTIAL - Draft 2

Installing the Access Point

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

- Safety Information, page 2-2
- Warnings, page 2-2
- Unpacking the Access Point, page 2-3
- Basic Installation Guidelines, page 2-3
- Before Beginning the Installation, page 2-4
- Installation Summary, page 2-6
- Connecting the 2.4-GHz Antennas, page 2-6
- Connecting the Ethernet and Power Cables, page 2-8

CISCO CONFIDENTIAL - Draft 2

Safety Information

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

FCC Safety Compliance Statement

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

General Safety Guidelines

- Do not touch or move antenna(s) while the unit is transmitting or receiving.
- Do not hold any component containing a radio so that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the local codes, the national codes, and the safety directors of such environments.

Warnings

Translated versions of the following safety warnings are provided in Appendix A, "Translated Safety Warnings."

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:**
15A 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

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

CISCO CONFIDENTIAL - Draft 2

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 1200 Series Access Point
- Cisco Aironet 1200 Series Power Module (Universal power supply)
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- Cisco product registration and Cisco documentation feedback cards

The optional 2.4-GHz radio upgrade kit is shipped with the following items:

- 2.4-GHz radio card (802.11b or 802.11g)
- Installation guide
- A product registration card
- A T-10 tamper-resistant Torx L-wrench
- 2.4-GHz radio product compliance label

The optional 5-GHz radio upgrade kit is shipped with the following items:

- 5-GHz radio module (RM20A, RM21A, or RM22A)
- Installation guide
- A product registration card
- A T-10 tamper-resistant Torx L-wrench
- A 5-GHz radio product compliance label

If anything is missing or damaged, contact your Cisco representative for support.

Basic Installation Guidelines

Because the access point is a radio device, it is susceptible to common causes of 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 large steel structures such as shelving units, bookcases, and filing cabinets 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.

CISCO CONFIDENTIAL - Draft 2

Installation Above Suspended Ceilings

The access point uses a metal enclosure having 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. For mounting instructions, refer to the Chapter 6, "Mounting Instructions."

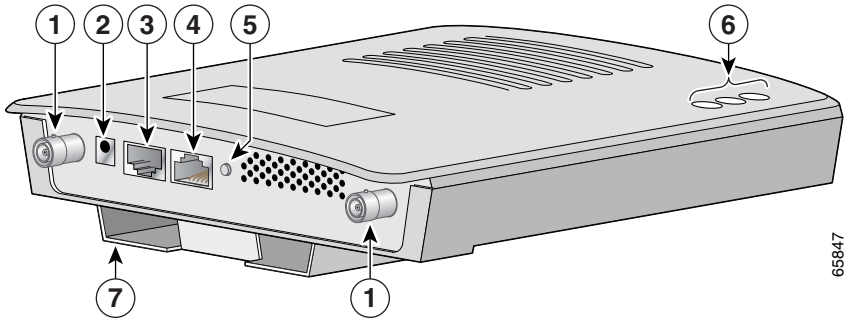
Caution Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space, all other power injectors and power modules are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

Note If you plan to mount the access point in environmental air space and will upgrade to a 5-GHz radio, Cisco recommends that you mount the access point horizontally with its antennas pointing down. Doing so will result in the access point complying with regulatory requirements for environmental air space after the 5-GHz radio is installed.

Before Beginning the Installation

Before you begin the installation process, please refer to Figure 2-1, Figure 2-2, and Figure 2-3 to become familiar with the access point's layout, connectors, and 5-GHz module location.

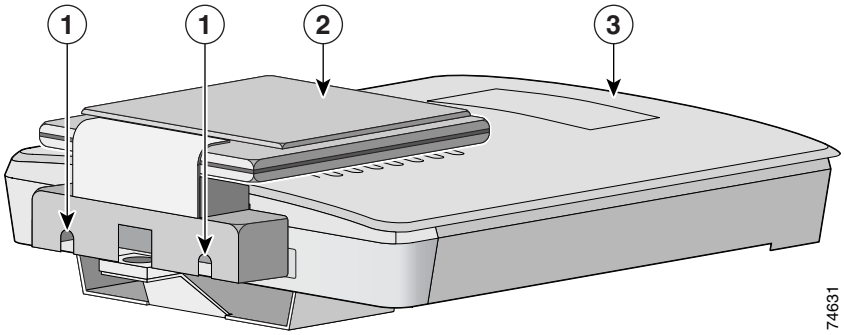
Figure 2-1 Access Point Layout and Connectors



1	2.4-GHz antenna connectors	**5**	Mode button
2	48-VDC power port	**6**	Status LEDs
3	Ethernet port (RJ-45)	**7**	Mounting bracket
4	Console port (RJ-45)		

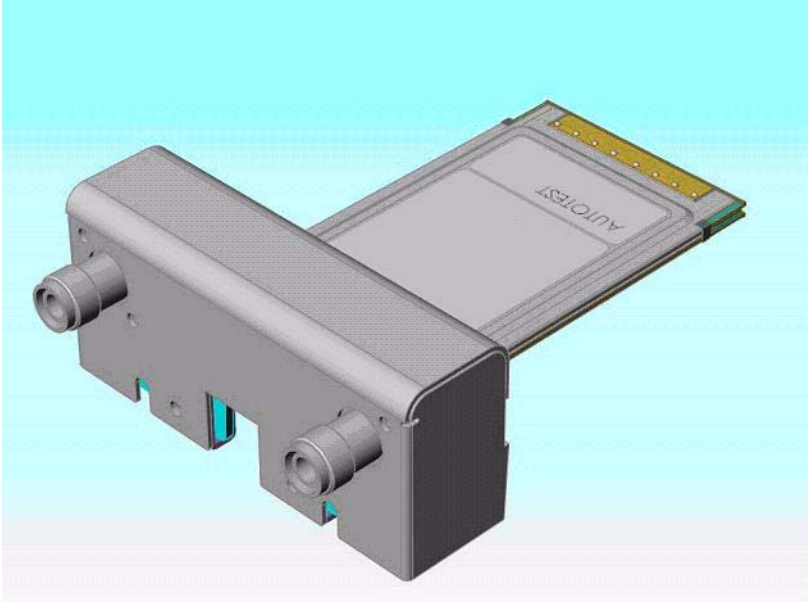
CISCO CONFIDENTIAL - Draft 2

Figure 2-2 Access Point with 5-GHz Radio Module (RM20A or RM21A)



1	Module mounting screws	**3**	Access point
2	Integrated antenna in patch position (RM20A or RM21A radio module)		

Figure 2-3 RM22A Radio Module with External RP-TNC Antenna Connectors



1	Module mounting screws	**3**	5-GHz radio
2	5-GHz antenna connectors (RP-TNC)		

CISCO CONFIDENTIAL - Draft 2

Installation Summary

While installing the access point, you must perform the following operations:

- If you have a 2.4-GHz radio upgrade kit, refer to the "2.4-GHz Radio Upgrade" section on page 7-1.
- If you have a 5-GHz radio module upgrade kit (RM20A, RM21A,or RM22A) refer to the *"5-GHz Radio Module Upgrade" section on page 8-1*.
- If your access point has a built-in 2.4-GHz radio, connect a single antenna or dual diversity antennas (refer to the "Connecting the 2.4-GHz Antennas" section on page 2-6*)*.
- If your access point has an installed RM22A radio module, connect a single antenna or dual diversity antennas (refer to the "Connecting the 5-GHz External Antennas" section on page 2-7*)*.
- Connect Ethernet and power cables (refer to the "Connecting the Ethernet and Power Cables" section on page 2-8).
- Configure basic settings (refer to Chapter 3, "Configuring the Access Point for the First Time").
- Configure security and other access point options.
- Use the mounting kit to install the access point on a convenient flat horizontal or vertical surface, such as a desktop, book shelf, file cabinet, wall, or ceiling. For additional information on mounting, refer to Chapter 6, "Mounting Instructions."

Connecting the 2.4-GHz Antennas

The access point supports a single antenna or dual diversity antennas. Two RPTNC antenna connectors are provided on the back of the unit for the 2.4-GHz radio.

Note RPTNC antenna connectors are used for both the 2.4 GHz and 5 GHz radios. You must be careful to ensure that you connect your 2-4 GHz antenna to the 2-4 GHz radio connectors (refer to Figure 2-1 for connector locations).

To attach your antenna or antenna cable to the access point, follow these steps:

Step 1 Attach an antenna or antenna cable to the **2.4-GHz Right/Primary** (RPTNC) antenna connector on the back of the access point and hand tighten. If you are using two antennas for diversity coverage, attach the second antenna or antenna cable to the **2.4-GHz Left** (RPTNC) antenna connector.

Step 2 If you are using a Cisco Aironet 2 dBi antenna, orient the antenna depending on how you intend to mount the access point.

- On a table or desk, orient the antenna straight up.
- On a vertical surface, such as a wall, orient the antenna straight up.
- On a ceiling, orient the antenna straight down.

Step 3 If you are using another Cisco Aironet antenna, refer to the antenna mounting instructions that came with your antenna.

CISCO CONFIDENTIAL - Draft 2

Connecting the 5-GHz External Antennas

The access point supports an RM22A radio module for use with a single antenna or dual diversity antennas. Two RPTNC antenna connectors are provided on the back of the module for the 5-GHz radio.

Note RPTNC antenna connectors are used for both the 2.4 GHz and 5 GHz radios. You must be careful to ensure that you connect your 5 GHz antenna to the 5 GHz radio connectors (refer to Figure 2-3 for connector locations).

If you are using the RM22A radio module, follow these steps below:

Step 1 Attach the Cisco Aironet 5-GHz antenna cable to the **Right/Primary** 5-GHz (RPTNC) antenna connector on the back of the radio module and hand tighten. If you are using two antennas for diversity coverage, attach the second antenna cable to the **Left** 5-GHz (RPTNC) antenna connector.

Note The Cisco Aironet antenna cables have a blue marker label near the antenna connector and the radio module has a corresponding blue label near the 5-GHz antenna connectors.

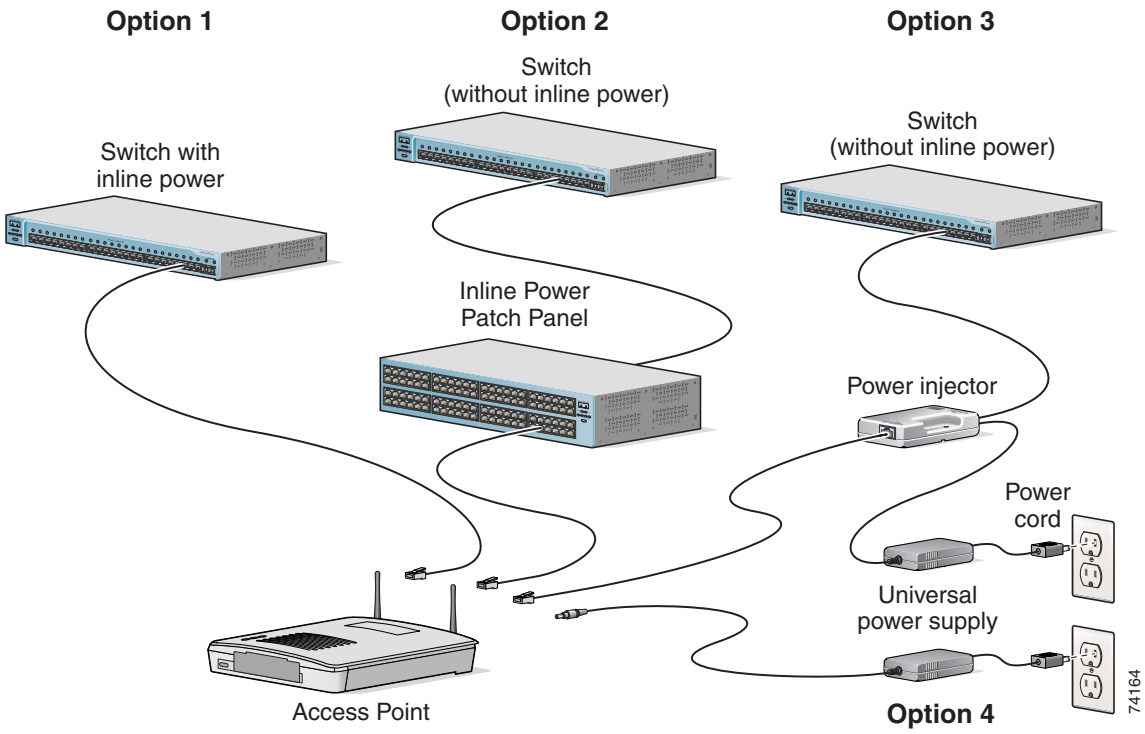
Step 2 To mount your Cisco Aironet antenna, refer to the instructions that came with your antenna.

CISCO CONFIDENTIAL - Draft 2

Connecting the Ethernet and Power Cables

The access point receives power through the Ethernet cable or an external power module. Figure 2-4 shows the power options for the access point.

Figure 2-4 Access Point Power Options



The access point power options are listed below:

- A switch with inline power, such as a Cisco Catalyst 3500XL, 3550-24 PWR, 4000, or 6500 switch
- An inline power patch panel, such as a Cisco Catalyst Inline Power Patch Panel
- A power injector
- A power module (Universal power supply)

Note Currently, the Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

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

CISCO CONFIDENTIAL - Draft 2

Connecting to an Ethernet Network with an Inline Power Source

Caution The Cisco Aironet Power Injector for the 1100 and 1200 series is designed for use with 1100 series or 1200 series access points only. Using the power injector with other Ethernet-ready devices can damage the equipment.

Caution The Cisco Aironet Power Injector for the 1100 and 1200 series is not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

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

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

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

- A switch with inline power, such as a Cisco Catalyst 3500XL, 3550-24 PWR, 4000, or 6500 switch.
- An inline power switch panel, such as a Cisco Catalyst Inline Power Patch Panel.
- The end of a Cisco Aironet power injector labeled *To AP/Bridge*. Connect the other end labeled *To Network* to the 10/100 Ethernet LAN.

Note If you use a power supply or power injector to power the access point, you must use the power supply included with your access point and the Cisco Aironet Power Injector for the 1100 and 1200 series access points.

Connecting to an Ethernet Network with Local Power

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

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

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

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

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

CISCO CONFIDENTIAL - Draft 2

Powering Up the Access Point

When power is applied to the access point, it begins a routine power-up sequence that you can monitor by observing the three LEDs on top of the access point. After you observe all three LEDs turning green to indicate the starting of the IOS operating system, the Status LED blinks green signifying that IOS is operational. When in an operational status, the Ethernet LED is steady green when no traffic is being passed and dark during periods when traffic is being passed. The sequence takes about 1 minute to complete. Refer to Chapter 9, "Troubleshooting," 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 Chapter 3, "Configuring the Access Point for the First Time," for instructions on assigning basic settings to the access point.

Configuring the Access Point for the First Time

This chapter describes how to configure basic settings on your access point for the first time. The contents of this chapter are similar to the instructions in the quick start guide that shipped with your access point. You can configure all the settings described in this chapter using the CLI, but it might be simplest to browse to the access point's web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

This chapter contains these sections:

- Before You Start, page 3-2
- Obtaining and Assigning an IP Address, page 3-3
- Connecting to the Access Point Locally, page 3-3
- Assigning Basic Settings, page 3-4
- Protecting Your Wireless LAN, page 3-8
- Using the IP Setup Utility, page 3-9
- Assigning an IP Address Using the CLI, page 3-12
- Using a Telnet Session to Access the CLI, page 3-12

CISCO CONFIDENTIAL - Draft 2

Before You Start

Before you install the access point, make sure you are using a computer connected to the same network as the access point, and obtain the following information from your network administrator:

- A system name for the access point
- The case-sensitive wireless service set identifier (SSID) for your radio network
- If not connected to a DHCP server, a unique IP address for your access point (such as 172.17.255.115)
- If the access point is not on the same subnet as your PC, a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)
- If you use IPSU to find or assign the access point IP address, the MAC address from the label on the bottom of the access point (such as 00164625854c)

Resetting the Access Point to Default Settings

If you need to start over during the initial setup process, follow these steps to reset the access point to factory default settings using the access point MODE button:

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

Step 2 Press and hold the MODE button while you reconnect power to the access 2 to 3 seconds), and release the button. All access point settings return to factory defaults.

Follow these steps to return to default settings using the web-browser interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

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

Step 3 Enter your username in the User Name field. The default username is **Cisco**.

Step 4 Enter the access point password in the Password field and press **Enter**. The default password is **Cisco**. The Summary Status page appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

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.

CISCO CONFIDENTIAL - Draft 2

Obtaining and Assigning an IP Address

To browse to the access point's Express Setup page, you must either obtain or assign the access point's IP address using one of the following methods:

- Connect to the access point console port and assign a static IP address. Follow the steps in the "Connecting to the Access Point Locally" section on page 3-3 to connect to the console port.
- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address using one of the following methods:
  - Connect to the access point console port and use the **show ip interface brief** command to display the IP address. Follow the steps in the "Connecting to the Access Point Locally" section on page 3-3 to connect to the console port.
  - Provide your organization's network administrator with your access point's Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The access point's MAC address is on label attached to the bottom of the access point.
  - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. You can also use IPSU to assign an IP address to the access point if it did not receive an IP address from the DHCP server. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, Me, NT, and XP.

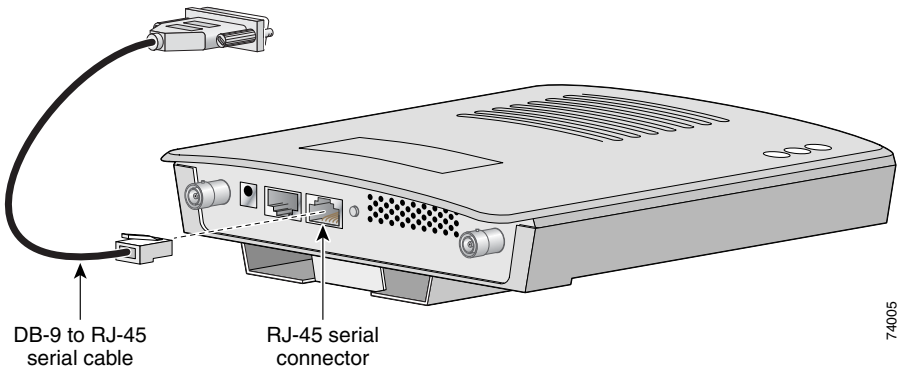
    For information on IPSU, refer to "Using the IP Setup Utility" section on page 3-9.

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. 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 serial port on the access point and to the COM port on a computer. Figure 3-1 shows the serial port connection.

Figure 3-1 Connecting the Serial Cable



CISCO CONFIDENTIAL - Draft 2

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 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.

Assigning Basic Settings

After you determine or assign the access point's IP address, you can browse to the access point's Express Setup page and perform an initial configuration:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

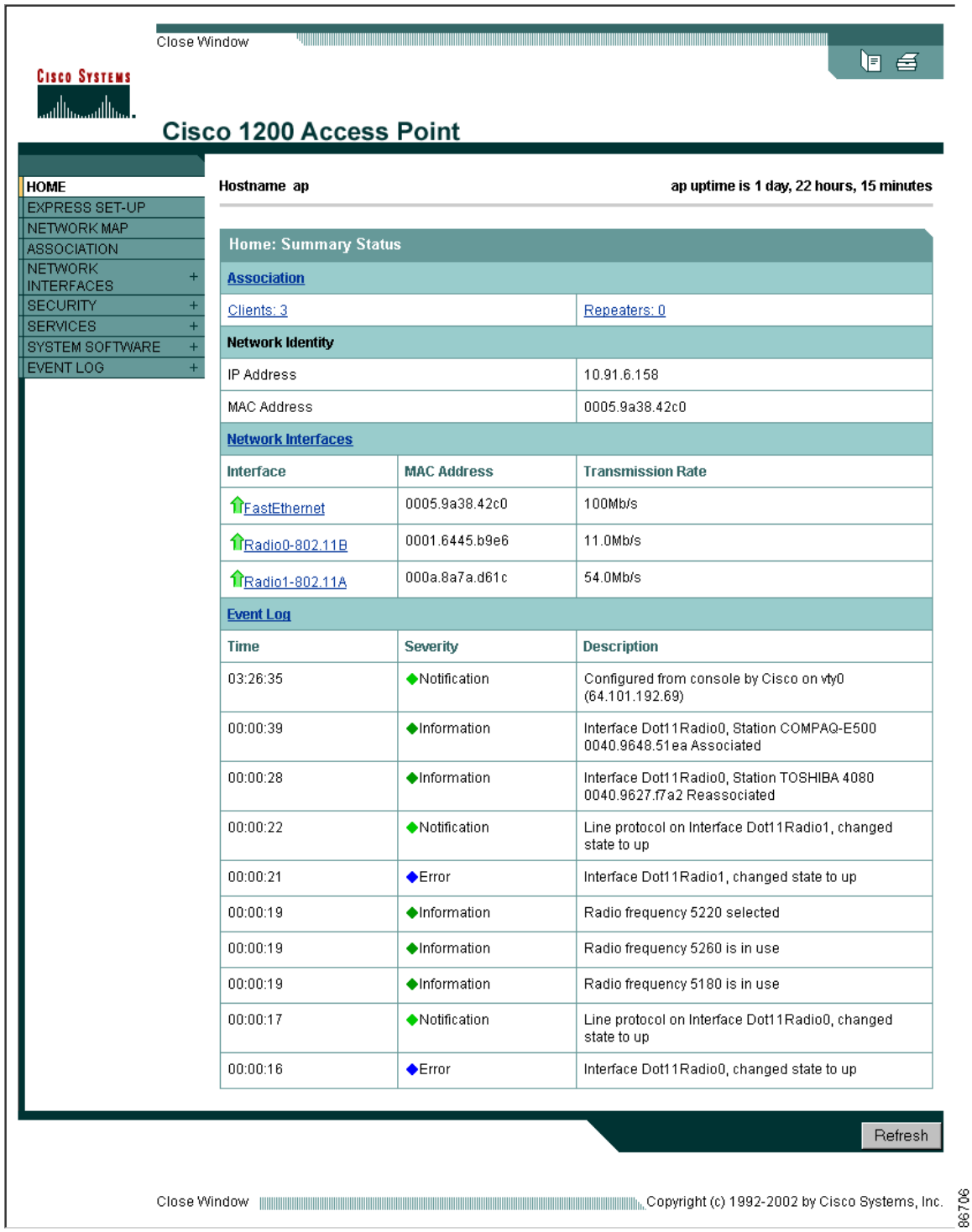
Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Press **Tab** to bypass the Username field and advance to the Password field.

Step 4 Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears. Figure 3-2 shows the Summary Status page.

CISCO CONFIDENTIAL - Draft 2

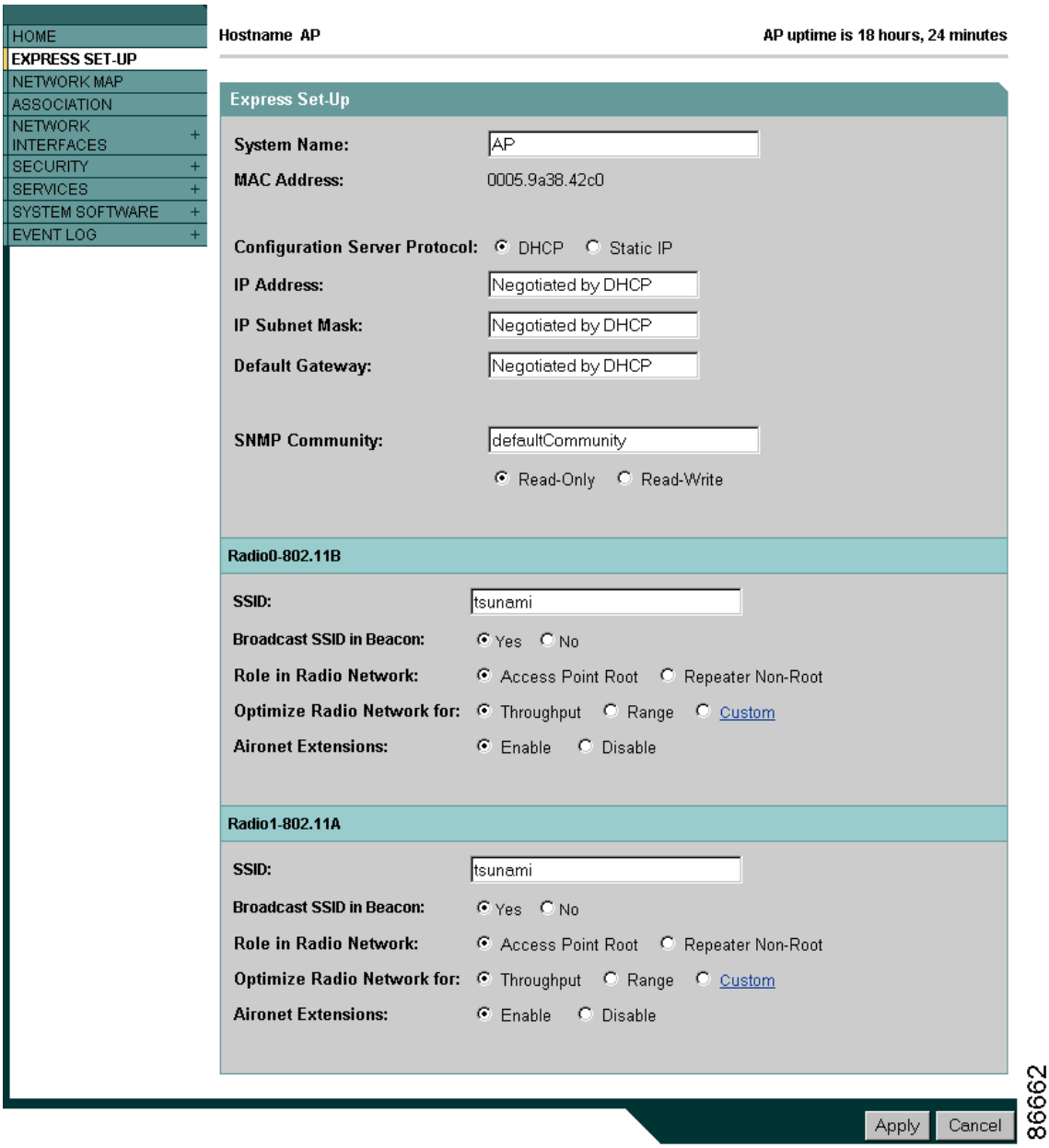
Figure 3-2 Summary Status Page



Step 5 Click **Express Setup**. The Express Setup screen appears. Figure 3-3 shows the Express Setup page.

CISCO CONFIDENTIAL - Draft 2

Figure 3-3 Express Setup Page



Step 6 Enter the configuration settings you obtained from your system administrator. The configurable settings include:

- **System Name**— The system name, while not an essential setting, helps identify the access point on your network. The system name appears in the titles of the management system pages.
- **Configuration Server Protocol**—Click on the button that matches the network's method of IP address assignment.
  - **DHCP**—IP addresses are automatically assigned by your network's DHCP server.
  - **Static IP**—The access point uses a static IP address that you enter in the IP address field.

CISCO CONFIDENTIAL - Draft 2

- **IP Address**—Use this setting to assign or change the access point's IP address. If DHCP is enabled for your network, leave this field blank.

Note If the access point's IP address changes while you are configuring the access point using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the access point. If you lose your connection, reconnect to the access point using its new IP address. Follow the steps in the "Resetting the Access Point to Default Settings" section on page 3-2 if you need to start over.

- **IP Subnet Mask**—Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. If DHCP is enabled, leave this field blank.
- **Default Gateway**—Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
- **Radio Service Set ID (SSID)**—Enter the case-sensitive SSID (32 alphanumeric characters maximum) provided by your network administrator. The SSID is a unique identifier that client devices use to associate with the access point.
- **Broadcast SSID in Beacon**—Use this setting to allow devices that do not specify an SSID to associate with the access point.
  - **Yes**—This is the default setting; it allows devices that do not specify an SSID to associate with the access point.
  - **No**—Devices must specify an SSID to associate with the access point. With No selected, the SSID used by the client devices must match exactly the access point's SSID.
- **Role in Radio Network**—Click on the button that describes the role of the access point on your network. Select **Access Point (Root)** if your access point is connected to the wired LAN. Select **Repeater (Non-Root)** if it is not connected to the wired LAN.
- **Optimize Radio Network for**—Use this setting to select either preconcerted settings for the access point radio or customized settings for the access point radio.
  - **Throughput**—Maximizes the data volume handled by the access point but might reduce its range.
  - **Range**—Maximizes the access point's range but might reduce throughput.
  - **Custom**—The access point uses settings you enter on the Network Interfaces: Radio-802.11b Settings page. Clicking **Custom** takes you to the Network Interfaces: Radio-802.11b Settings page.
- **Aironet Extensions**—Enable this setting if there are only Cisco Aironet devices on your wireless LAN.
- **SNMP Community**—If your network is using SNMP, enter the SNMP Community name provided by your network administrator and select the attributes of the SNMP data (also provided by your network administrator).

Step 7 Click **Apply** to save your settings. If you changed the IP address, you lose your connection to the access point. Browse to the new IP address to reconnect to the access point.

Your access point is now running but probably requires additional configuring to conform to your network's operational and security requirements. Consult the chapters in this manual for the information you need to complete the configuration.

CISCO CONFIDENTIAL - Draft 2

Note You can restore the access point to its factory defaults by unplugging the power jack and plugging it back in while holding down the Mode button for a few seconds, or until the Status LED turns amber.

Default Settings on the Express Setup Page

Table 3-1 lists the default settings for the settings on the Express Setup page.

Table 3-1 Default Settings on the Express Setup Page

Setting	Default
System Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default; if DHCP is disabled, the default setting is 10.0.0.1
IP Subnet Mask	Assigned by DHCP by default; if DHCP is disabled, the default setting is 255.255.255.224
Default Gateway	Assigned by DHCP by default; if DHCP is disabled, the default setting is 0.0.0.0
Radio Service Set ID (SSID)	tsunami
Broadcast SSID in Beacon	Yes[1]
Role in Radio Network	Access point (root)
Optimize Radio Network for	Throughput
Aironet Extensions	Enable
SNMP Community	defaultCommunity

1. When you assign multiple SSIDs, this setting no longer appears.

Protecting Your Wireless LAN

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your building. Configure some combination of these security features to protect your network from intruders:

- Unique SSIDs that are not broadcast in the access point beacon (see *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*)
- WEP and additional WEP features, such as TKIP and broadcast key rotation (see *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points)*

CISCO CONFIDENTIAL - Draft 2

- Dynamic WEP and client authentication (see *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*)

Using the IP Setup Utility

IPSU enables you to find the access point's IP address when it has been assigned by a DHCP server. You can also use IPSU to set the access point's IP address and SSID if they have not been changed from the default settings. This section explains how to install the utility, how to use it to find the access point's IP address, and how to use it to set the IP address and the SSID.

Note IPSU can be used only on the following operating systems: Windows 95, 98, NT, 2000, ME, or XP.

Tip Another simple way to find the access point's IP address is to look on the Status screen in the Aironet Client Utility on a client device associated to the access point.

Obtaining and Installing IPSU

IPSU is available on the Cisco web site. Follow these steps to obtain and install IPSU:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

Step 2 Click **Option 2: Aironet Wireless Software Display Tables**.

Step 3 Locate the access point firmware and utilities section and click **Cisco Aironet 1200 Series (Cisco IOS Software)**.

Step 4 Click **IPSUvxxxxxx.exe**. The *vxxxxxx* identifies the software package version number.

Step 5 On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply.

Step 6 Click **Submit**.

Step 7 Read and accept the terms and conditions of the Software License Agreement.

Step 8 Select the file again to download it.

Step 9 Download and save the file to a temporary directory on your hard drive and then exit the Internet browser.

Step 10 Double-click **IPSUvxxxxxx.exe** in the temporary directory to expand the file.

Step 11 Double-click **Setup.exe** and follow the steps provided by the installation wizard to install IPSU.

The IPSU icon appears on your computer desktop.

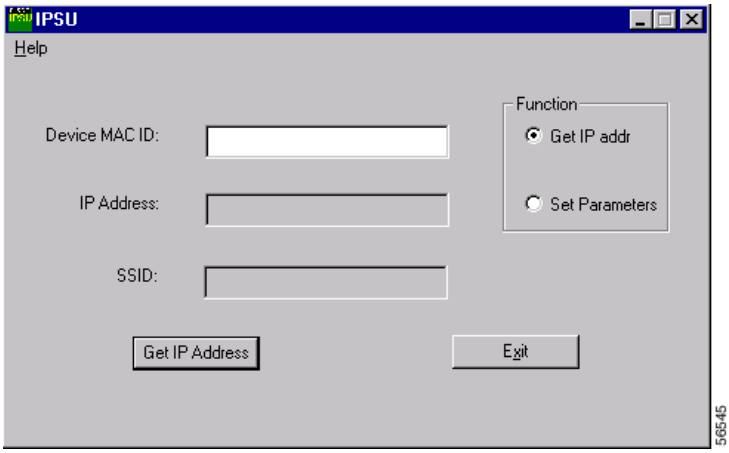
CISCO CONFIDENTIAL - Draft 2

Using IPSU to Find the Access Point's IP Address

If your access point receives an IP address from a DHCP server, you can use IPSU to find its IP address. Because IPSU sends a reverse-ARP request based on the access point MAC address, you must run IPSU from a computer on the same subnet as the access point. Follow these steps to find the access point's IP address:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see Figure 3-4).

Figure 3-4 IPSU Get IP Address Screen



Step 2 When the utility window opens, make sure the *Get IP addr* radio button in the Function box is selected.

Step 3 Enter the access point's MAC address in the Device MAC ID field. The access point's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point's MAC address might look like the following example:

000164xxxxxx

Note The MAC address field is not case-sensitive.

Step 4 Click **Get IP Address**.

Step 5 When the access point's IP address appears in the IP Address field, write it down.

If IPSU reports that the IP address is 10.0.0.1, the default IP address, then the access point did not receive a DHCP-assigned IP address. To change the access point IP address from the default value using IPSU, refer to the "Using IPSU to Set the Access Point's IP Address and SSID" section on page 3-11.

CISCO CONFIDENTIAL - Draft 2

Using IPSU to Set the Access Point's IP Address and SSID

If you want to change the default IP address (10.0.0.1) of the access point, you can use IPSU. You can also set the access point's SSID at the same time.

Note IPSU can change the access point's IP address and SSID only from their default settings. After the IP address and SSID have been changed, IPSU cannot change them again.

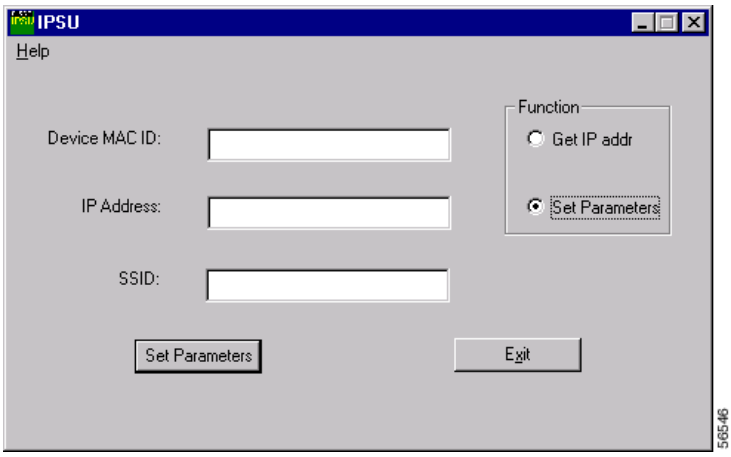
Note The computer you use to assign an IP address to the access point must have an IP address in the same subnet as the access point (10.0.0.x).

Follow these steps to assign an IP address and an SSID to the access point:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility.

Step 2 Click the **Set Parameters** radio button in the Function box (see Figure 3-5).

Figure 3-5 IPSU Set Parameters Screen



Step 3 Enter the access point's MAC address in the Device MAC ID field. The access point's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point's MAC address might look like this example:

004096xxxxxx

Note The MAC address field is not case-sensitive.

Step 4 Enter the IP address you want to assign to the access point in the IP Address field.

Step 5 Enter the SSID you want to assign to the access point in the SSID field.

Note You cannot set the SSID without also setting the IP address. However, you can set the IP address without setting the SSID.

CISCO CONFIDENTIAL - Draft 2

Step 6 Click **Set Parameters** to change the access point's IP address and SSID settings.

Step 7 Click **Exit** to exit IPSU.

Assigning an IP Address Using the CLI

When you connect the access point to the wired LAN, the access point links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the access point's Ethernet and radio ports, the network uses the BVI.

When you assign an IP address to the access point using the CLI, you must assign the address to the BVI. Beginning in privileged EXEC mode, follow these steps to assign an IP address to the access point's BVI:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface bvi1**	Enter interface configuration mode for the BVI.
Step 3	**ip address** *address mask*	Assign an IP address and address mask to the BVI. **Note** If you are connected to the access point using a Telnet session, you lose your connection to the access point when you assign a new IP address to the BVI. If you need to continue configuring the access point using Telnet, use the new IP address to open another Telnet session to the access point.

Using a Telnet Session to Access the CLI

Follow these steps to browse to access the CLI using a Telnet session. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.

Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point's IP address.

Step 3 In the Host Name field, type the access point's IP address and click **Connect**.

Using the Web-Browser Interface

This chapter describes the web-browser interface that you can use to configure the access point. It contains these sections:

- Using the Web-Browser Interface for the First Time, page 4-2
- Using the Management Pages in the Web-Browser Interface, page 4-2
- Using Online Help, page 4-5

The web-browser interface contains management pages that you use to change access point settings, upgrade firmware, and monitor and configure other wireless devices on the network.

Note The access point web-browser interface is fully compatible with Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

CISCO CONFIDENTIAL - Draft 2

Using the Web-Browser Interface for the First Time

Use the access point's IP address to browse to the management system. See the "Obtaining and Assigning an IP Address" section on page 3-3 for instructions on assigning an IP address to the access point.

Follow these steps to begin using the web-browser interface:

Step 1 Start the browser.

Step 2 Enter the access point's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**. The Summary Status page appears.

Using the Management Pages in the Web-Browser Interface

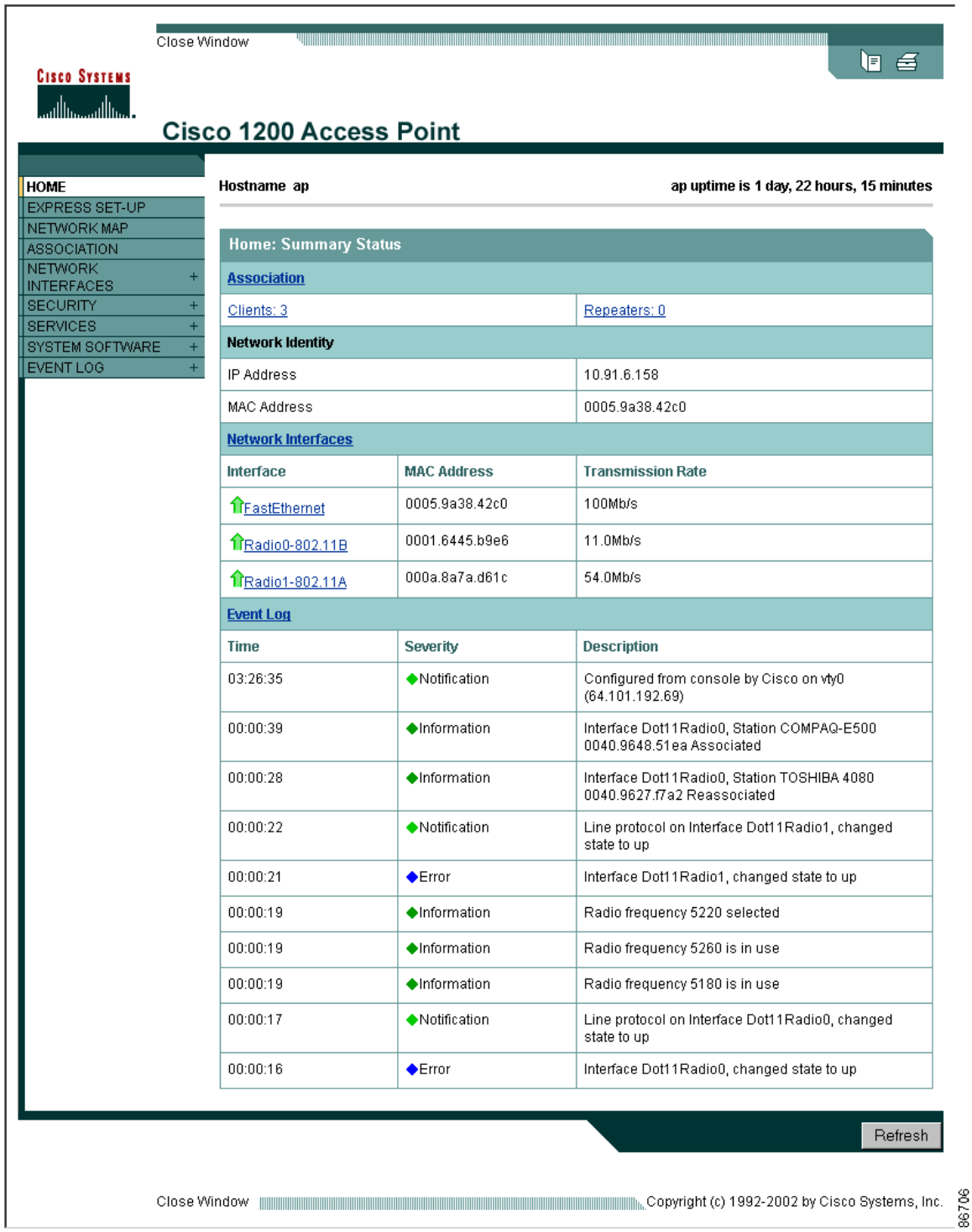
The system management pages use consistent techniques to present and save configuration information. A navigation bar is on the left side of the page, and configuration action buttons appear at the bottom. You use the navigation bar to browse to other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

Note Changes are applied only when you click **Apply**. It's important to remember that clicking your browser's **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made on the page and keeps you on that page.

Figure 4-1 shows the web-browser interface home page.

CISCO CONFIDENTIAL - Draft 2

Figure 4-1 Web-Browser Interface Home Page



CISCO CONFIDENTIAL - Draft 2

Using Action Buttons

Table 4-1 lists the page links and buttons that appear on most management pages.

Table 4-1 Common Buttons on Management Pages

Button/Link	Description
Navigation Links	
Home	Displays access point status page with information on the number of radio devices associated to the access point, the status of the Ethernet and radio interfaces, and a list of recent access point activity.
Express Setup	Displays the Express Setup page that includes basic settings such as system name, IP address, and SSID.
Network Map	Displays a list of infrastructure devices on your wireless LAN.
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.
Network Interfaces	Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.
Security	Displays a summary of security settings and provides links to security configuration pages.
Services	Displays status for several access point features and links to configuration pages for Telnet/SSH, CDP, domain name server, filters, proxy Mobile IP, QoS, SNMP, SNTP, and VLANs.
System Software	Displays the version number of the firmware that the access point is running and provides links to configuration pages for upgrading and managing firmware.
Event Log	Displays the access point event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.
Configuration Action Buttons	
Apply	Saves changes made on the page and remains on the page.
Refresh	Updates status information or statistics displayed on a page.
Cancel	Discards changes to the page and remains on the page.
Back	Discards any changes made to the page and returns to the previous page.

CISCO CONFIDENTIAL - Draft 2

Character Restrictions in Entry Fields

Because the 1200 series access point uses Cisco IOS software, there are certain characters that you cannot use in the entry fields on the web-browser interface. Table 4-2 lists the prohibited characters and the fields in which you cannot use them.

Table 4-2 Prohibited Characters for Web-Browser Interface Entry Fields

Entry Field Type	Prohibited Characters
Password entry fields	**?** **“** **$** **[** **+**
All other entry fields	**?** **“** **$** **[** **+** You also cannot use these three characters as the first character in an entry field: **!** **#** **;**

Using Online Help

Click the help icon at the top of any page in the web-browser interface to display online help. Figure 4-2 shows the print and help icons.

Figure 4-2 Print and Help Icons

When a help page appears in a new browser window, use the Select a topic drop-down menu to display the help index or instructions for common configuration tasks, such as configuring VLANs.

CISCO CONFIDENTIAL - Draft 2

Using the Command-Line Interface

This chapter describes the IOS command-line interface (CLI) that you can use to configure your access point. It contains these sections:

- IOS Command Modes, page 5-2
- Getting Help, page 5-3
- Abbreviating Commands, page 5-3
- Using no and default Forms of Commands, page 5-3
- Understanding CLI Messages, page 5-4
- Using Command History, page 5-4
- Using Editing Features, page 5-5
- Searching and Filtering Output of show and more Commands, page 5-8
- Accessing the CLI, page 5-8

CISCO CONFIDENTIAL - Draft 2

IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the access point, you begin in user mode, often called *user EXEC mode*. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the access point reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you must enter privileged EXEC mode before you can enter the global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the access point reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 5-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *ap*.

Table 5-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your access point.	`ap>`	Enter **logout** or **quit**.	Use this mode to: • Change terminal settings • Perform basic tests • Display system information
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`ap#`	Enter **disable** to exit.	Use this mode to verify commands. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`ap(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire access point.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`ap(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet and radio interfaces. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

CISCO CONFIDENTIAL - Draft 2

Getting Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in Table 5-2.

Table 5-2 Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

*abbreviated-command-entry***?**	Obtains a list of commands that begin with a particular character string.
	For example:
	`ap# di?`
	`dir disable disconnect`

*abbreviated-command-entry***<Tab>**	Completes a partial command name.
	For example:
	`ap# sh conf<tab>`
	`ap# show configuration`

?	Lists all commands available for a particular command mode. For example: `ap> ?`
command **?**	Lists the associated keywords for a command. For example: `ap> show ?`

command keyword **?**	Lists the associated arguments for a keyword.
	For example:
	`ap(config)# cdp holdtime ?`
	`  <10-255>  Length of time (in sec) that receiver must keep this packet`

Abbreviating Commands

You have to enter only enough characters for the access point to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command:

```
ap# show conf
```

Using no and default Forms of Commands

Most configuration commands also have a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

CISCO CONFIDENTIAL - Draft 2

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Understanding CLI Messages

Table 5-3 lists some error messages that you might encounter while using the CLI to configure your access point.

Table 5-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your access point to recognize the command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (**?**) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Using Command History

The IOS provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs as described in these sections:

- Changing the Command History Buffer Size, page 5-4
- Recalling Commands, page 5-5
- Disabling the Command History Feature, page 5-5

Changing the Command History Buffer Size

By default, the access point records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the access point records during the current terminal session:

ap# **terminal history** [**size** *number-of-lines*]

CISCO CONFIDENTIAL - Draft 2

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the access point records for all sessions on a particular line:

```
ap(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 5-4:

Table 5-4 Recalling Commands

Action[1]	Result
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the **terminal history** global configuration command and **history** line configuration command.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line. It contains these sections:

- Enabling and Disabling Editing Features, page 5-6
- Editing Commands Through Keystrokes, page 5-6
- Editing Command Lines that Wrap, page 5-7

CISCO CONFIDENTIAL - Draft 2

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
ap# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# no editing
```

Editing Commands Through Keystrokes

Table 5-5 shows the keystrokes that you need to edit command lines.

Table 5-5 Editing Commands Through Keystrokes

Capability	Keystroke[1]	Purpose
Move around the command line to make changes or corrections.	**Ctrl-B** or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The access point provides a buffer with the last ten items that you deleted.	**Ctrl-Y**	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	**Delete** or **Backspace**	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.

CISCO CONFIDENTIAL - Draft 2

Table 5-5 Editing Commands Through Keystrokes (continued)

Capability	Keystroke[1]	Purpose
Capitalize or lowercase words or capitalize a set of letters.	**Esc C**	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	**Ctrl-V** or **Esc Q**	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The `More` prompt appears for output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the `More` prompt.	**Return**	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the access point suddenly sends a message to your screen.	**Ctrl-L** or **Ctrl-R**	Redisplay the current command line.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
ap(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
ap(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
ap(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

CISCO CONFIDENTIAL - Draft 2

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the "Editing Commands Through Keystrokes" section on page 5-6.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command **|** {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Accessing the CLI

You can open the access point's CLI using Telnet or Secure Shell (SSH).

Opening the CLI with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.

CISCO CONFIDENTIAL - Draft 2

Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the access point's IP address.

Step 3 In the Host Name field, type the access point's IP address and click **Connect**.

Step 4 At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.

Opening the CLI with Secure Shell

Secure Shell Protocol is a protocol that provides a secure, remote connection to networking devices set up to use it. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. See the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for detailed instructions on setting up the access point for SSH access.

CISCO CONFIDENTIAL - Draft 2

Mounting Instructions

This appendix provides instructions for mounting the access point to suspended ceilings, vertical surfaces, or horizontal surfaces using the access point mounting bracket.

The following sections are included in this chapter:

- Overview, page 6-2
- Mounting on a Horizontal or Vertical Surface, page 6-3
- Mounting Below a Suspended Ceiling, page 6-4
- Mounting Above a Suspended Ceiling, page 6-5
- Attaching the Access Point to the Mounting Bracket, page 6-7
- Securing the Access Point to the Mounting Bracket, page 6-7

CISCO CONFIDENTIAL - Draft 2

Overview

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

- Horizontal or vertical flat surfaces, such as walls or ceilings
- Suspended ceilings

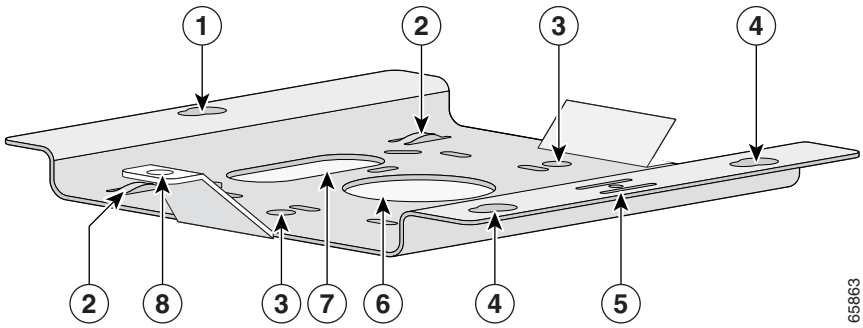
The access point ships with a detachable mounting bracket and the necessary mounting hardware. Because it is detachable, you can use the mounting bracket as a template to mark the positions of the mounting holes for your installation. You then install the mounting bracket and attach the access point when you are ready. Refer to Figure 6-1 to locate the various mounting holes for the method you intend to use.

Note The Cisco Aironet 1200 Series Access Point provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space (such as above suspended ceilings) in accordance with Section 300-22(C) of the National Electrical Code (NEC).

Note If you plan to mount the access point in environmental air space and will upgrade to a 5-GHz radio, Cisco recommends that you mount the access point horizontally with its antennas pointing down. Doing so will result in the access point complying with regulatory requirements for environmental air space after the 5-GHz radio is installed.

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

Figure 6-1 Mounting Bracket



1	Access point mount	**5**	Locking detent
2	Cable tie points	**6**	Wall cable access
3	Ceiling mount holes	**7**	Suspended ceiling cable access
4	Access point mounts	**8**	Security hasp

CISCO CONFIDENTIAL - Draft 2

A mounting hardware kit is provided that contains the hardware and fasteners necessary to mount the access point. Refer to the Table 6-1 to identify the materials you need to mount your access point, then go to the section containing the specific mounting procedure.

Table 6-1 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 Four wall anchors 3/16 in. (4.7 mm) or 3/32 in. (2.3 mm) drill bit Drill Standard screwdriver	Yes Yes No No No
Suspended ceiling	Two caddy fasteners with studs Two plastic spacers Two 1/4–20 Keps nuts with built-in washers Standard screwdriver Appropriate wrench or pliers	Yes Yes Yes No No

Mounting on a Horizontal or Vertical Surface

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

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

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

Step 3 Install the anchors into the wall if you are using them. Otherwise, go to Step 4.

Step 4 Secure the mounting bracket to the surface using the #8 fasteners.

Note On a vertical surface, mount the bracket with its security hasp facing down.

Step 5 Attach the access point to the mounting bracket.

Note You can make your installation more secure by mounting it to a stud or major structural member and using the appropriate fasteners.

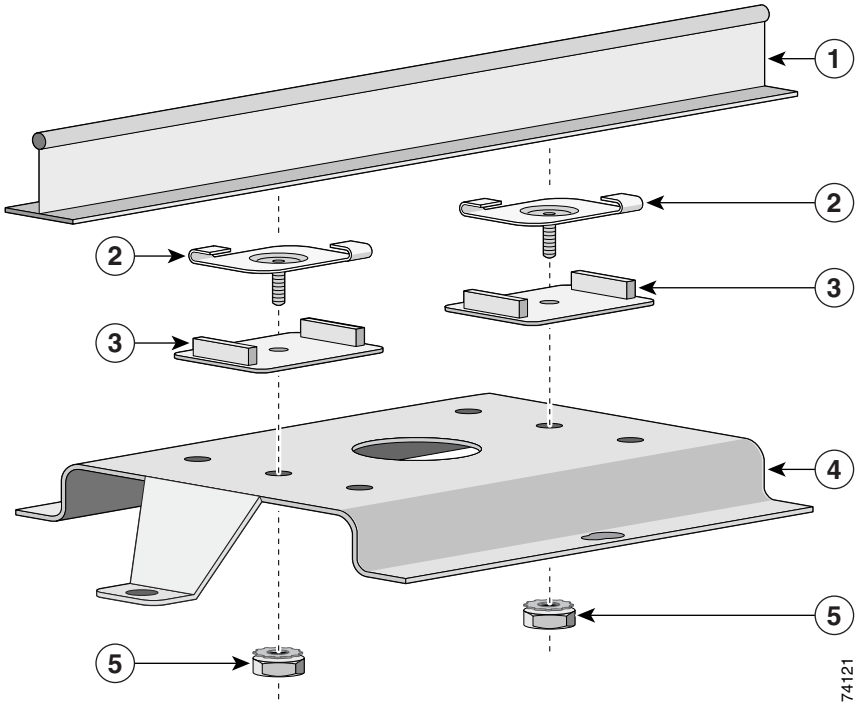
CISCO CONFIDENTIAL - Draft 2

Mounting Below a Suspended Ceiling

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

You should review Figure 6-2 before beginning the mounting process.

Figure 6-2 Mounting Bracket Parts



1	Suspended ceiling T-rail	**4**	Mounting bracket
2	Caddy fastener	**5**	Keps nut (contains an attached lock washer)
3	Plastic spacer		

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 caddy fasteners to the suspended ceiling T-rail.

Step 3 Use the mounting bracket to adjust the distance between the caddy fasteners so that they align with the holes in the mounting bracket.

Step 4 Use a standard screwdriver to tighten the caddy fastener studs in place on the suspended ceiling T-rail. Do not overtighten.

Step 5 Install a plastic spacer on each caddy fastener stud. The spacer's legs should contact the suspended ceiling T-rail.

Step 6 Attach the mounting bracket to the caddy fastener studs and start a Keps nut on each stud.

CISCO CONFIDENTIAL - Draft 2

Step 7 Use a wrench or pliers to tighten the Keps nuts. Do not overtighten.

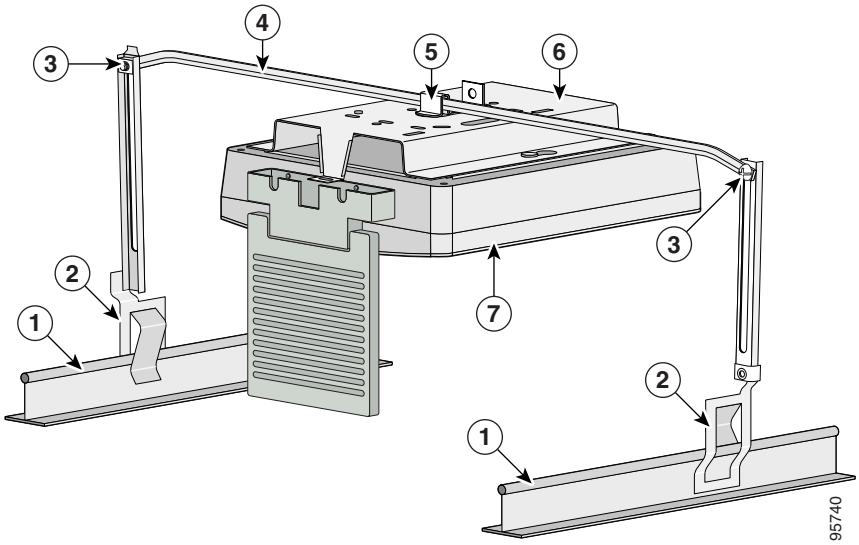
Step 8 Attach the access point to the mounting bracket.

Mounting Above a Suspended Ceiling

The access point mounting bracket 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 and BHC, 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 6-3 before proceeding.

Figure 6-3 Mounting Bracket Parts

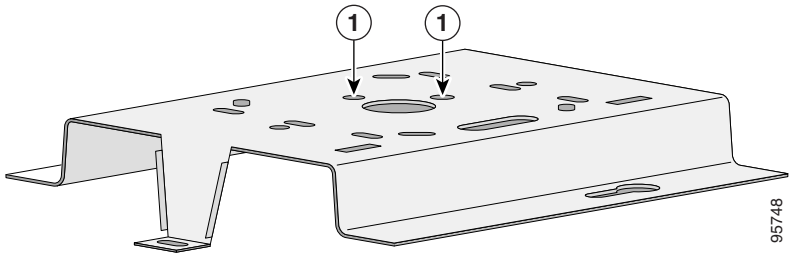


1	Suspended ceiling T-rail	**5**	Bracket mounting clip
2	T-rail clip	**6**	Access point mounting bracket
3	Height adjustment screw	**7**	Access point
4	T-bar box hanger		

CISCO CONFIDENTIAL - Draft 2

The bracket mounting clip requires the use of an access point mounting bracket (700-13520-03) with two extra holes (see Figure 6-4).

Figure 6-4 Mounting Bracket Holes



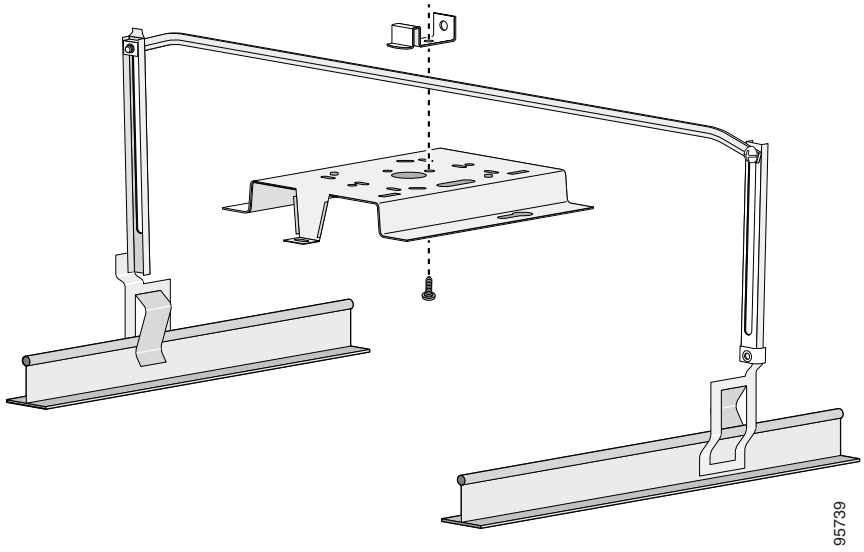
1	Extra holes	

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 bracket.

Step 2 Place the clip over the T-bar box hanger and secure it to the access point mounting bracket (see Figure 6-5) with the 1/4-20 fastener (supplied with the T-bar hanger).

Figure 6-5 Access Point Mounting Bracket



Note The illustration shows the access point mounting bracket 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 antennas so that they are pointing down when mounted on the T-bar Box hanger. Orient the 5-GHz antenna for patch or omnidirectional operation as desired.

CISCO CONFIDENTIAL - Draft 2

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 6-3).

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 Attach the access point to the access point mounting bracket (refer to the "Attaching the Access Point to the Mounting Bracket" section.

Step 9 Connect the Ethernet cables to the access point.

Note The access point power module and power injector are not rated for mounting above suspended ceilings. Therefore, you must use the Ethernet cable to supply power.

Step 10 If you need additional security, you can secure the access point to a nearby immovable object using a Kensington lock and security cable.

Step 11 Verify that the access point is operating before replacing the ceiling tile.

Attaching the Access Point to the Mounting Bracket

Follow these steps to attach the access point to the mounting bracket:

Step 1 Line up the three mounting pins on the access point with the large ends of the keyhole-shaped holes on the mounting bracket.

Step 2 Insert the access point into the keyhole shaped holes and maintain a slight pressure to hold it in place.

Step 3 Slide the access point's mounting pins into the small ends of the keyhole-shaped holes on the mounting bracket and push the connector end of the access point. You will hear a click when the locking detent contacts the access point and locks it into place.

Step 4 Attach and adjust the antenna(s) or antenna cables.

Step 5 Connect the Ethernet cable to the access point's Ethernet port.

Step 6 If using local power, insert the 1200 series power module cable connector into the access point's 48-VDC power port.

Securing the Access Point to the Mounting Bracket

The security hasp on the mounting bracket enables you to lock the access point to the bracket to make it more secure. When the access point is properly installed on the mounting bracket, the holes in the security hasps line up so you can install a padlock.

Known compatible padlocks are Master Lock models 120T or 121T.

CISCO CONFIDENTIAL - Draft 2

2.4-GHz Radio Upgrade

This chapter provides upgrade instructions for the 2.4-GHz (IEEE 802.11b or IEEE 802.11g) radio card and includes the following sections:

- Upgrade Overview, page 7-2
- Opening the Access Cover, page 7-3
- Removing a Blank Spacer Card, page 7-4
- Removing a 2.4-GHz Radio, page 7-5
- Installing a 2.4-GHz Radio, page 7-7
- Finding the Software Version, page 7-10

CISCO CONFIDENTIAL - Draft 2

Upgrade Overview

This section provides instructions for upgrading the access point 2.4-GHz radio.

Caution Your access point must be running Cisco IOS Release 12.2(13)JA or later before you upgrade to the IEEE 802.11g radio; otherwise your access point may not be able to complete the boot sequence until the radio is removed. For additional information, refer to the "Finding the Software Version" section.

The following operations summarize the upgrade procedure:

1. Remove all cables and power connections from the access point.
2. Follow standard electrostatic discharge (ESD) procedures.
3. Place the access point on an ESD-protected work surface.
4. Open the access point's 2.4-GHz radio access cover.
5. For an access point without a 2.4-GHz radio feature, remove the blank spacer card.
6. For an access point with a 2.4-GHz radio feature, remove the existing 2.4-GHz radio card.
7. Install the new 2.4-GHz radio card.
8. Close the access point 2.4-GHz radio access cover.

Caution ESD can damage the Cisco Aironet radio and the internal components of the access point. It is recommended that the 2.4-GHz radio upgrade procedures be performed by an ESD-trained service technician at an ESD-protected workstation.

Note After you install the new radio, all configurable radio settings will be at default values. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for complete instructions on configuring the new radio.

Unpacking the Radio

Each 2.4-GHz radio is shipped with the following items:

- Quick start guide
- A product registration card
- A T-10 tamper-resistant Torx L-wrench
- A 1200 series access point 2.4-GHz radio compliance label

Note The IEEE 802.11g radio also contains an1100 series access point product compliance label (not needed for a 1200 series access point) and a 1200 series access point product compliance label.

If anything is missing or damaged, contact your Cisco representative for support.

CISCO CONFIDENTIAL - Draft 2

Opening the Access Cover

To open the 2.4-GHz radio access cover, follow these steps:

Step 1 Remove all cables and power connections from the access point.

Step 2 Remove all static-generating items from the work area, such as plastic material, styrofoam cups, and other similar items.

Step 3 Place the access point and the new 2.4-GHz radio (in its antistatic bag) on an antistatic work surface.

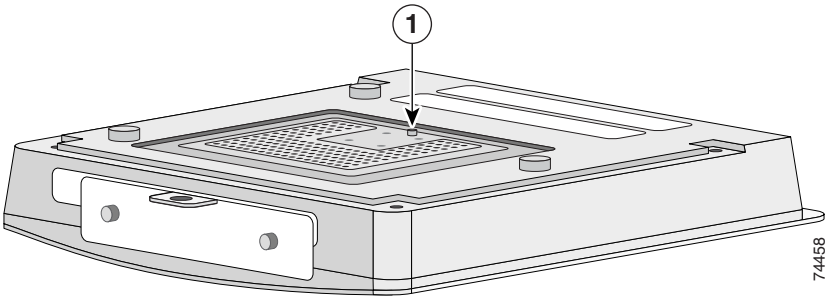
Step 4 Discharge any static buildup on your body by touching a grounded surface (antistatic work surface) before proceeding.

Step 5 Position the access point so that the bottom cover is facing up.

Caution The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

Step 6 Remove the bottom access cover using the T-10 tamper-resistant Torx L-wrench provided with your Cisco radio card (see Figure 7-1).

Figure 7-1 Location of 2.4-GHz Radio Access Cover Screw



1	Access Cover Screw	

If your access point was not configured with a 2.4-GHz radio, go to the "Removing a Blank Spacer Card" section. If you are replacing an existing 2.4-GHz radio, go to the "Removing a 2.4-GHz Radio" section.

CISCO CONFIDENTIAL - Draft 2

Removing a Blank Spacer Card

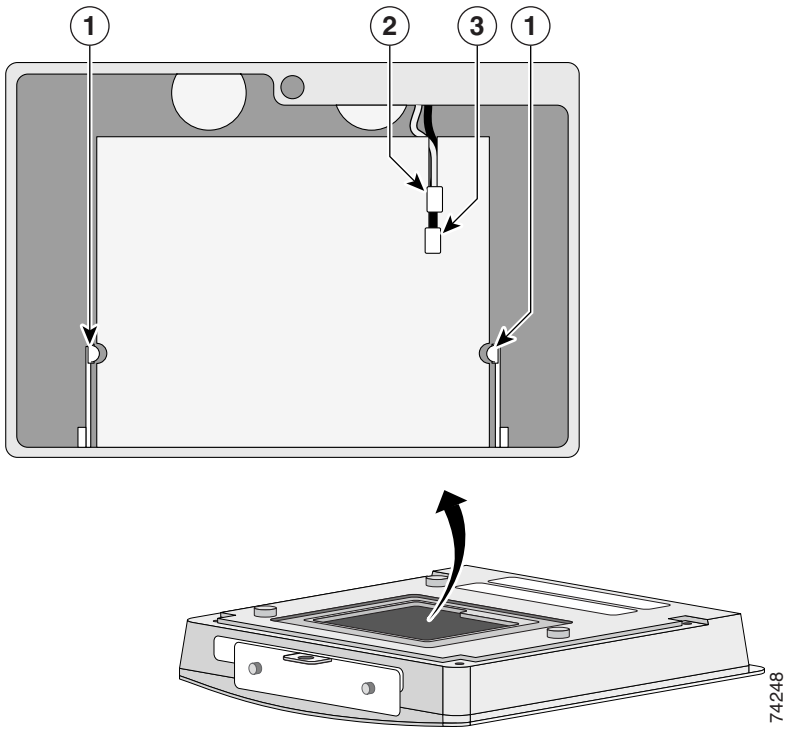
When your access point is not factory-configured with a 2.4-GHz radio, it contains a blank spacer card in the internal mini-PCI connector. You must remove the blank spacer card prior to installing a new 2.4-GHz radio card.

Caution Handle all components carefully and observe all ESD precautions. The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

To remove the blank spacer card from the mini-PCI connector, following these steps:

Step 1 Push the card-retaining clips (on each side of card) away from the card (see Figure 7-2). When released, the board springs up.

Figure 7-2 Location of Retaining Clips on Blank Spacer Card



1	Card-retaining clips	**3**	Antenna connector (black wire)
2	Antenna connector (white wire)		

Step 2 Carefully bend the card near the slots in opposite directions to provide enough clearance to remove the antenna wires.

CISCO CONFIDENTIAL - Draft 2

Step 3 Remove the antenna wires from the blank spacer card.

Caution To avoid damaging the antenna wire assemblies, handle them by their connectors.

Step 4 Remove the blank spacer card from the mini-PCI connector.

For instructions on installing the radio card, go to the "Installing a 2.4-GHz Radio" section.

Removing a 2.4-GHz Radio

To remove a 2.4-GHz radio card from your access point, follow these steps:

Caution The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

Step 1 Use your fingers to carefully remove the antenna wire connectors from the 2.4-GHz radio card.

Caution The antenna connectors can be damaged by using a pair of long-nose pliers during the removal process.

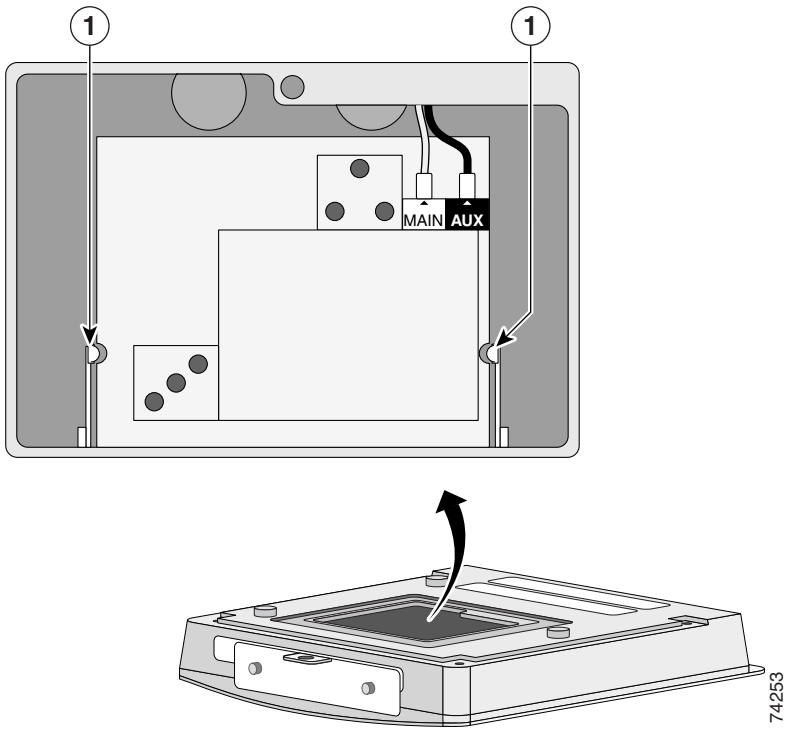
Caution To avoid damaging the antenna wire assemblies, handle them by their connectors.

CISCO CONFIDENTIAL - Draft 2

Step 2 Remove the 2.4-GHz radio card from the mini-PCI connector by performing the following operations:

a. Push the card-retaining clips (on each side of card) away from the card (see Figure 7-3). When released, the radio card springs up (see Figure 7-4).

Figure 7-3 Location of Retaining Clips on 2.4-GHz Radio Card



1	Card-retaining clips	

b. Grasp the radio card only on the edges, being careful not to touch components on the board or the gold connector pins.

c. Remove the 2.4-GHz card from the mini-PCI connector.

Step 3 Place the removed 2.4GHz radio card into an anti-static bag.

For instructions on installing a new radio card, go to the "Installing a 2.4-GHz Radio" section.

CISCO CONFIDENTIAL - Draft 2

Installing a 2.4-GHz Radio

To install a new 2.4-GHz radio card into the access point, follow these steps:

Caution The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

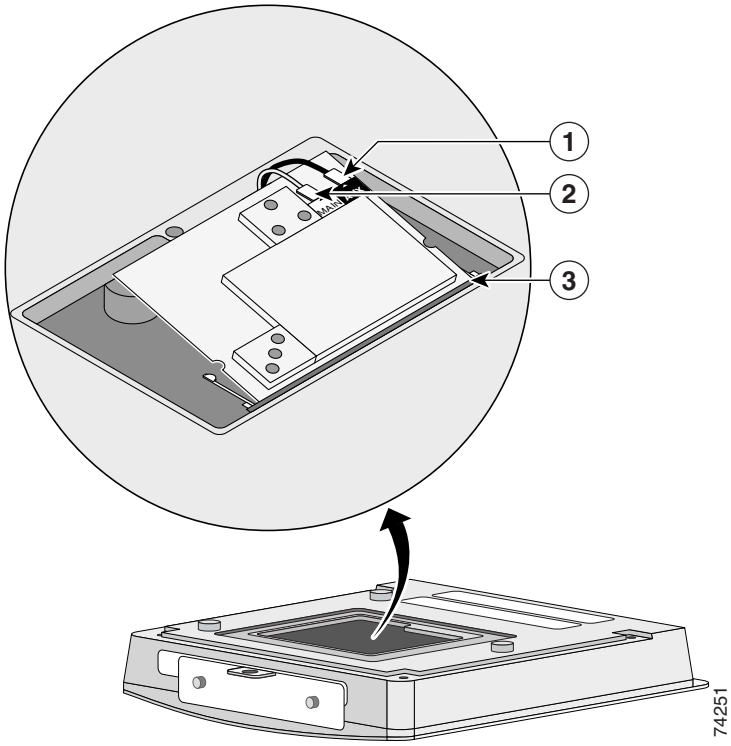
Step 1 Carefully remove the Cisco Aironet 2.4-GHz radio card from its anti-static bag.

Step 2 Grasp the radio card only on the edges, being careful not to touch components on the board or the gold connector pins.

Step 3 Connect the black antenna wire connector to the radio card antenna connector marked by the black label (see Figure 7-4).

Caution To avoid damaging the antenna wire assemblies, handle them by their connectors.

Figure 7-4 Antenna Connector Labels and Mini-PCI Connector



1	Antenna connector (black wire)	**3**	Mini-PCI connector
2	Antenna connector (white wire)		

Step 4 Connect the white antenna wire connector to the radio card antenna connector marked by the white label (see Figure 7-4).

CISCO CONFIDENTIAL - Draft 2

Step 5 Insert the radio card into the access point's mini-PCI connector by following these steps:

a. Tilt the radio card at approximately 20° to 30° so that its gold pins are aligned with the mini-PCI connector (see Figure 7-4).

b. Push the card into the mini-PCI connector until it clicks into place.

Step 6 Carefully push the card down (towards the access point's motherboard) until the card-retaining clips lock into the notches on the side of the radio card (you will hear a click).

Step 7 Carefully position the antenna wires so that the metal connectors do not touch each other.

Caution Do not allow antenna connectors to touch while power is applied, or the radio can be damaged. If they are touching, carefully rotate them in opposite directions until they are separated.

Step 8 Reinstall the 2.4-GHz radio access cover and use the T-10 tamper-resistant Torx L-wrench to tighten the cover's retaining screw.

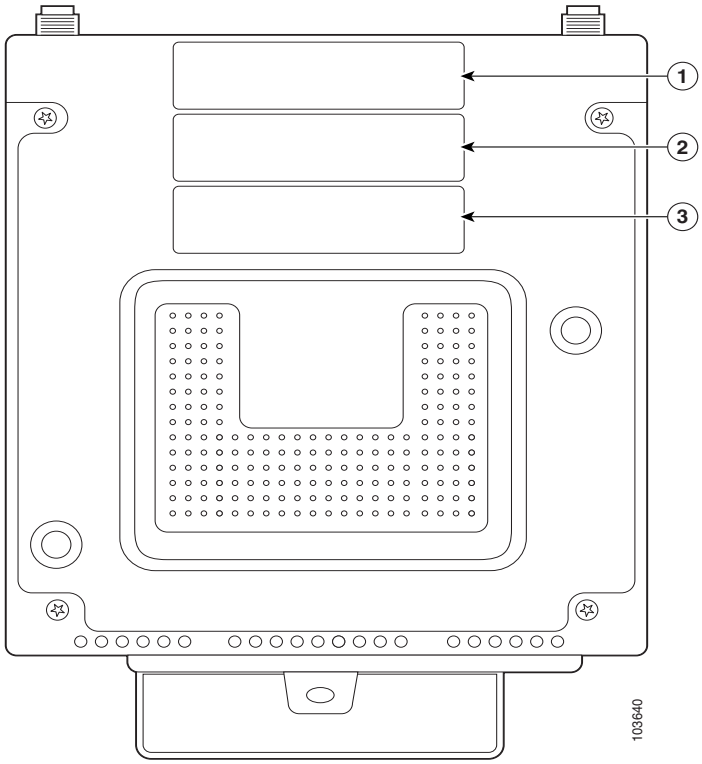
Step 9 Look at the compliance labels on your access point. Depending on the model you originally ordered, there may be up to three labels affixed to the case.

CISCO CONFIDENTIAL - Draft 2

Attaching the Compliance Labels

There are three places on the 1200 series access point dedicated to compliance labels, one for the product compliance label and two for the radio compliance labels. The label locations are shown in Figure 7-5.

Figure 7-5 Access Point Compliance Labels



1	Product compliance label	**3**	Radio compliance label
2	Radio compliance label		

The product compliance label always occupies the top space (location 1). The two spaces below (locations 2 and 3) contain the radio compliance labels. Whether or not locations 2 or 3 contain labels depends on how your access point is configured. For example, a dual-band access point could have two radio compliance labels (one for each radio device installed), or it could have only a product compliance label, depending on how it was ordered.

Make sure that your access point has the correct labels after you install or upgrade its radio configuration so that it will be in compliance with regulations in your country.

CISCO CONFIDENTIAL - Draft 2

Placing the Labels

The 802.11g radio upgrade kit ships with the following labels for the 1100 and 1200 series access points:

- 1100 series access point upgrade label (AIR-1121G-x-K9 UPGRADE)—not used on the 1200 series access point.
- 1200 series product compliance label (AIR-AP1231G-x-K9)
- 1200 series radio compliance label (AIR-MP21G-x-K9)

Table 7-1 shows where to place the labels on your 1200 series access point, based on the model you are upgrading. Follow these steps to place the labels correctly:

Step 1 Check the product compliance label to identify the model number of your 1200 series access point.

Step 2 Use the matrix in Table 7-1 to decide which labels to use and where to place them on the access point.

Table 7-1

1200 Series Model	AIR-MP21G-x-K9 Radio Compliance Label	AIR-AP1231G-x-K9 Product Compliance Label
AIR-AP1200	Place over existing AIR-MP20B-x-K9 radio compliance label or location 2 if no label exists.	—
AIR-AP1210		
AIR-AP1220A		
AIR-AP1230A		
AIR-AP1220B	—	Place over existing AIR-AP12xx-x-K9 product compliance label.
AIR-AP1230B		

Step 3 Discard any labels that you did not use.

The radio card installation is now complete. To configure the radio with your wireless network settings, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Finding the Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version** EXEC command. This example shows command output from an access point running Cisco IOS Release 12.2(11)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(11)JA
Copyright (c) 1986-2003 by Cisco Systems, Inc.
```

On access points running IOS software, you can also find the software version on the System Software page in the access point's web-browser interface.

If your access point does not run IOS software, the software version appears at the top left of most pages in the web-browser interface.

5-GHz Radio Module Upgrade

This chapter provides upgrade instructions for a 5-GHz radio module and includes the following sections:

- Upgrade Overview, page 8-2
- Removing the 5-GHz Radio Access Cover, page 8-2
- Removing a 5-GHz Radio Module, page 8-3
- Installing a 5-GHz Radio Module, page 8-5

CISCO CONFIDENTIAL - Draft 2

Upgrade Overview

This section provides instructions for upgrading the access point 5-GHz radio module (RM20A, RM21A, or RM22A). The following operations summarize the upgrade procedure:

1. Remove all cables and power connections from the access point.
2. Place your access point on a flat surface.
3. For an access point without the 5-GHz radio feature, remove the 5-GHz radio access cover.
4. For an access point with the 5-GHz radio feature, remove the existing 5-GHz radio module.
5. Install the new 5-GHz radio module.

Caution Your access point must be running Cisco IOS Release 12.3(2)JA or later before you upgrade to the RM21A or RM22A radio module; otherwise your access point may not be able to complete the boot sequence until the radio is removed. For additional information, refer to the "Finding the Software Version" section.

Note After you install the radio module, all configurable radio settings will be at default values. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for complete instructions on configuring the new radio.

Unpacking the Radio Module

Each 5-GHz radio module is shipped with the following items:

- Quick start guide
- A product registration card
- A T-10 tamper-resistant Torx L-wrench
- A 5-GHz radio compliance label

If anything is missing or damaged, contact your Cisco representative for support.

Removing the 5-GHz Radio Access Cover

On access points without an installed 5-GHz radio module, you must remove the access cover that covers the 5-GHz radio slot. To remove the 5-GHz radio access cover, follow these steps:

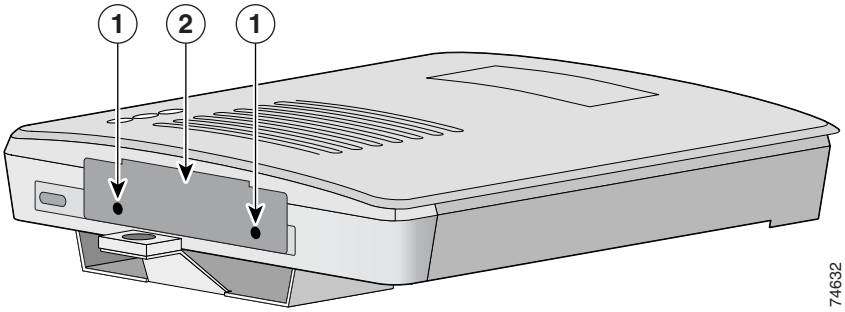
Step 1 Remove all cables and power connections from the access point.

Step 2 Place the access point on a flat surface so that the unit is upright with the front end facing you.

CISCO CONFIDENTIAL - Draft 2

Step 3 Remove the 5-GHz access cover using the supplied Torx L-wrench (see Figure 8-1).

Figure 8-1 5-GHz Radio Access Cover



1	Access Cover Screws	**2**	Access Cover

Removing a 5-GHz Radio Module

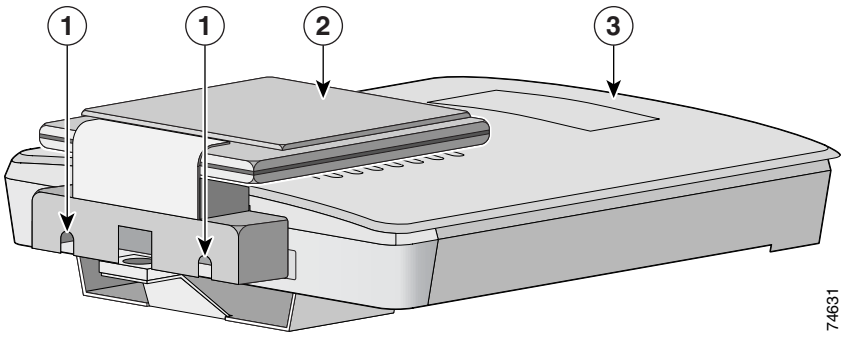
To remove the 5-GHz radio module, follow these steps:

Step 1 Remove all cables and power connections from the access point.

Step 2 Place the access point on a flat surface so that the unit is upright with the front end facing you.

Step 3 Unscrew the two mounting screws using the supplied Torx L-wrench (Figure 8-2).

Figure 8-2 5-GHz Radio Module



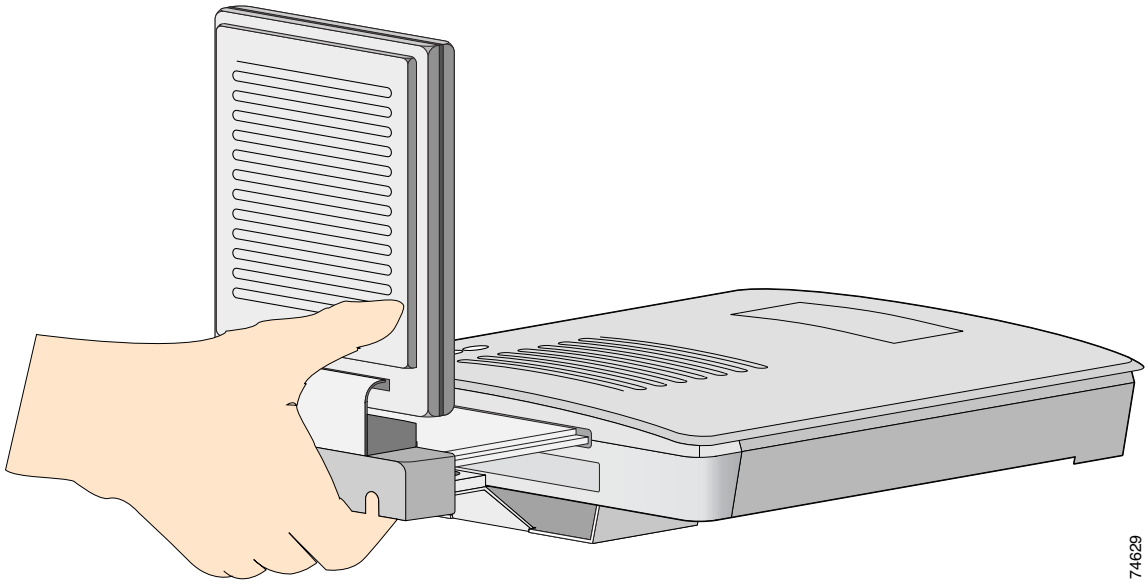
1	Mounting screws	**3**	Access point
2	5-GHz radio module antenna		

Note Do not attempt to remove the mounting screws from the module; they are captured in the module housing.

CISCO CONFIDENTIAL - Draft 2

Step 4 Insert your fingers into the base (latch opening) of the 5-GHz radio module (closest to the access point) and pull straight out from the access point (see Figure 8-3).

Figure 8-3 Removing the 5-GHz Radio Module



Step 5 For a radio module with built-in antenna, fold the antenna down (towards the attached radio card) and insert the module into a static protected bag.

Step 6 For a radio module with connectors, insert the radio module into a static protected bag.

To install a new 5-GHz radio module, see the "Installing a 5-GHz Radio Module" section on page 8-5.

CISCO CONFIDENTIAL - Draft 2

Installing a 5-GHz Radio Module

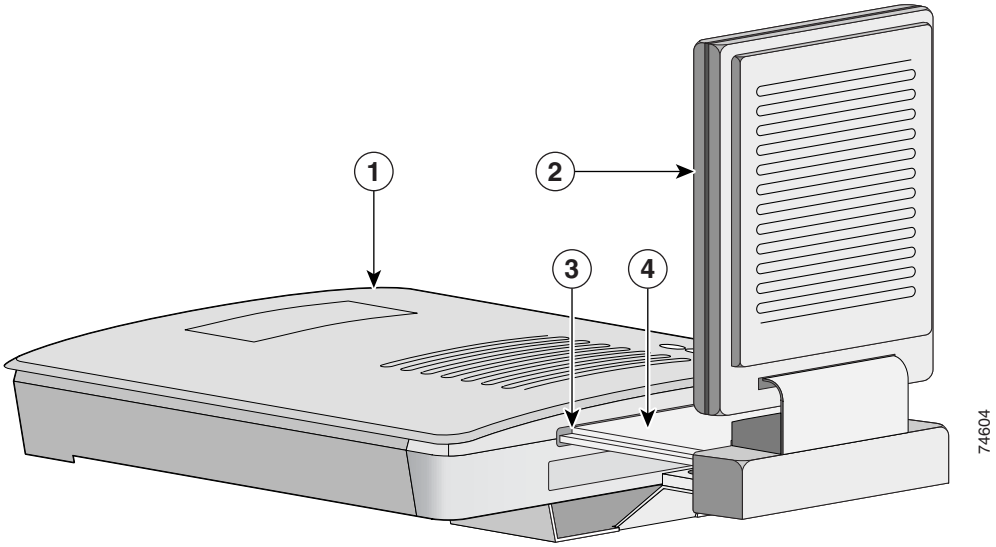
To install a new 5-GHz radio module (RM20A, RM21A, or RM22A) into your access point, follow these steps:

Step 1 Before you can install a new 5-GHz radio module, you must remove the access cover or an existing 5-GHz radio module (refer to "Removing the 5-GHz Radio Access Cover" or "Removing a 5-GHz Radio Module").

Step 2 Place the access point on a flat surface so that the unit is upright with the front end facing you.

Step 3 Grasp the new 5-GHz radio module by it's base (with the latch opening point down or the antenna pointing up) and insert the card into the access point's card-bus slot (see Figure 8-4).

Figure 8-4 Installing a 5-GHz Radio Module (RM20A or RM21A Shown)



1	Access point	**3**	Access point card-bus slot
2	5-GHz radio module antenna	**4**	5-GHz radio card

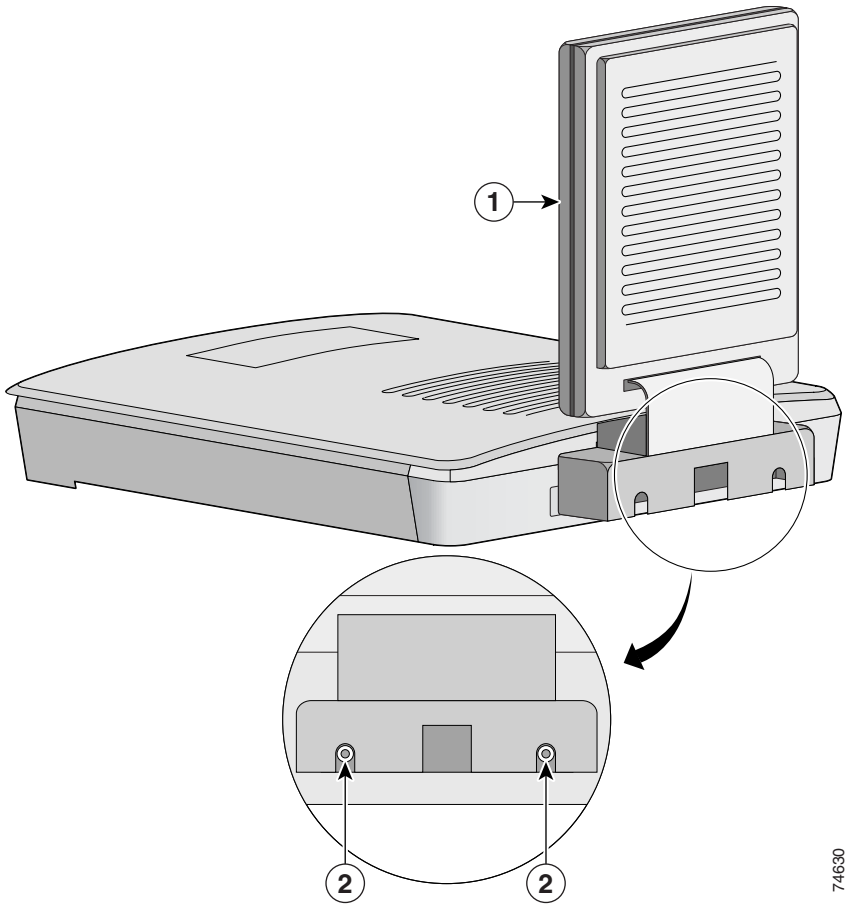
Step 4 Push the 5-GHz radio module into the slot until you hear a slight click.

CISCO CONFIDENTIAL - Draft 2

Step 5 Tighten the 5-GHz radio module mounting screws using the supplied Torx L-wrench (see Figure 8-5).

Note The RM22A radio module has the same mounting screws.

Figure 8-5 Location of Mounting Screws (RM20A or RM21A) Shown)



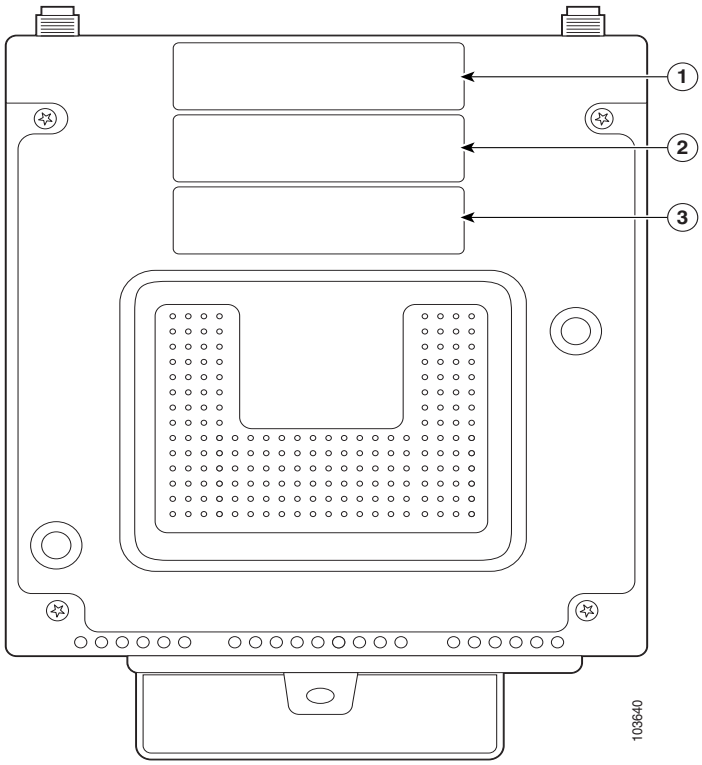
1	5-GHz radio module antenna	**2**	Mounting screws

CISCO CONFIDENTIAL - Draft 2

Attaching the Compliance Label

There are three places on the 1200 series access point dedicated to compliance labels, one for the product compliance label and two for the radio compliance labels. The label locations are shown in Figure 8-7.

Figure 8-6 Access Point Compliance Label Locations



1	Product compliance label	**3**	Radio compliance label
2	Radio compliance label		

The product compliance label always occupies the top space (location 1). The two spaces below the product compliance label (locations 2 and 3) contain the radio compliance labels. Whether or not locations 2 or 3 contain labels depends on how your access point is configured. For example, the access point could have two radio compliance labels (one for each radio device installed), or the access point could have only a product compliance label, depending on how it was ordered.

Make sure that your access point has the correct labels after you install or upgrade its radio configuration so that it will be in compliance with regulations in your country.

Follow these steps to place the label correctly:

Step 1 Refer to Figure 8-7 for the compliance label locations.

Step 2 Remove the backing paper from the 5-GHz radio compliance label.

Step 3 If your access point has a 5-GHz radio compliance label, place the new label over the existing label.

Step 4 If your access point does not have a 5-GHz radio compliance label, place the new label in an empty location (see Figure 8-7).

CISCO CONFIDENTIAL - Draft 2

The 5-GHz radio module installation is now complete and radio settings are at default values. To configure the 5-GHz radio with your wireless network settings refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.*

Finding the Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version** EXEC command. This example shows command output from an access point running Cisco IOS Release 12.2(11)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(11)JA
Copyright (c) 1986-2003 by Cisco Systems, Inc.
```

On access points running IOS software, you can also find the software version on the System Software page in the access point's web-browser interface.

If your access point does not run IOS software, the software version appears at the top left of most pages in the web-browser interface.

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Product Support > Wireless > Wireless LAN**):

http://www.cisco.com/tac

Sections in this chapter include:

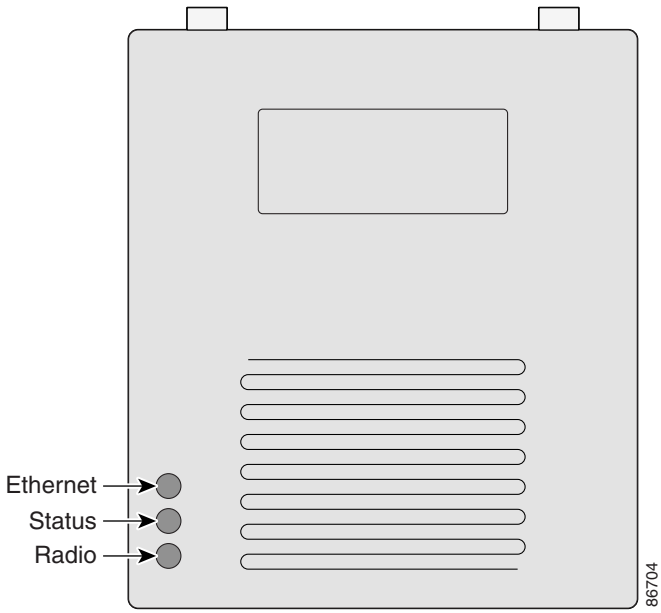
- Checking the Top Panel LEDs, page 9-2
- Checking Basic Settings, page 9-4
- Resetting to the Default Configuration, page 9-4
- Reloading the Access Point Image, page 9-6
- Obtaining the Access Point Image File, page 9-8
- Obtaining the TFTP Server Software, page 9-9

CISCO CONFIDENTIAL - Draft 2

Checking the Top Panel LEDs

If your access point is not communicating, check the three LEDs on the top panel. You can use them to quickly assess the unit's status. Figure 9-1 shows the LEDs.

Figure 9-1 Access Point LEDs



The LEDs signals have the following meanings (for additional details refer to Table 9-1):

- The Ethernet LED signals traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

CISCO CONFIDENTIAL - Draft 2

Table 9-1 Top Panel LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting IOS.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	-	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failure	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
Firmware Upgrade	–	Red	–	Loading new firmware image.

CISCO CONFIDENTIAL - Draft 2

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.

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. The access point default SSID is *tsunami*.

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 appears 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.

Running the Carrier Busy Test

You can use the carrier busy test to determine the least congested channel for a radio interface (802.11g or 802.11a). You should typically run the test several times to obtain the best results and to avoid temporary activity spikes.

Note The carrier busy test is primarily used for a single access point or a bridge environment. For sites with multiple access points, a site survey is typically performed to determine the best operating locations and operating frequencies for the access points.

CISCO CONFIDENTIAL - Draft 2

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

Perform these steps to activate the carrier busy test:

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

Step 2 Click **Network Interfaces** and the Network Interface Summary screen appears.

Step 3 Choose the radio interface experiencing problems by clicking **Radio0-802.11G** or **Radio1-802.11A**. The respective radio status page appears.

Step 4 Click the **Carrier Busy Test** tab and the Carrier Busy Test screen appears.

Step 5 Click **Start** to begin the carrier busy test.

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

Running the Ping/Link Test

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

a. Perform a test using a specified number of packets and then display the test results.

b. Perform a test that continuously operates until you stop the test and then displays the test results.

Perform these steps to activate the ping or link test:

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

Step 2 Click **Association** and the main association page appears.

Step 3 Click the MAC address of an associated wireless device and the Statistics page for that device appears.

Step 4 Click the **Ping/Link Test** tab and the Ping/Link Test page appears.

Step 5 If you want to specify the number of packets to use in the test, perform these steps:

a. Enter the desired number of packets in the Number of Packets field

b. Enter the desired packet size in the Packet Size field.

c. Click **Start**. The test automatically stops when all packets are utilized.

Step 6 If you want to use a continuous test, perform these steps:

a. Enter the desired packet size in the Packet Size field.

b. Click **Start** to activate the test.

c. When desired, click **Stop** to stop the test.

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

CISCO CONFIDENTIAL - Draft 2

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.

Step 2 Press and hold the MODE button while you reconnect power to the access point.

Step 3 Hold the MODE button until the Status LED turns amber (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 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 the steps below 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. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

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

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 appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

CISCO CONFIDENTIAL - Draft 2

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 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 pressing and holding the MODE button for around 30 seconds. 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.

Caution Your access point must be running specific Cisco IOS software releases before you upgrade its radios; otherwise your access point might not be able to complete the boot sequence until the radio is removed (see Table 9-2). For additional information, refer to the "Finding the Software Version" section.

Table 9-2 Required Cisco IOS Software Release

Radio Upgrade	Required Cisco IOS Software Release
IEEE 802.11g	12.2(13)JA or later
RM21A or RM22A	12.3(2)JA or later

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 three red LEDs, 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 the steps below to reload the access point image file:

Step 1 The PC you intend to use must be configured with a static IP address between 10.0.0.2 and 10.0.0.30.

CISCO CONFIDENTIAL - Draft 2

Step 2 Place a copy of the access point image file (such as c1200-k9w7-tar.122-13.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 **c1200-k9w7-tar.default**.

Step 4 Activate the TFTP server.

Step 5 Connect the PC to the access point power injector using a Category 5 (CAT5) Ethernet cable.

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 status LED turns red (approximately 20 to 30 seconds), and release the **MODE** button.

Step 9 Wait until the access point reboots as indicated by all LEDs turning green followed by the status LED blinking green.

Step 10 After the access point reboots, you must reconfigure the access point by using the Web interface, the Telnet interface, or 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.

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 the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

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

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 appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **Browse** button to locate the access point image file (such as c1200-k9w7-tar.122-13.JA.tar) on your PC.

Step 7 Click the **Upload** button.

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

CISCO CONFIDENTIAL - Draft 2

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 the instructions below to use a TFTP server:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

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

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 appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

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 c1200-k9w7-tar.122-13.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 appears that indicates the upgrade is complete, click **OK**.

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

Obtaining the Access Point Image File

Caution Your access point must be running specific Cisco IOS software releases before you upgrade its radios; otherwise your access point might not be able to complete the boot sequence until the radio is removed (see Table 9-2). For additional information, refer to the "Finding the Software Version" section.

Table 9-3 Required Cisco IOS Software Release

Radio Upgrade	Required Cisco IOS Software Release
IEEE 802.11g	12.2(13)JA or later
RM21A or RM22A	12.3(2)JA or later

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://www.cisco.com/public/sw-center/sw-wireless.shtml

Step 2 Click **Option 2: Aironet Wireless Software Display Tables**.

CISCO CONFIDENTIAL - Draft 2

Step 3 Find the access point firmware and utilities section and click **Cisco Aironet 1200 Series** (**Cisco IOS Software**).

Step 4 Click on the access point image file, such as c1200-k9w7-tar.122-13.JA.tar.

Step 5 On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply.

Step 6 Click **Submit**.

Step 7 Read and accept the terms and conditions of the Software License Agreement.

Step 8 Select the image file again to download it.

Step 9 Download and save the image file to your hard drive and then exit the Internet browser.

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.

Translated Safety Warnings

This appendix provides translations of the safety warnings that appear in this publication. These translated warnings apply to other documents in which they appear in English. The following safety warnings appear in this appendix:

- Statement 245B—Explosive Device Proximity Warning, page A-2
- Statement 332—Antenna Installation Warning, page A-3
- Statement 1001—Work During Lightning Activity Warning, page A-4
- Statement 1004—Installation Instructions Warning, page A-5
- Statement 1005—Circuit Breaker (15A) Warning, page A-6

CISCO CONFIDENTIAL - Draft 2

Statement 245B—Explosive Device Proximity Warning

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

Waarschuwing **Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermde ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.**

Varoitus **Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.**

Attention **Ne jamais utiliser un équipement de réseau sans fil à proximité d'un détonateur non blindé ou dans un lieu présentant des risques d'explosion, sauf si l'équipement a été modifié à cet effet.**

Warnung **Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.**

Avvertenza **Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.**

Advarsel **Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.**

Aviso **Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.**

¡Advertencia! **No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.**

Varning! **Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.**

CISCO CONFIDENTIAL - Draft 2

Statement 332—Antenna Installation Warning

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

Waarschuwing **Om te voldoen aan de FCC radiofrequentie (RF) blootstellingslimieten dienen antennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.**

Varoitus **FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan antennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.**

Attention **Pour se conformer aux limites d'exposition à la fréquence radio préconisées par la FCC (Federal Communications Commission), les antennes doivent se situer à un minimum de 20 cm de toute personne.**

Warnung **Um die in den FCC-Richtlinien festgelegten Expositionshöchstgrenzen für Radiofrequenzen (RF) nicht zu überschreiten, sollten Antennen mindestens 20 cm entfernt von Personen aufgestellt werden.**

Avvertenza **Per conformarsi ai limiti FCC di esposizione a radiofrequenza (RF), le antenne devono stare ad una distanza minima di 20 cm dal corpo di ogni persona.**

Advarsel **I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal antenner befinne seg på en avstand av minst 20 cm eller mer fra mennesker.**

Aviso **Para estar de acordo com as normas FCC de limites de exposição para freqüência de rádio (RF), as antenas devem estar distantes no mínimo 20 cm (7,9 pol) do corpo de qualquer pessoa.**

¡Advertencia! **Para cumplir con los límites de exposición de radio frecuencia (RF) de la Comisión Federal de Comunicaciones (FCC) es preciso ubicar las antenas a un mínimo de 20 cm (7,9 pulgadas) o más del cuerpo de las personas.**

Varning! **För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör antenner placeras på minst 20 cm avstånd från alla människor.**

CISCO CONFIDENTIAL - Draft 2

Statement 1001—Work During Lightning Activity Warning

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

Waarschuwing **Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.**

Varoitus **Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.**

Attention **Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.**

Warnung **Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.**

Avvertenza **Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.**

Advarsel **Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.**

Aviso **Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).**

¡Advertencia! **No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.**

Varning! **Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.**

Figyelem **Villámlás közben ne dolgozzon a rendszeren, valamint ne csatlakoztasson és ne húzzon ki kábeleket!**

Предупреждение Не следует работать с устройством, а также подключать или отключать кабели во время грозы.

警告 请勿在发生雷电时操作系统，也不要在此期间连接或断开电缆。

警告 雷が発生しているときは、システムに手を加えたり、ケーブルの接続や取り外しを行わないでください。

CISCO CONFIDENTIAL - Draft 2

Statement 1004—Installation Instructions Warning

Warning	**Read the installation instructions before connecting the system to the power source.** Statement 1004
Waarschuwing	**Raadpleeg de installatie-instructies voordat u het systeem op de voedingsbron aansluit.**
Varoitus	**Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.**
Attention	**Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.**
Warnung	**Vor dem Anschließen des Systems an die Stromquelle die Installationsanweisungen lesen.**
Avvertenza	**Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.**
Advarsel	**Les installasjonsinstruksjonene før systemet kobles til strømkilden.**
Aviso	**Leia as instruções de instalação antes de ligar o sistema à fonte de energia.**
¡Advertencia!	**Lea las instrucciones de instalación antes de conectar el sistema a la red de alimentación.**
Varning!	**Läs installationsanvisningarna innan du kopplar systemet till strömförsörjningsenheten.**
Figyelem	**Mielőtt áramforráshoz csatlakoztatná a rendszert, olvassa el az üzembe helyezési útmutatót!**
Предупреждение	Перед подключением устройства к источнику электропитания ознакомьтесь с данной инструкцией по установке.
警告	在将系统与电源连接之前，请仔细阅读安装说明。
警告	必ず設置手順を読んでから、システムを電源に接続してください。

CISCO CONFIDENTIAL - Draft 2

Statement 1005—Circuit Breaker (15A) Warning

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
15A Statement 1005

Waarschuwing **Dit product is afhankelijk van de installatie van het gebouw voor beveiliging tegen kortsluiting (overstroom). Controleer of de beschermingsinrichting niet meer dan:**
15A is.

Varoitus **Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että suojalaitteen mitoitus ei ole yli:**
15A

Attention **Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifiez que le courant nominal du dispositif de protection n'est pas supérieur à :**
15A

Warnung **Dieses Produkt ist darauf angewiesen, dass im Gebäude ein Kurzschluss- bzw. Überstromschutz installiert ist. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung nicht mehr als:**
15A beträgt.

Avvertenza **Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia un rating superiore a:**
15A

Advarsel **Dette produktet er avhengig av bygningens installasjoner av kortslutnings (overstrøm)-beskyttelse. Påse at verneenheten ikke er merket høyere enn:**
15A

Aviso **Este produto depende das instalações existentes para proteção contra curto-circuito (sobrecarga). Assegure-se de que o fusível ou disjuntor não seja superior a:**
15A

¡Advertencia! **Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) del edificio. Asegúrese de que el dispositivo de protección no sea superior a:**
15A

Varning! **Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att skyddsanordningen inte har högre märkvärde än:**
15A

Figyelem **A termék védelmi rendszerének része az épület kábelezésébe épített rövidzárlat (túláram) elleni védelem is. Gondoskodjon róla, hogy a készüléket védő eszköz legfeljebb a következő áramerősségre legyen méretezve:**
15A

CISCO CONFIDENTIAL - Draft 2

Предупреждение Защита устройства от короткого замыкания (перегрузки) осуществляется с помощью оборудования, являющегося частью электропроводки здания. Убедитесь, что номинал защитного устройства не превышает:
15A

警告 此产品的短路（过载电流）保护由建筑物的供电系统提供。确保短路保护设备的额定电流不大于：
15A

警告 この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。保護装置の定格が以下の値を超えないことを確認してください。
15A

CISCO CONFIDENTIAL - Draft 2

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1200 Series Access Points.

This appendix contains the following sections:

- Manufacturers Federal Communication Commission Declaration of Conformity Statement
- Department of Communications—Canada
- European Community, Switzerland, Norway, Iceland, and Liechtenstein
- Declaration of Conformity for RF Exposure
- Guidelines for Operating Cisco Aironet Access Points in Japan

CISCO CONFIDENTIAL - Draft 2

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Tested To Comply
With FCC Standards

FOR HOME OR OFFICE USE

Models:

AIR-AP1200 with AIR-MP20B-A-K9 and/or AIR-RM20A-A-K9;
AIR-AP1210 with AIR-MP20B-A-K9 or AIR-MP21G-A-K9, and/or AIR-RM20A-A-K9 or AIR-RM21A-A-K9 or AIR-RM22A-A-K9;
AIR-AP1220B-A-K9, AIR-AP1230B-A-K9, AIR-AP1220A-A-K9, AIR-AP1230A-A-K9, or AIR-AP1231G-A-K9

FCC Certification number:

LDK 102042 (AIR-MP20B-A-K9) or
LDK 102049 (AIR-MP21G-A-K9) and/or
LDK 102045 (AIR-RM20A-A-K9)
LDK 102053 (AIR-RM21A-A-K9 and AIR-RM22A-A-K9)

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.

CISCO CONFIDENTIAL - Draft 2

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas or those listed in Table B-1. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

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

Table B-1 Access Point 2.4-GHz Antennas

Radio		Antenna		
IEEE 802.11b	**IEEE 802.11g**	**Cisco Part Number**	**Model**	**Gain (dBi)**
Yes	–	AIR-ANT1949	Yagi	13.5
Yes	–	AIR-ANT4121	Omni-directional	12.0
Yes	–	AIR-ANT24120	Omni-directional	12.0
Yes	Yes	AIR-ANT2410Y-R	Yagi-directional	10.0
Yes	Yes	AIR-ANT3549	Patch	8.5
Yes	Yes	AIR-ANT2012	Spatial diversity	6.5
Yes	Yes	AIR-ANT1729	Patch	6.0
Yes	Yes	AIR-ANT2506	Omni-directional	5.1
Yes	Yes	AIR-ANT3213	Omni-directional	5.0
Yes	Yes	AIR-ANT1728	Omni-directional	5.0
Yes	Yes	AIR-ANT3195	Patch	3.0
Yes	Yes	AIR-ANT5959	Omni-directional	2.0
Yes	Yes	AIR-ANT4941	Dipole	2.2

Department of Communications—Canada

Canadian Compliance Statement

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

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur 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 CONFIDENTIAL - Draft 2

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

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

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprecheneden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Directiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directive 1999/5/EC.
Έλληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigencies essentialles et aux autres dispositions pertinantes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.
Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-directiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

CISCO CONFIDENTIAL - Draft 2

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

The following CE mark is affixed to access points with a 2.4 GHz radio:

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.

Note Combinations of power levels and antennas resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and other countries that have adopted the European R&TTE directive 1999/5/EC or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

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

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

The following CE mark is affixed to the 54 Mbps, 5 GHz access points:

- For AIR-RM20A, AIR-RM21A, and AIR-RM22A

CE 0682

CISCO CONFIDENTIAL - Draft 2

Declaration of Conformity for RF Exposure

The radio module 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. For the IEEE 802.11B antennas, AIR-ANT24120, AIR-ANT4121 and AIR-ANT1949 the equipment should be positioned more than 2 m (6.56 ft) from your body or nearby persons. For all other approved antennas the equipment shoud be installed more than 20 cm (7.9 in.) from your body or nearby persons.

The access point (with 5 GHz integrated antenna) 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 antennas. The access point's co-located 2.4 GHz (2.2 dBi) and 5 GHz integrated antennas support a minimum separation distance of 10 cm (3.9 in.) and are compliant with the applicable FCC RF exposure limit when transmitting simultaneously.

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

Guidelines for Operating Cisco Aironet Access Points in Japan

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

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

CISCO CONFIDENTIAL - Draft 2

English Translation

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

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

   Contact Number: `03-5549-6500`

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operatingCisco Aironet access points inTaiwan. 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 2

All Access Points

Chinese Translation

低功率電波輻射性電機管理辦法

第十四條　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。

第十七條　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。

95815

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

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 17

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 2

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 statements for the European Union countries are listed below:

CISCO SYSTEMS

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

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

Declare under our sole responsibility that the product,

AIR-MPI 350 / 2.4 GHz 11 Mbps Mini PCI Embedded Adapter
Variants : AIR-MPI 352, AIR-MP20B-E-K9

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

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09**
Health & Safety	**EN60950: 1992+A1+A2+A3+A4**
Radio	**EN 300.328-1 and -2: 2000-7**

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

The product carries the CE Mark:

Date & Place of Issue: 1 April 2002 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 136186rev1

CISCO CONFIDENTIAL - Draft 2

DECLARATION OF CONFORMITY

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

according to EN 45014

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

Declare under our sole responsibility that the product,

Product:	***AIR-AP1220B-E-K9 / Wireless LAN Access Point*** *(2,4 GHz version)*
Variants:	***AIR-AP1230B-E-K9; AIR-AP1200 / AIR-AP1210*** *platform with* ***AIR-MP20B-E-K9*** */ 2.4 GHz Mini PCI Radio Module*
Options included:	***AIR-MP20B-E-K9*** */ 2.4 GHz Mini PCI Radio Module*

Fulfils the essential requirements of the Directives 1999/5/EC and 93/42/EEC.

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09** **EN 60601-1-2: 2001**
Health & Safety	**EN60950: 1992+A1+A2+A3+A4**
Radio	**EN 300.328-1: 2001-12; EN 300.328-2: 2001-12**

The following conformity assessment procedures have been followed:

- Directive 1999/5/EC : procedure referred to in Article 10.4 and Annex III.
- Directive 93/42/EEC: procedure referred to in Article 11.5 and Annex VII.

The product carries the CE Mark:

Date & Place of Issue: 9 October 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 195677rev3

CISCO CONFIDENTIAL - Draft 2

CISCO SYSTEMS

DECLARATION OF CONFORMITY

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

according to EN 45014

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

Declare under our sole responsibility that the product,

Product: ***AIR-AP1220A-A-K9*** */ Dual Band Wireless LAN Access Point (2.4 GHz /5 GHz)*
Variants: ***AIR-AP1230A-A-K9; AIR-AP1200 / AIR-AP1210*** *platform with* ***AIR-RM20A-A-K9*** */ 5 GHz Wireless LAN Module (IEEE802.11a)*
Options included: ***AIR-RM20A-A-K9*** */ 5 GHz Wireless LAN Module (IEEE802.11a)*
Optional: ***AIR-MP20B-E-K9*** */ 2.4 GHz Mini PCI Radio Module (IEEE802.11b)*

Fulfils the essential requirements of the Directives 1999/5/EC and 93/42/EEC

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09** **EN 60601-1-2: 2001**	
Health & Safety	**EN60950: 1992+A1+A2+A3+A4**	
Radio	**2.4 GHz :**	**EN 300.328-1: 2001-12; EN 300.328-2: 2001-12**
	5 GHz:	**Draft EN 301.893: 2002-07** *(except for clause 4.6.3.1, see annex for details)*

With regard to the Directive 93/42/EEC, the conformity procedure referred to in Article 11.5 and Annex VII has been followed.

With regard to the Directive 1999/5/EC, the conformity assessment procedure referred to in Article 10 and Annex IV has been followed in association with the notified body listed below:

Cetecom ICT Services GmbH, Saarbrucken - Germany

The product carries the CE Mark: CE 0682 !

Date & Place of Issue: 9 October 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 236853rev2

CISCO CONFIDENTIAL - Draft 2

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

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

Declare under our sole responsibility that the product,

Product:	***AIR-AP1231G-E-K9*** */ 2.4 GHz 54 Mbps Wireless LAN Access Point*
Variants:	***AIR-AP1210*** *platform with* ***AIR-MP21G-E-K9*** *2.4 GHz 54 Mbps Mini PCI Radio Module*
Options included:	***AIR-MP21G-E-K9*** *2.4 GHz 54 Mbps Mini PCI Radio Module*

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

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328-2: 2001-12; EN 300 328: 2003-04**

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

The product carries the CE Mark:

Date & Place of Issue: 15 September 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 323388

CISCO CONFIDENTIAL - Draft 2

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

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

Declare under our sole responsibility that the product,

AIR-MP21G-E-K9 */ 2.4 GHz 54 Mbps Mini PCI Radio Module*

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

The following standards were applied:

EMC	**EN 301 489-1: 2002-08; EN 301 489-17: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328-2: 2001-12; EN 300 328: 2003-04**

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

The product carries the CE Mark:

Date & Place of Issue: 15 September 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 323389

CISCO CONFIDENTIAL - Draft 2

Access Point Specifications

This appendix provides technical specifications for the Cisco Aironet 1200 Series Access Point. Table C-1 lists the technical specifications for the access point.

Table C-1 Access Point Specifications

Category	Access Point with 802.11b or 802.11g Radio	Access Point with 802.11a Radio Module
Size	6.56 in. W x 7.23 in. D x 1.66 in. H 16.67 cm W x 18.36 cm D x 4.22 cm H	With the antenna in the patch position (RM20A and RM21A): 6.56 in. W x 8.04 in. D x 2.21 in. H 16.67 cm W x 20.42 cm D x 5.61 With the RM22A radio module: 6.56 in. W x 8.76 in. D x 1.66 in. H 16.67 cm W x 22.25 cm D x 4.22 cm H
Status Indicators	Three indicators on the top panel: Ethernet traffic, status, and radio traffic.	
Connectors	Base unit: Back panel (left to right): reverse-TNC antenna connector; power connector (for plug-in AC power module); RJ-45 connector for 10BASE-T or 100BASE-T Ethernet connections; upside down RJ-45 connector for serial connections; reverse-TNC antenna connector. Front Panel: Card Bus connector used for an 802.11a radio module. RM22A radio module: Left and right reverse-TNC antenna connectors	
Input Voltage	48 VDC nominal. Operational up to 60 VDC. Voltage higher than 60 VDC can damage the unit.	

CISCO CONFIDENTIAL - Draft 2

Table C-1 Access Point Specifications (continued)

Category	Access Point with 802.11b or 802.11g Radio	Access Point with 802.11a Radio Module
Input Power	With 802.11b radio: 6.0 W (typical) With 802.11g radio: 6.2 W (typical)	With RM20A radio module: 8.0 W (typical) With 802.11b radio and RM20A radio module: 10.0 W (typical) With 802.11g radio and RM20A radio module: 10.2 W (typical) With RM21A or RM22A radio module: TBD W (typical) With 802.11b radio and (RM21A or RM22A radio module: TBD W (typical) With 802.11g radio and (RM21A or RM22A radio module: TBD W (typical)
Operating Temperature	Base unit with 802.11b or 802.11g radio: –4 to 131°F (–20 to 55°C) 1200 series power injector: 32 to 104°F (0 to 40°C)	Access point (with two radios): –4 to 122°F (–20 to 50°C) 1200 series power injector: 32 to 104°F (0 to 40°C)
Storage Temperature	–40 to 185°F (–40 to 85°C)	
Weight	Without mounting bracket: 1.6 lbs (0.73 kg) with 802.11b or 802.11g radio 1.87 lbs (0.85 kg) with RM20A or RM21A radio module 1.97 lbs (0.89 kg) with RM20A or RM21A radio module and 802.11b or 802.11g radio 1.83 lbs (0.83 kg) with RM22A radio module 1.93 lbs (0.88 kg) with RM22A radio module and 802.11b or 802.11g radio	

CISCO CONFIDENTIAL - Draft 2

Table C-1 Access Point Specifications (continued)

Category	Access Point with 802.11b or 802.11g Radio	Access Point with 802.11a Radio Module
Power Output	With 802.11b radio: 100, 50, 30, 20, 5, or 1 mW With 802.11g radio: 100, 50, 30, 20, 5, or 1 mW (at 1, 2, 5.5, and 11 Mbps) 30, 20, 10, 5, or 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) (Depending on the regulatory domain in which the access point is installed)	RM20A radio module: 16 dBm 13 dBm 10 dBm 7 dBm RM21A radio module or RM22A radio module: 17 dBm 15 DBm 14 dBm 11 dBm 10 dBm 8 dBm 5 dBm 2 dBm -1 dBm **Note** These values are based on the FCC peak measurement method as defined in FCC 15.407 (A)(4) (Depending on the regulatory domain in which the access point is installed)
Antenna	A diversity system with two reverse-TNC connectors for external antennas (Cisco antennas are sold separately).	RM20A radio module: A diversity system consisting of two integrated 4.5 dBi omnidirectional gain or two integrated 6 dBi directional gain depending on the positioning of the antenna. RM21A radio module: A diversity system consisting of a dipole array providing 5 dBi omnidirectional gain or 9 dBi directional gain depending on the positioning of the antenna. RM22A radio module: A diversity system with two reverse-TNC antenna connectors for external antennas (Cisco antennas are sold separately).

CISCO CONFIDENTIAL - Draft 2

Table C-1 Access Point Specifications (continued)

Category	Access Point with 802.11b or 802.11g Radio	Access Point with 802.11a Radio Module
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)	RM20A radio module: UNII 1—5.15 to 5.25 GHz UNII 2—5.25 to 5.35 GHz RM21A radio module or RM22A radio module: UNII 1—5.15 to 5.25 GHz UNII 2—5.25 to 5.35 GHz UNII 3—5.725 to 5.850 GHz (Depending on the regulatory domain in which the access point is installed)
Modulation	802.11b radio: Complementary Code Keying (CCK) 802.11g radio: OFDM	Orthogonal Frequency Division Multiplex (OFDM)
Subcarrier modulation	CCK (5.5 Mbps and 11 Mbps) BPSK (1 Mbps, 6 Mbps and 9 Mbps) QPSK (2 Mbps, 12 Mbps and 18 Mbps) 16-QAM (24 Mbps and 36 Mbps) 64-QAM (48 Mbps and 54 Mbps)	BPSK (6 Mbps and 9 Mbps) QPSK (12 Mbps, 12 Mbps and 18 Mbps) 16-QAM (24 Mbps and 36 Mbps) 64-QAM (48 Mbps and 54 Mbps)
Data rates	802.11b radio: 1, 2, 5.5, and 11 Mbps 802.11g radio: 1, 2, 5.5, and 11 Mbps 6, 9, 12, 18, 24, 36, 48, and 54 Mbps	6, 9, 12, 18, 24, 36, 48, and 54 Mbps

CISCO CONFIDENTIAL - Draft 2

Table C-1 Access Point Specifications (continued)

Category	Access Point with 802.11b or 802.11g Radio	Access Point with 802.11a Radio Module
Typical Range	Indoor (across office cubicle walls): 802.11b radio: (100 mW output power) 350 ft at 1 Mbps 150 ft at 11 Mbps 802.11g radio: (100 mW output power) 410 ft (125.0 m) at 1 Mbps 270 ft (82.3 m) at 2 Mbps 220 ft (67.1 m) at 5.5 Mbps 160 ft (48.8 m) at 11 Mbps (30 mW output power) 300 ft (91.4 m) at 6 Mbps 210 ft (67.1 m) at 12 Mbps 180 ft (54.9 m) at 18 Mbps 90 ft (27.4 m) at 54 Mbps Outdoor: 802.11b radio (100 mW output power): 2000 ft at 1 Mbps 800 ft at 11 Mbps 802.11g radio: (100 mW output power) 2000 ft (609.6 m) at 1 Mbps 1000 ft (304.8 m) at 11 Mbps (30 mW output power) 1300 ft (396.2 m) at 6 Mbps 600 ft (182.9 m) at 18 Mbps 250 ft (76.2 m) at 54 Mbps **Note** Using 2.2dBi antennas at the access point and the client adapter.	Indoor (across office cubicle walls): RM20A radio module: 165 ft (50.3 m) at 6 Mbps 130 ft (39.6 m) at 12 Mbps 110 ft (33.5 m) at 18 Mbps 45 ft (13.7 m) at 54 Mbps **Note** Using 40mW output power with 6 dBi antennas at the access point and client adapter. RM21A radio module or RM22A radio module: TBD ft (TBD m) at 6 Mbps TBD ft (TBD m) at 12 Mbps TBD ft (TBD m) at 18 Mbps TBD ft (TBD m) at 54 Mbps Outdoor: RM20A radio module: 1000 ft (304.8 m) at 6 Mbps 100 ft (30.5 m) at 54 Mbps **Note** Using 40mW output power with 6 dBi antennas at the access point and client adapter. RM21A radio module or RM22A radio module: TBD ft (TBD m) at 6 Mbps TBD ft (TBD m) at 54 Mbps
Compliance	The 1200 series access point complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings. **Caution** The 1200 series power injectors and power modules are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings. **Note** If you plan to mount the access point in environmental air space using a 802.11a radio, Cisco recommends that you mount the access point horizontally with its antennas pointing down. Doing so results in the access point complying with regulatory requirements for environmental air space with an 802.11a radio installed.	

CISCO CONFIDENTIAL - Draft 2

Table C-1 Access Point Specifications (continued)

Category	Access Point with 802.11b or 802.11g Radio	Access Point with 802.11a Radio Module
Safety	Designed to meet: • UL 1950 Third Edition • CSA 22.2 No. 950-95 • IEC 60950 Second Edition, including Amendments 1-4 with all deviations • EN 60950 Second Edition, including Amendments 1-4	Designed to meet: • UL 1950 Third Edition • CSA 22.2 No. 950-95 • IEC 60950 Second Edition, including Amendments 1-4 with all deviations • EN 60950 Second Edition, including Amendments 1-4
Radio Approvals	802.11b radio: FCC Part 15.247 Canada RSS-210 Japan ARIB-STD-33B EN 300.328 ARIB STD-66 802.11g radio: FCC Parts 15.247, 15.205, 15.209 Canada RSS-210 Japan ARIB-STD-33B Japan ARIB-STD-66 Europe EN-300.328	FCC Part 15.407 Canada RSS-210 Japan ARIB STD-T71 EN 301.893
EMI and Susceptibility	FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) EN 55022 B AS/NZS 3548 Class B VCCI Class B EN 55024 EN 301.489-1 EN 301.489-17	
RF Exposure	OET-65C RSS-102 ANSI C95.1	

Channels and Antenna Settings

This appendix lists the IEEE 802.11b (2.4-GHz), IEEE 802.11g (2.4-GHz), and IEEE 802.11a (5-GHz) channels, maximum power levels, and antenna gains supported by the world's regulatory domains.

The following topics are covered in this appendix:

- Channels, page D-2
- Maximum Power Levels and Antenna Gains, page D-5

CISCO CONFIDENTIAL - Draft 2

Channels

IEEE 802.11b (2.4-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b 22-MHz-wide channel are shown in Table D-1.

Table D-1 Channels for IEEE 802.11b

Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (-A)	China (-C)	EMEA (-E)	Israel (-I)	Japan (-J)
1	2412	X	X	X	–	X
2	2417	X	X	X	–	X
3	2422	X	X	X	–	X
4	2427	X	X	X	–	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	–	X
10	2457	X	X	X	–	X
11	2462	X	X	X	–	X
12	2467	–	–	X	–	X
13	2472	–	–	X	–	X
14	2484	–	–	–	–	X

Note Mexico is included in the Americas (–A) regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.

CISCO CONFIDENTIAL - Draft 2

IEEE 802.11g (2.4-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11g 22-MHz-wide channel are shown in Table D-2.

Table D-2 Channels for IEEE 802.11g

Channel Identifier	Center Frequency (MHz)	Regulatory Domains							
		Americas (–A)		EMEA (–E)		Israel (–I)		Japan (–J)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	X	X	X	X	–	–	X	X
2	2417	X	X	X	X	–	–	X	X
3	2422	X	X	X	X	–	–	X	X
4	2427	X	X	X	X	–	–	X	X
5	2432	X	X	X	X	X	X	X	X
6	2437	X	X	X	X	X	X	X	X
7	2442	X	X	X	X	X	X	X	X
8	2447	X	X	X	X	X	X	X	X
9	2452	X	X	X	X	X	–	X	X
10	2457	X	X	X	X	X	–	X	X
11	2462	X	X	X	X	X	–	X	X
12	2467	–	–	X	X	X	–	X	X
13	2472	–	–	X	X	X	–	X	X
14	2484	–	–	–	–	–	–	X	–

CISCO CONFIDENTIAL - Draft 2

IEEE 802.11a (5-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are shown in Table D-3 and Table D-4.

Table D-3 Channels for IEEE 802.11a for the RM20A Radio Module

Channel Identifier	Center Frequency (MHz)	Regulatory Domains			
		Americas (–A)	Japan (–J)	Singapore (–S)	Taiwan (–T)
34	5170	–	X	–	–
36	5180	X	–	X	–
38	5190	–	X	–	–
40	5200	X	–	X	–
42	5210	–	X	–	–
44	5220	X	–	X	–
46	5230	–	X	–	–
48	5240	X	–	X	–
52	5260	X	–	–	X
56	5280	X	–	–	X
60	5300	X	–	–	X
64	5320	X	–	–	X

Note All channel sets are restricted to indoor usage except the Americas (–A), which allows for indoor and outdoor use on channels 52 through 64 in the United States.

Table D-4 Channels for IEEE 802.11a for the RM21A and RM22A Radio Modules

Channel Identifier	Center Frequency (MHz)	Regulatory Domains						
		Americas (–A)	China (–C)	EMEA (–E)	Japan (–J)	Norway (–N)	Singapore (–S)	Taiwan (–T)
UNII-1 (5150-5250 MHz)								
34	5170	–	–	–	X	–	–	–
36	5180	X	–	X	–	X	X	–
38	5190	–	–	–	X	–	–	–
40	5200	X	–	X	–	X	X	–
42	5210	–	–	–	X	–	–	–
44	5220	X	–	X	–	X	X	–
46	5230	–	–	–	X	–	–	–
48	5240	X	–	X		X	X	–

CISCO CONFIDENTIAL - Draft 2

Table D-4 Channels for IEEE 802.11a for the RM21A and RM22A Radio Modules (continued)

Channel Identifier	Center Frequency (MHz)	Regulatory Domains						
		Americas (–A)	China (–C)	EMEA (–E)	Japan (–J)	Norway (–N)	Singapore (–S)	Taiwan (–T)
UNII-2 (5250-5350 MHz)								
52	5260	X	–	X	–	X	–	X
56	5280	X	–	X	–	X	–	X
60	5300	X	–	X	–	X	–	X
64	5320	X	–	X	–	X	–	X
UNII-3 (5725-5850 MHz)								
149	5745	X	X	–	–	X	X	X
153	5765	X	X	–	–	X	X	X
157	5785	X	X	–	–	X	X	X
161	5805	X	X	–	–	X	X	X
165	5825	–	–	–	–	–	–	–

Maximum Power Levels and Antenna Gains

IEEE 802.11b (2.4-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table D-5 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11b regulatory domain.

Table D-5 Maximum Power Levels Per Antenna Gain for IEEE 802.11b

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (–A) (4 W EIRP maximum)	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
China (–C) (10 mW EIRP maximum)	2.2	5

CISCO CONFIDENTIAL - Draft 2

Table D-5 Maximum Power Levels Per Antenna Gain for IEEE 802.11b (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
EMEA (–E) (100 mW EIRP maximum)	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
Israel (–I) (100 mW EIRP maximum)	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
Japan (–J) (10 mW/MHz EIRP maximum)	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5

IEEE 802.11g (2.4-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table D-6 indicates the maximum power levels and antenna gains allowed for each IEEE 802.11g regulatory domain.

Table D-6 Maximum Power Levels Per Antenna Gain for IEEE 802.11g

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)	
		CCK Modulation	OFDM Modulation
Americas (–A) (4 W EIRP maximum)	2.2	100	30
	5	100	30
	6	100	30
	6.5	100	30
	8.5	100	30
	10	100	30

CISCO CONFIDENTIAL - Draft 2

Table D-6 Maximum Power Levels Per Antenna Gain for IEEE 802.11g (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)	
		CCK Modulation	OFDM Modulation
EMEA (–E) (100 mW EIRP maximum)	2.2	50	30
	5	30	10
	6	30	10
	6.5	20	10
	8.5	10	5
	10	10	5
Israel (–I) (100 mW EIRP maximum)	2.2	50	30
	5	30	10
	6	30	10
	6.5	20	10
	8.5	10	5
	10	10	5
Japan (–J) (10 mW/MHz EIRP maximum)	2.2	30	30
	5	30	30
	6	30	30
	6.5	30	30
	8.5	n/a	n/a
	10	n/a	n/a

IEEE 802.11a (5-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table D-7 indicates the maximum power levels allowed with RM20A radio module for each IEEE 802.11a regulatory domain.

Table D-7 Maximum Power Per Antenna Gain for the RM20A Radio Module

Regulatory Domain	Maximum Power Level (mW) with 6-dBi Antenna Gain
Americas (–A) (160 mW EIRP maximum on channels 36-48, (800 mW EIRP maximum on channels 52-64)	40
Japan (–J) (10 mW/MHz EIRP maximum)	40
Singapore (–S) (100 mW EIRP maximum)	20
Taiwan (–T) (800 mW EIRP maximum)	40

CISCO CONFIDENTIAL - Draft 2

Table D-8 indicates the maximum power levels allowed with the 5 dBi integrated antenna and the RM21A radio module for each IEEE 802.11a regulatory domain.

Table D-8 Maximum Power for RM21A Radio Module with 5 dBi Integrated Antenna

Channel Identifier	Center Frequency (MHz)	Maximum Power Levels (dBm) in the Regulatory Domains						
		Americas (–A)	China (–C)	EMEA (–E)	Japan (–J)	North America (-N)	Singapore (–S)	Taiwan (-T)
UNII-1 (5150-5250 MHz)								
34	5170	–	–	–	15	–	–	–
36	5180	15	–	17	–	15	17	–
38	5190	–	–	–	15	–	–	–
40	5200	15	–	17	–	15	17	–
42	5210	–	–	–	15	–	–	–
44	5220	15	–	17	–	15	17	–
46	5230	–	–	–	14	–	–	–
48	5240	15	–	17		15	17	–
UNII-2 (5250-5350 MHz)								
52	5260	17	–	17	–	17		–
56	5280	17	–	17	–	17		15
60	5300	17	–	17	–	17		15
64	5320	17	–	17	–	17		15
UNII-3 (5725-5850 MHz)								
149	5745	17	17	–	–	17	15	17
153	5765	17	17	–	–	17	15	17
157	5785	17	17	–	–	17	15	17
161	5805	17	17	–	–	17	15	17
165	5825	–	–	–	–	–	–	–

CISCO CONFIDENTIAL - Draft 2

Table D-9 indicates the maximum power levels allowed with the 9 dBi integrated antenna and the RM21A radio module for each IEEE 802.11a regulatory domain.

Table D-9 Maximum Power for RM21A Radio Module with 9 dBi Integrated Antenna

Channel Identifier	Center Frequency (MHz)	Maximum Power Levels (dBm) in the Regulatory Domains						
		Americas (–A)	China (–C)	EMEA (–E)	Japan (–J)	North America (-N)	Singapore (–S)	Taiwan (-T)
UNII-1 (5150-5250 MHz)								
34	5170	–	–	–	11	–	–	–
36	5180	11	–	11	–	11	14	–
38	5190	–	–	–	11	–	–	–
40	5200	11	–	11	–	11	14	–
42	5210	–	–	–	11	–	–	–
44	5220	11	–	11	–	11	14	–
46	5230	–	–	–	11	–	–	–
48	5240	11	–	11	–	11	14	–
UNII-2 (5250-5350 MHz)								
52	5260	17	–	11	–	17	–	–
56	5280	17	–	11	–	17	–	11
60	5300	17	–	11	–	17	–	11
64	5320	11	–	11	–	11	–	11
UNII-3 (5725-5850 MHz)								
149	5745	17	17	–	–	17	11	17
153	5765	17	17	–	–	17	11	17
157	5785	14	17	–	–	14	11	14
161	5805	11	17	–	–	11	11	11
165	5825	–	–	–	–	–	–	–

CISCO CONFIDENTIAL - Draft 2

Table D-10 and Table D-11 indicates the maximum power levels allowed with the RM22A radio module and external antennas and for each IEEE 802.11a regulatory domain.

Table D-10 Maximum Power for the RM22A Radio Module with up to 9.5 dBi External Antennas

Channel Identifier	Center Frequency (MHz)	Maximum Power Levels (dBm) in the Regulatory Domains					
		Americas (–A)	China (–C)	Japan (–J)	North America (-N)	Singapore (–S)	Taiwan (-T)
UNII-1 (5150-5250 MHz)							
34	5170	–	–	11	–	–	–
36	5180	11	–	–	11	14	–
38	5190	–	–	11	–	–	–
40	5200	11	–	–	11	14	–
42	5210	–	–	11	–	–	–
44	5220	11	–	–	11	14	–
46	5230	–	–	11	–	–	–
48	5240	11	–	–	11	14	–
UNII-2 (5250-5350 MHz)							
52	5260	17	–	–	17	–	–
56	5280	17	–	–	17	–	11
60	5300	17	–	–	17	–	11
64	5320	11	–	–	11	–	11
UNII-3 (5725-5850 MHz)							
149	5745	17	17	–	17	11	17
153	5765	17	17	–	17	11	17
157	5785	14	17	–	14	11	14
161	5805	11	17	–	11	11	11
165	5825	–	–	–	–	–	–

CISCO CONFIDENTIAL - Draft 2

Caution To avoid exceeding maximum conducted power levels in the EU regulatory domain when using a 7- or a 9.5-dBi external antenna, you must manually set the access point output power level as shown in. Refer to the *Setting Maximum Power Levels for EU and Other Countries* document that shipped with your access point.

Table D-11 Maximum Power for the RM22A Radio Module with External Antennas in the EMEA (-E) Regulatory Domain

Channel Identifier	Center Frequency (MHz)	Maximum Power Levels (dBm) in the EMEA (-E) Regulatory Domain				
		4 dBi Antenna	4.5 dBi Antenna	6 dBi Antenna	7 dBi Antenna	9.5 dBi Antenna
UNII-1 (5150-5250 MHz)						
34	5170	–	–	–	–	–
36	5180	17	17	15	15	11
38	5190	–	–	–	–	–
40	5200	17	17	15	15	11
42	5210	–	–	–	–	–
44	5220	17	17	15	15	11
46	5230	–	–	–	–	–
48	5240	17	17	15	15	11
UNII-2 (5250-5350 MHz)						
52	5260	17	17	15	15	11
56	5280	17	17	15	15	11
60	5300	17	17	15	15	11
64	5320	11	11	15	15	11
UNII-3 (5725-5850 MHz)						
149	5745	–	–	–	–	–
153	5765	–	–	–	–	–
157	5785	–	–	–	–	–
161	5805	–	–	–	–	–
165	5825	–	–	–	–	–

CISCO CONFIDENTIAL - Draft 2

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 2

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.

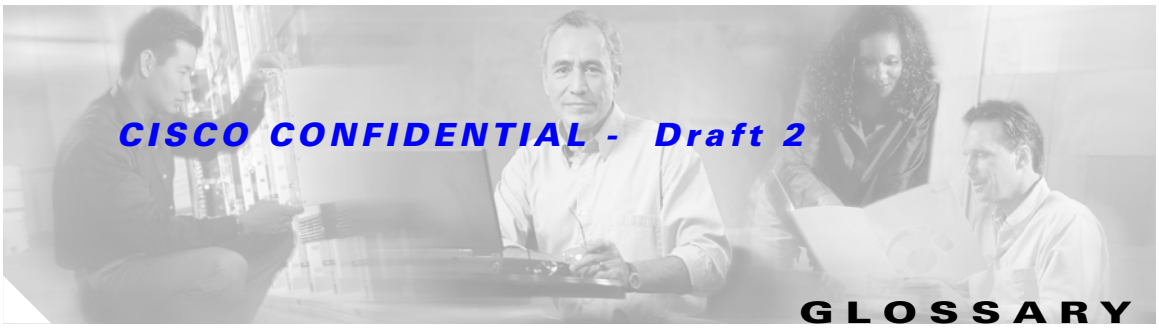
Note Both the Ethernet and console ports use RJ-45 connectors. Be careful to avoid accidently connecting the serial cable to the Ethernet port connector.

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[1, 2, 3, 4]	Pins	Signals[1, 2, 3, 4]
1	NC	–	–
2	NC	–	–
3	TXD	2	RXD
4	GND	5	GND
5	GND	5	GND
6	RXD	3	TXD
7	NC	–	–
8	NC	–	–

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



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.

B

beacon 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.

BOOTP Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

CISCO CONFIDENTIAL - Draft 2

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

cell 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.

client A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi 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.

DHCP 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.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

Domain Name 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.

DNS 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.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

CISCO CONFIDENTIAL - Draft 2

E

EAP 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.

Ethernet 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

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

IEEE 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.

infrastructure The wired Ethernet network.

IP Address The Internet Protocol (IP) address of a station.

IP subnet mask 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.

isotropic An antenna that radiates its signal in a spherical pattern.

CISCO CONFIDENTIAL - Draft 2

M

MAC 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.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

O

omni-directional This typically refers to a primarily circular antenna radiation pattern.

Orthogonal Frequency Division Multiplex (OFDM) 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

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

Quadruple Phase Shift Keying 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.

CISCO CONFIDENTIAL - Draft 2

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.

U

UNII 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.

UNII-1 Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.

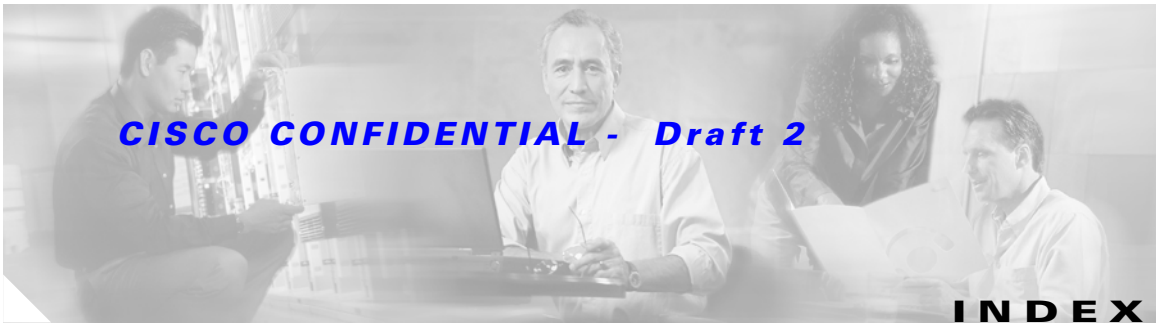
unicast packet A single data message (packet) sent to a specific IP address.

W

WEP 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.

workstation A computing device with an installed PC card.

CISCO CONFIDENTIAL - Draft 2



A

abbreviating commands 5-3
access point image 9-6
antenna
  connectors C-2
  gains D-5
  warnings A-1
Apply button 4-4

B

Back button 4-4
basic settings, checking 9-4

C

Cancel button 4-4
Cisco TAC 9-1
CLI
  abbreviating commands 5-3
  command modes 5-2
  editing features
    enabling and disabling 5-6
    keystroke editing 5-6
    wrapped lines 5-7
  error messages 5-4
  filtering command output 5-8
  getting help 5-3
  history
    changing the buffer size 5-4
    described 5-4
    disabling 5-5
    recalling commands 5-5
  no and default forms of commands 5-3
  terminal emulator settings 3-4
command-line interface
  See CLI
command modes 5-2
commands
  abbreviating 5-3
  no and default 5-3
connectors C-1, C-2
console port E-2

D

data rates C-3
declarations of conformity B-1
default, configuration, resetting 9-4
default commands 5-3

E

editing features
  enabling and disabling 5-6
  keystrokes used 5-6
  wrapped lines 5-7
EIRP, maximum D-5, D-6, D-7
error messages, during command entry 5-4
Ethernet indicator 9-2
extended temperature range 2-3

F

FCC Declaration of Conformity B-2

CISCO CONFIDENTIAL - Draft 2

FCC Safety Compliance 2-2
filtering
  show and more command output 5-8
frequencies D-2, D-3, D-4
frequency range C-3

G

global configuration mode 5-2

H

help, for the command line 5-3
history
  changing the buffer size 5-4
  described 5-4
  disabling 5-5
  recalling commands 5-5
Home button 4-4

I

indicators 9-2
input power C-1
installation guidelines 2-3
interface configuration mode 5-2
IP address, finding and setting 3-10
IPSU 3-9

K

key features 1-2

L

LED indicators
  Ethernet 9-2
  radio traffic 9-2
  status 9-2

M

MAC 3-10, 3-11
management options, CLI 5-1
Mode button 9-6
modulation C-3

N

no commands 5-3

O

OK button 4-4
operating temperature C-2

P

package contents 2-3
password reset 9-4
pinouts, serial cable E-2
power
  connecting 2-7
  injector 2-7
  input C-1
  output C-2
power level, maximum D-5
privileged EXEC mode 5-2

R

radio, indicator 9-2
range, radio C-4
regulatory
  domains D-2, D-3, D-4
regulatory information B-1

CISCO CONFIDENTIAL - Draft 2

reloading access point image 9-6
RF exposure B-6

S

safety warnings, translated A-1
serial
  cable E-2
  Cisco cable E-2
size C-1
SSH Communications Security, Ltd. 5-9
status indicators 9-2, C-1
storage temperature C-2

T

TAC 9-1
Telnet 3-12
temperature
  operating C-2
  storage C-2
terminal emulator 3-4
TFTP server 9-6
troubleshooting 9-1

U

unpacking 2-3
user EXEC mode 5-2

V

voltage range C-1

W

warnings 2-2, A-1
Web-based interface
  common buttons 4-4
  compatible browsers 4-1
web site, Cisco Software Center 3-9, 9-8
weight C-2
WEP key 9-4

CISCO CONFIDENTIAL - Draft 2