



CISCO CONFIDENTIAL - Draft 2



Cisco Aironet 1130AG Series Access Point Hardware Installation Guide

November 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-6226-01



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.

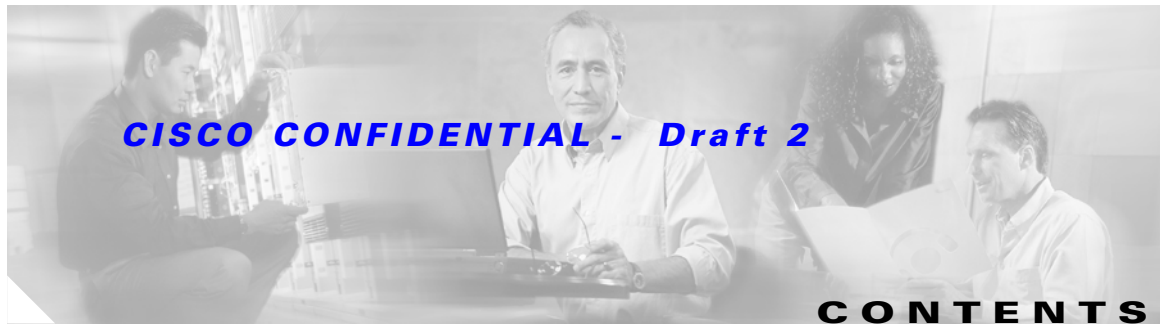
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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)



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
Overview	1-1
Hardware Features	1-2
Dual-Radio Operation	1-2
Ethernet Port	1-3
Console Port	1-3
LEDs	1-3
Power Sources	1-4
Anti-Theft Features	1-4
UL 2043 Certification	1-6
Network Configuration Examples	1-6
Root Unit on a Wired LAN	1-6
Repeater Unit that Extends Wireless Range	1-8
Central Unit in an All-Wireless Network	1-9

CISCO CONFIDENTIAL - Draft 2

- Installing the Access Point 2-1**
 - Safety Information 2-2
 - FCC Safety Compliance Statement 2-2
 - General Safety Guidelines 2-2
 - Warnings 2-2
 - Unpacking the Access Point 2-3
 - Package Contents 2-3
 - Basic Installation Guidelines 2-3
 - Before Beginning the Installation 2-4
 - Access Point Layout and Connectors 2-4
 - Mounting Plate 2-5
 - Suspended Ceiling Adjustable T-Rail Clips 2-6
 - Installation Summary 2-7
 - Opening the Access Point Cover 2-8
 - Mounting the Access Point 2-9
 - Mounting on a Horizontal or Vertical Surface 2-10
 - Mounting Below a Suspended Ceiling 2-11
 - Mounting Above a Suspended Ceiling 2-13
 - Mounting on a Network Cable Box 2-14
 - Mounting on a Desktop or Shelf 2-15
 - Rotating the Cisco Logo 2-15
 - Attaching the Access Point to the Mounting Plate 2-16
 - Connecting the Ethernet and Power Cables 2-17
 - Connecting to an Ethernet Network with an Inline Power Source 2-18
 - Connecting to an Ethernet Network with Local Power 2-19
 - Securing the Access Point 2-19
 - Using a Security Cable 2-19
 - Securing the Access Point to the Mounting Plate 2-20
 - Powering Up the Access Point 2-21
- Configuring the Access Point for the First Time 3-1**
 - Before You Start 3-2
 - Resetting the Access Point to Default Settings 3-2
 - Using the Mode Button 3-2
 - Using the Web-Browser Interface 3-2
 - Obtaining and Assigning an IP Address 3-3
 - Connecting to the Access Point Locally 3-3
 - Assigning Basic Settings 3-4

CISCO CONFIDENTIAL - Draft 2

Default Settings on the Express Setup Page	3-8
Protecting Your Wireless LAN	3-9
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
Assigning an IP Address Using the CLI	3-11
Using a Telnet Session to Access the CLI	3-11
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
Using the Command-Line Interface	5-1
Cisco 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

CISCO CONFIDENTIAL - Draft 2

Troubleshooting 6-1

- Checking the Access Point LEDs 6-2
- Checking Basic Settings 6-4
 - SSID 6-4
 - WEP Keys 6-5
 - Security Settings 6-5
- Low Power Condition 6-5
 - CDP Inline Power Negotiation 6-6
 - Inline Power Status Messages 6-6
 - Inline Power Exception 6-7
 - Issuing the Cisco IOS Command 6-7
- Running the Carrier Busy Test 6-8
- Running the Ping/Link Test 6-8
- Resetting to the Default Configuration 6-9
 - Using the MODE Button 6-9
 - Using the Web Browser Interface 6-10
- Reloading the Access Point Image 6-10
 - Using the MODE Button 6-11
 - Web Browser Interface 6-12
 - Browser HTTP Interface 6-12
 - Browser TFTP Interface 6-12
- Obtaining the Access Point Image File 6-13
- Obtaining the TFTP Server Software 6-13

Translated Safety Warnings A-1

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

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-3
 - Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC B-3
- Declaration of Conformity for RF Exposure B-5

CISCO CONFIDENTIAL - Draft 2

Guidelines for Operating Cisco Aironet Access Points in Japan **B-6**

 Japanese Translation **B-6**

 English Translation **B-6**

Declaration of Conformity Statements **B-7**

Access Point Specifications C-1

Channels and Power Levels D-1

 Channels and Maximum Power Levels **D-2**

 IEEE 802.11b/g (2.4-GHz Band) **D-2**

 IEEE 802.11a (5-GHz Band) **D-3**

Console Cable Pinouts E-1

 Overview **E-2**

 Console Port Signals and Pinouts **E-2**

GLOSSARY

INDEX

CISCO CONFIDENTIAL - Draft 2

Preface

Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1130AG 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 IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard IOS Release 12.2 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** from the Cisco IOS Software drop-down menu.

This guide also includes an overview of the access point web-based interface (APWI), which contains all the functionality of the command-line interface (CLI). This guide does not provide field-level descriptions of the APWI windows nor does it provide the procedures for configuring the access point from the APWI. 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.

Organization

This guide is organized into these chapters:

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

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

[Chapter 3, “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, “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 Power Levels,” 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.



Note

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

CISCO CONFIDENTIAL - Draft 2**Caution**

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

**Warning**

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

Waarschuwing

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

Varoitus

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

Attention

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

Warnung

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

Avvertenza

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

Advarsel

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

CISCO CONFIDENTIAL - Draft 2

Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning!	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

Related Publications

These documents provide complete information about the access point:

- *Release Notes for Cisco Aironet 1130AG Series Access Point*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *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>

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

CISCO CONFIDENTIAL - Draft 2

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 - TBD

The access point serial number label contains the following information:

- Model number, such as *AIR-AP1310*
- 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 1130AG 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 1130 series access point is a Wi-Fi certified, wireless LAN transceiver.

The access point contains two integrated radios: a 2.4-GHz radio (IEEE 802.11g) and a 5-GHz radio (IEEE 802.11a). 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 1-6](#)

CISCO CONFIDENTIAL - Draft 2

Hardware Features

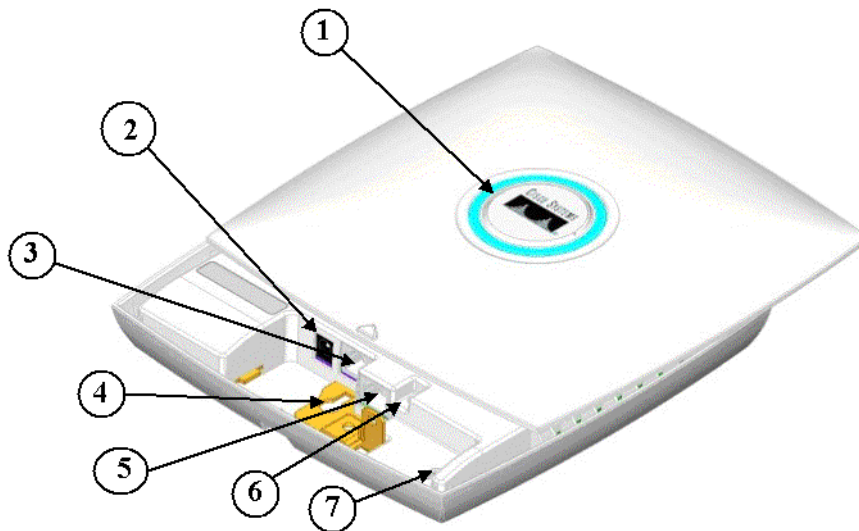
This section describes access point features. Refer to [Appendix C, “Access Point Specifications,”](#) for a list of access point specifications.

Key hardware features of the access point include:

- Dual-radio operation (see [page 1-2](#))
- Ethernet port (see [page 1-3](#))
- Console port (see [page 1-3](#))
- LEDs, (see [page 1-3](#))
- Power sources (see [page 1-4](#))
- Anti-theft features (see [page 1-4](#))
- UL 2043 certification (see [page 1-6](#))

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

Figure 1-1 Access Point Hardware Features



1	Status LED	5	Console port (RJ-45)
2	48-VDC power port	6	Mode button
3	Ethernet port (RJ-45)	7	Ethernet and Radio LEDs
4	Keyhole slot		

Dual-Radio Operation

The access point supports simultaneous radio operation using a 2.4-GHz 802.11g radio and a 5-GHz 802.11a radio. Each radio uses 2-dBi dual-diversity integrated antennas.

The 5-GHz radio incorporates an Unlicensed National Information Infrastructure (UNII) radio transceiver operating in the UNII 5-GHz frequency bands. The 802.11g radio is called *Radio0* and the 802.11a radio is called *Radio1*.

CISCO CONFIDENTIAL - Draft 2

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. The port is located in a cable bay area that is hidden by the top cover (see [Figure 1-1](#)).

Console Port

The serial console port provides access to the access point's command-line interface (CLI) using a terminal emulator program. The port is located in a cable bay area that is hidden by the top cover (see [Figure 1-1](#)). 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.

**Note**

Your console cable connector must not include over-molding or a cable boot because of space limitations within the cable bay area of the access point.

LEDs

The report Ethernet has three LEDs to indicate Ethernet activity, association status, radio activity, and other status indications (refer to the ["Checking the Access Point LEDs" section on page 6-2](#) for additional information).

- The Status LED provides general operating status and error indications.
- The Ethernet LED is located in the cable bay area under the access point top cover. This LED signals Ethernet traffic on the wired Ethernet LAN and provides Ethernet error indications.
- The Radio LED signals that wireless packets are being transmitted or received over the radio interface and provides radio error indications.

[Figure 1-1](#) shows the locations of the three LEDs.

CISCO CONFIDENTIAL - Draft 2**Power Sources**

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

**Warning**

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

The access point supports the following power sources:

- Power module (supplied)
- Inline power:
 - Cisco Aironet Power Injector (AIR-PWRINJ3 or AIR-PWRINJ-FIB)
 - An inline power capable switch, such as the Cisco Catalyst 3524 PWR XL, 3560-48PS, 3570-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
 - Other inline power switches supporting the IEEE 802.3af inline power standard

**Note**

Some switches and patch panels might not provide enough power to operate the access point when configured with both 2.4-GHz and 5-GHz radios. On power-up if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point also activates a Status LED low power error indication and creates an error log entry (refer to the [“Checking the Access Point LEDs”](#) section on page 6-2 and the [“Low Power Condition”](#) section on page 6-5).

Anti-Theft Features

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

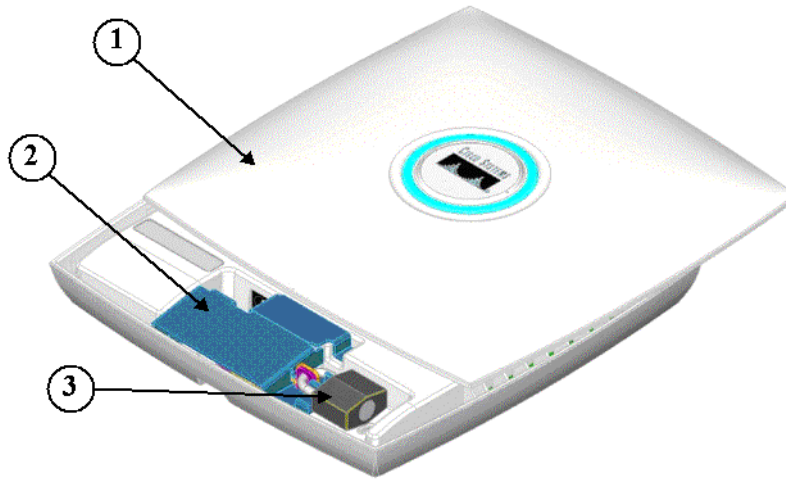
- Security cable keyhole—You can use the security cable slot to secure the access point using a standard security cable, such as those used on laptop computers.
- Security hasp adapter—When you mount the access point on a wall or ceiling using the mounting plate and the security hasp, you can lock the access point to the plate with a padlock (see [Figure 1-2](#)). Compatible padlocks are [Master Lock models 120T and 121T](#) or equivalent.

**Note**

The security hasp adapter covers the cable bay area (including the power port, Ethernet port, console port, and the mode button) to prevent the installation or removal of the cables or the activation of the mode button.

CISCO CONFIDENTIAL - Draft 2

Figure 1-2 Access Point with Security Hasp Adapter



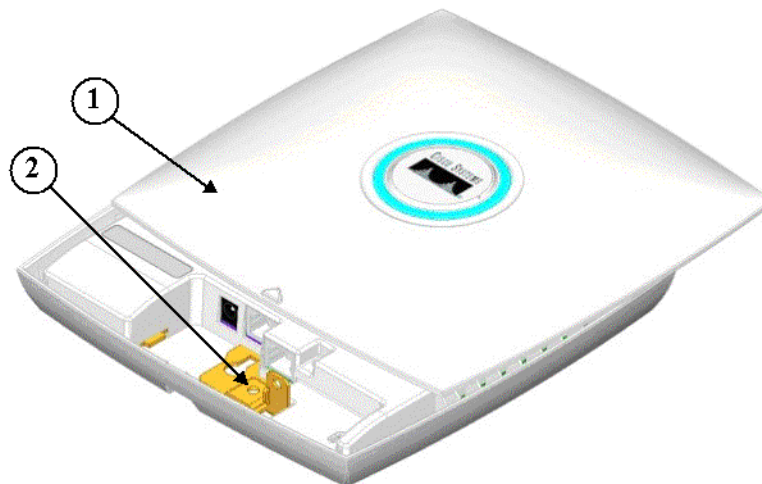
1	Access point cover in open position	3	Security padlock
2	Security hasp adapter		

- Security screw—The access point contains a security screw hole (see [Figure 1-3](#)) that can be used to attach the access point to the mounting plate to restrict access point removal. When a security-type screw (user supplied) is used, access to the mounting screws that attach the mounting plate is greatly restricted.



Note The use of a security-type screw does not restrict access to the access point cables or the mode button.

Figure 1-3 Access Point Security Screw Hole



1	Access point cover in open position	2	Security screw hole
---	-------------------------------------	---	---------------------

CISCO CONFIDENTIAL - Draft 2**UL 2043 Certification**

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

**Caution**

Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space, the AIR-PWRINJ3 power injector and the power module are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

Network Configuration Examples

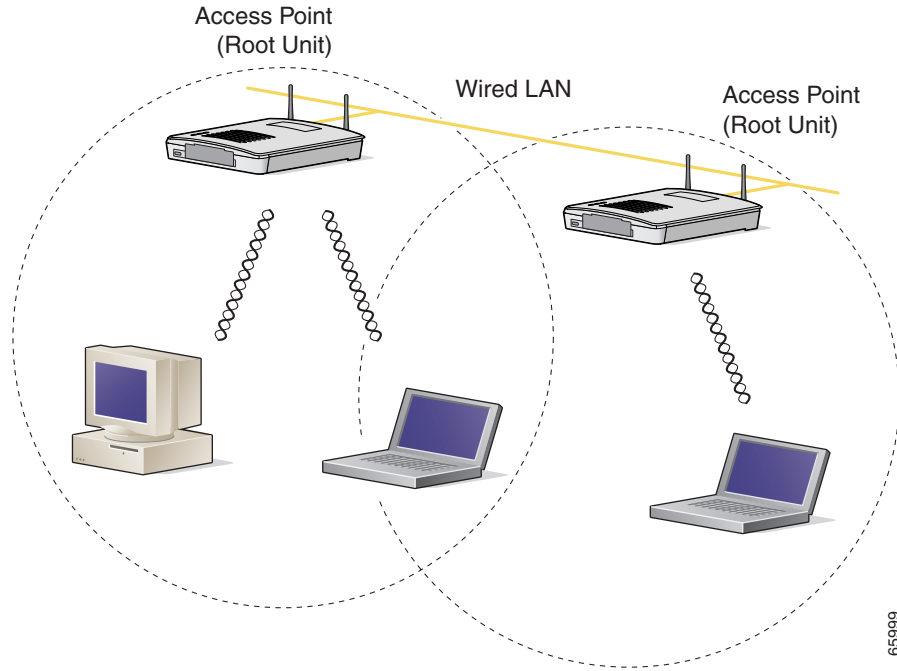
This section describes the access point's role in three common wireless network configurations. The access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

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 1-4](#) shows access points acting as root units on a wired LAN.

CISCO CONFIDENTIAL - Draft 2

Figure 1-4 Access Points as Root Units on a Wired LAN - need new picture



65599

CISCO CONFIDENTIAL - Draft 2

Repeater Unit that Extends Wireless Range

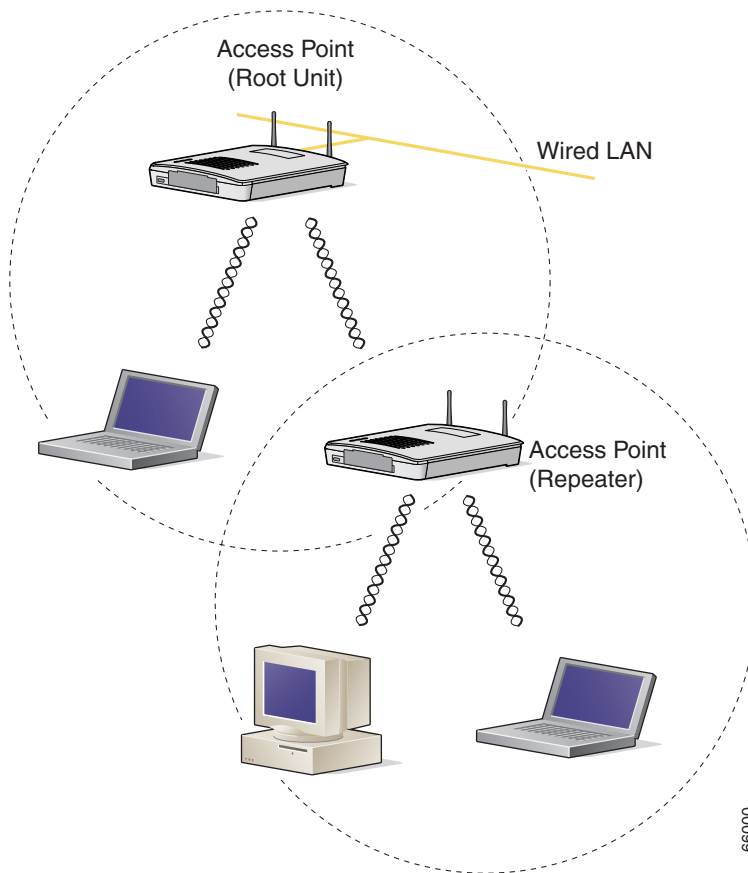
An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. [Figure 1-5](#) 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.

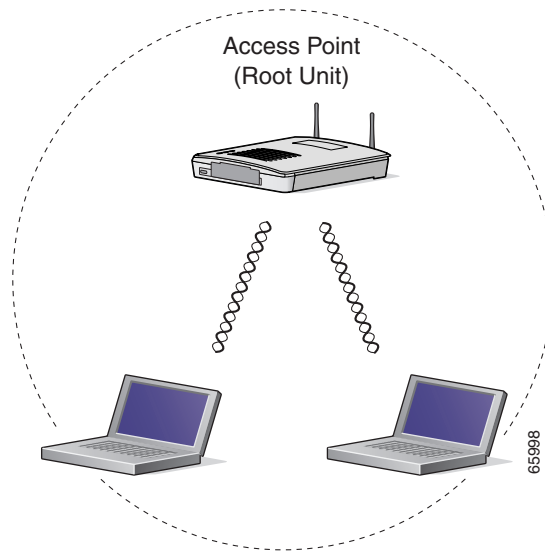
Figure 1-5 Access Point as Repeater - need new picture



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 1-6](#) shows an access point in an all-wireless network.

Figure 1-6 Access Point as Central Unit in All-Wireless Network - need new picture



CISCO CONFIDENTIAL - Draft 2



Installing the Access Point

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

- [Safety Information, page 2-2](#)
- [Warnings, page 2-2](#)
- [Unpacking the Access Point, page 2-3](#)
- [Basic Installation Guidelines, page 2-3](#)
- [Before Beginning the Installation, page 2-4](#)
- [Installation Summary, page 2-7](#)
- [Opening the Access Point Cover, page 2-8](#)
- [Mounting the Access Point, page 2-9](#)
- [Attaching the Access Point to the Mounting Plate, page 2-16](#)
- [Connecting the Ethernet and Power Cables, page 2-17](#)
- [Securing the Access Point, page 2-19](#)
- [Powering Up the Access Point, page 2-21](#)

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 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 1130AG Series Access Point
- Cisco Aironet 1130AG Series Power Module (universal power supply)
- Mounting hardware kit
 - One mounting plate
 - Two suspended ceiling adjustable T-rail clips
 - One security hasp adapter
 - **Four 6x32x¼ inch** flat head Phillips head machine screws
 - **One 8x32x3/16 inch** pan head Phillips head machine screws
 - **2 #8** plastic wall anchors
 - **2 #8x32x1inch** pan head screws
- *Quick Start Guide: Cisco Aironet 1130AG Series Access Point*
- Cisco product registration and Cisco documentation feedback cards

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 interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

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

CISCO CONFIDENTIAL - Draft 2

Before Beginning the Installation

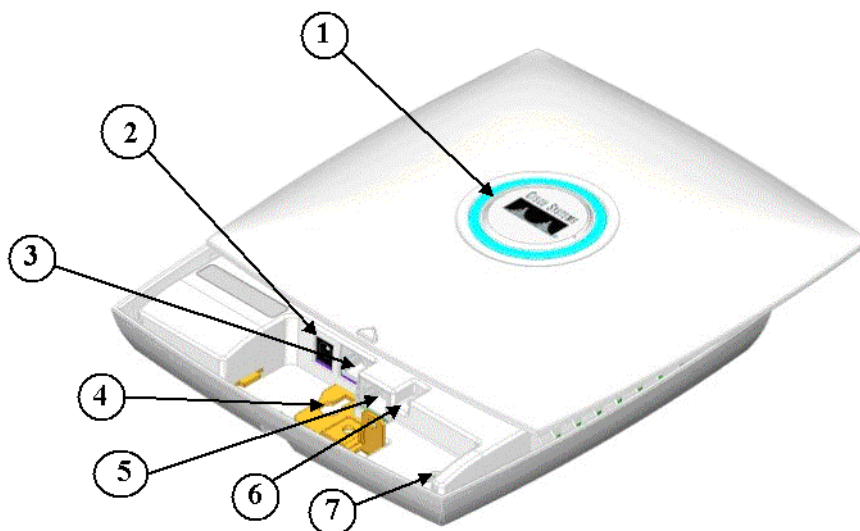
Before you begin the installation process, please refer to these sections to become familiar with the access point and the mounting hardware:

- “Access Point Layout and Connectors” section on page 2-4
- “Mounting Plate” section on page 2-5
- “Suspended Ceiling Adjustable T-Rail Clips” section on page 2-6

Access Point Layout and Connectors

Figure 2-1 identifies the main access point hardware features.

Figure 2-1 Access Point Hardware Features - TBD



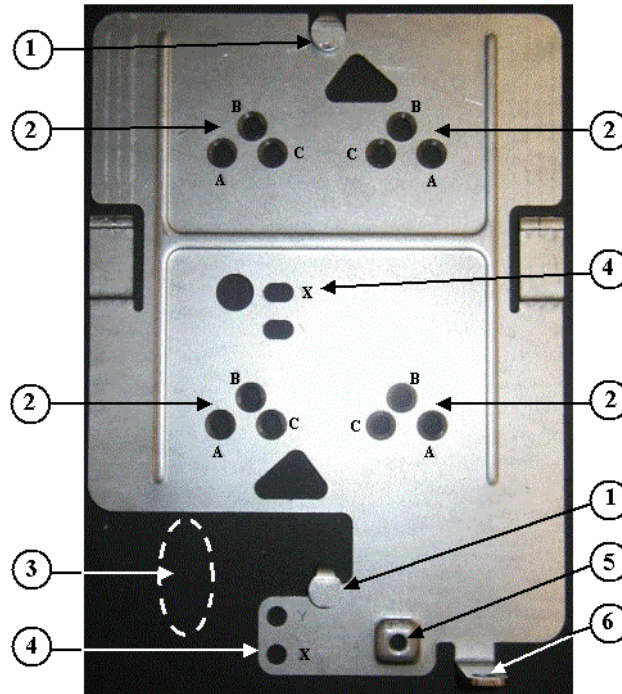
1	Status LED	5	Console port (RJ-45)
2	48-VDC power port	6	Mode button
3	Ethernet port (RJ-45)	7	Ethernet and Radio LEDs
4	Keyhole slot		

**Note**

There is a second keyhole slot located on the bottom of the unit near the security slot.

CISCO CONFIDENTIAL - Draft 2**Mounting Plate**

The access point mounting plate is designed to accommodate multiple mounting methods. The mounting holes on the plate are marked so you can easily identify the correct holes for a specific mounting method. You can use the mounting plate as a template to mark the locations for the cable hole and the mounting holes for your wall or ceiling installation. Refer to [Figure 2-2](#) to locate the various mounting holes for the method you intend to use.

Figure 2-2 Mounting Plate

1	Keyhole clip	4	Screw hole (X)
2	Screw holes (A, B, C)	5	Security screw hole
3	Location for cable access hole	6	Padlock hole

The mounting plate features are described below:

- Keyhole clips—used to attach the access point to the mounting plate. The keyhole clips slide into the access point keyhole slots on the bottom of the unit.
- Screw holes (A, B, C)—used to attach to the suspended ceiling adjustable T-rail clips.
- Screw hole (X)—used to attach to a network cable box, wall, or ceiling. The mounting kit contains two 8x32x1 inch pan head screws and wall anchors for wall or ceiling mounting.
- Security screw hole—used to secure the access point to the mounting plate.



Note You can use a special security screw to restrict the removal of the access point from the mounting plate.

CISCO CONFIDENTIAL - Draft 2

- Padlock hole—used to attach a padlock to secure the access point to the mounting plate. Compatible padlocks are **Master Lock models 120T and 121T** or equivalent. The security hasp adapter can also be used with the padlock for increase security protection.

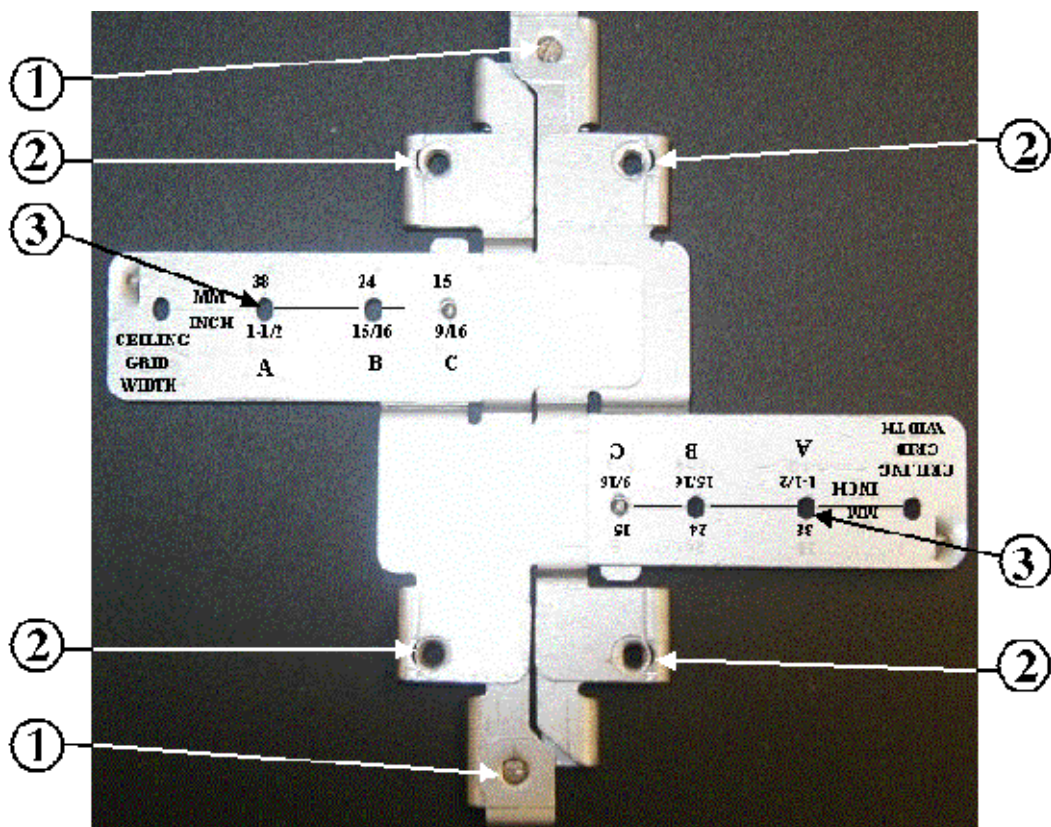


Note The security hasp covers the cable bay area (including the power port, Ethernet port, console port, and the mode button) to prevent the installation or removal of the cables or the activation of the mode button.

Suspended Ceiling Adjustable T-Rail Clips

The accessory kit contains two suspended ceiling adjustable T-rail clips; one for standard ceiling tile rails and the other for recessed ceiling tile rails. The clips are adjustable to accommodate three standard T-rail widths. Each clip contains detents that are used to adjust the clip to the T-rail. Each detent contains markings that indicate the T-rail width and the hole letter that corresponds to the correct mounting holes on the mounting plate. [Figure 2-3](#) shows the details of the adjustable T-rail clips.

Figure 2-3 T-Rail Clip Features



1	Adjustable T-rail clip	3	T-rail locking screw
2	Mounting plate screw holes (8x32 flat head screw)	4	T-rail width adjustment detents (A, B, C) correspond to the A, B, and C holes on the mounting plate

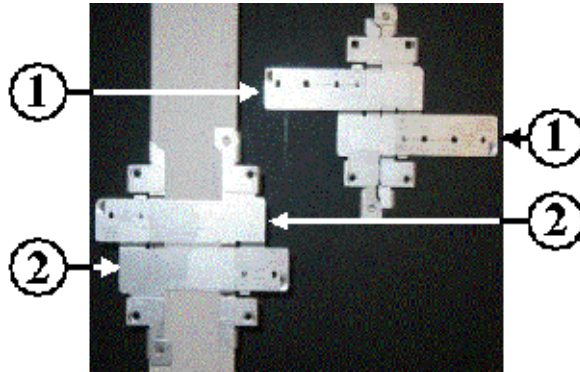
CISCO CONFIDENTIAL - Draft 2

The adjustable T-rail clip attaches to the mounting plate using four 6x32x1/4 inch flat head screws. The A, B, and C holes on the T-rail clips and the mounting plate correspond to these T-rail widths:

- A holes—used for 1 1/2 in (38 mm) T-rails
- B holes—used for 15/16 in (24 mm) T-rails
- C holes—used for 9/16 in (15 mm) T-rails

Figure 2-4 indicates where you should push to open and close the adjustable T-rail clips.

Figure 2-4 Adjusting the T-Rail Clips



1	Push here to open	2	Push here to close
----------	-------------------	----------	--------------------

Installation Summary

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

- Open the access point cover (see [“Opening the Access Point Cover”](#) section on page 2-8).
- Mount the access point on a convenient flat horizontal or vertical surface, such as a desktop, book shelf, file cabinet, wall, ceiling, or suspended ceiling T-rail (see the [“Mounting the Access Point”](#) section on page 2-9).
- Attach the access point to the mounting plate (see the [“Attaching the Access Point to the Mounting Plate”](#) section on page 2-16).
- Connect Ethernet and power cables (see the [“Connecting the Ethernet and Power Cables”](#) section on page 2-17).
- Secure the access point (see the [“Securing the Access Point”](#) section on page 2-19).
- Configure basic settings (refer to [Chapter 3, “Configuring the Access Point for the First Time”](#)).
- Configure security and other access point options (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*).

CISCO CONFIDENTIAL - Draft 2

Opening the Access Point Cover

The top cover provides access to the access point cable bay area containing the power connector, Ethernet port, console serial port, the mode button, and the Ethernet and Radio LEDs.

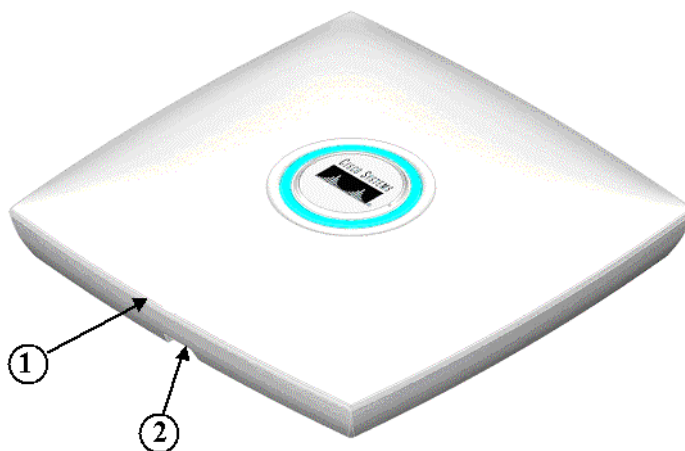
**Caution**

Do not attempt to pry open or lift the top cover of the access point, because you could damage the cover. Carefully read the instructions in this section before attempting to open the access point cover.


The cover is designed to partially open by sliding back from a secured position. Follow these steps to open the top cover:

- Step 1** Locate the cable opening on the end of the unit (see [Figure 2-5](#)).

Figure 2-5 Cable Opening in Access Point Housing



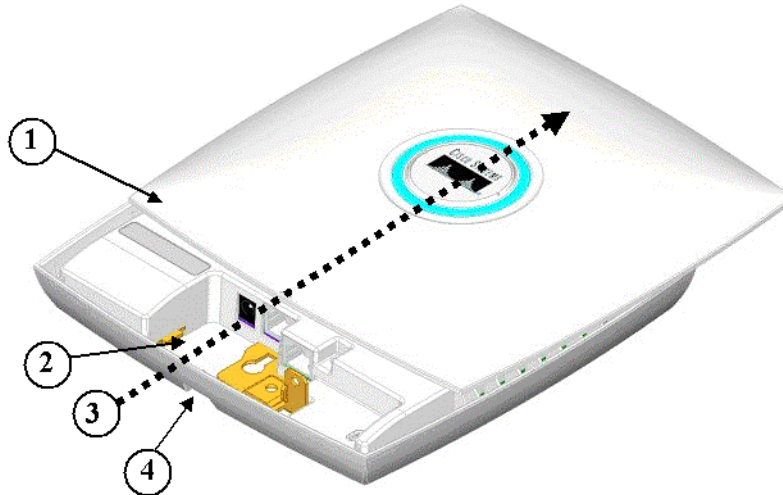
1	Top cover	2	Cable Opening
----------	-----------	----------	---------------

- Step 2** Place your thumb on the top cover (above the triangle mark ) and gently push towards the Status LED.

CISCO CONFIDENTIAL - Draft 2

- Step 3** Continue to slowly slide the cover back across the access point until you reach the cover stop (see [Figure 2-6](#)).

Figure 2-6 *Opening the Access Point Cover*



1	Access point cover (maximum open position)	3	Opening direction
2	Cable bay area	4	Cable opening (in access point housing)

Mounting the Access Point

This section describes the steps necessary to mount the access point using these methods:

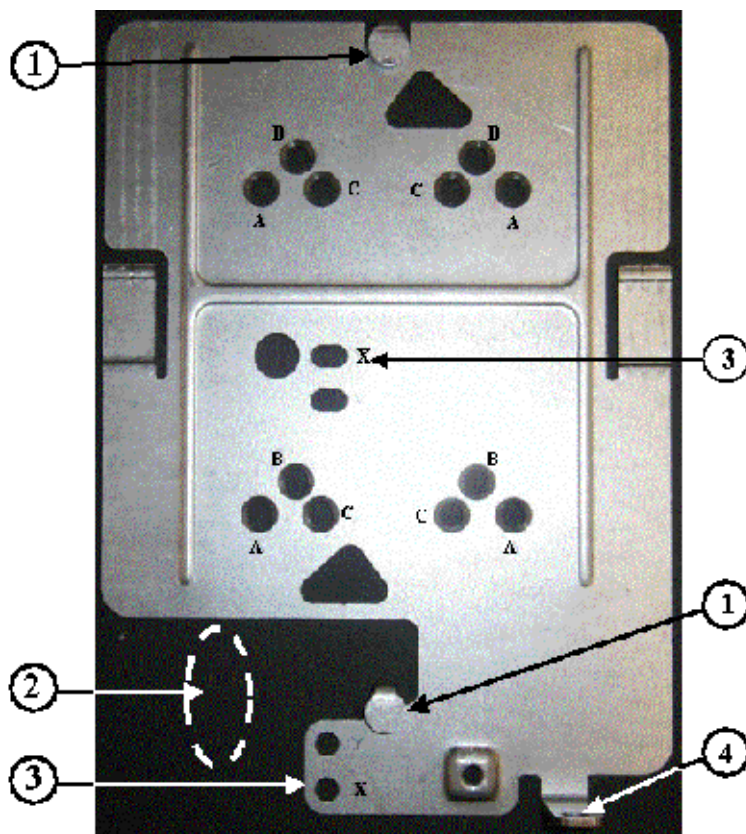
- Horizontal or vertical surface—see the [“Mounting on a Horizontal or Vertical Surface”](#) section on page 2-10
- Under a suspended ceiling—[“Mounting Below a Suspended Ceiling”](#) section on page 2-11
- Network cable box—[“Mounting on a Network Cable Box”](#) section on page 2-14
- Desktop or shelf—see the [“Mounting on a Desktop or Shelf”](#) section on page 2-15

CISCO CONFIDENTIAL - Draft 2**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 plate as a template to mark the locations of the two mounting holes (labeled with an X) and the location of the cable access hole (see [Figure 2-7](#)).

Figure 2-7 Mounting Plate



1	Keyhole clip	3	X mounting hole
2	Cable access hole location	4	Padlock hole

- Step 2** Drill one of the following sized holes at the X mounting hole locations you marked:
- 3/16 in. (4.7 mm) if you are using the supplied wall anchors
 - 1/8 in. (6.3 mm) if you are not using wall anchors
- Step 3** Insert the wall anchors into the mounting holes if you are using them.
- Step 4** If needed, drill or cut a cable access hole large enough for the access point cables and pull the cables through the access hole until you have about 1 foot of exposed cables protruding from the hole.

CISCO CONFIDENTIAL - Draft 2

Step 5 Position the mounting plate over the wall anchors or the drilled holes.

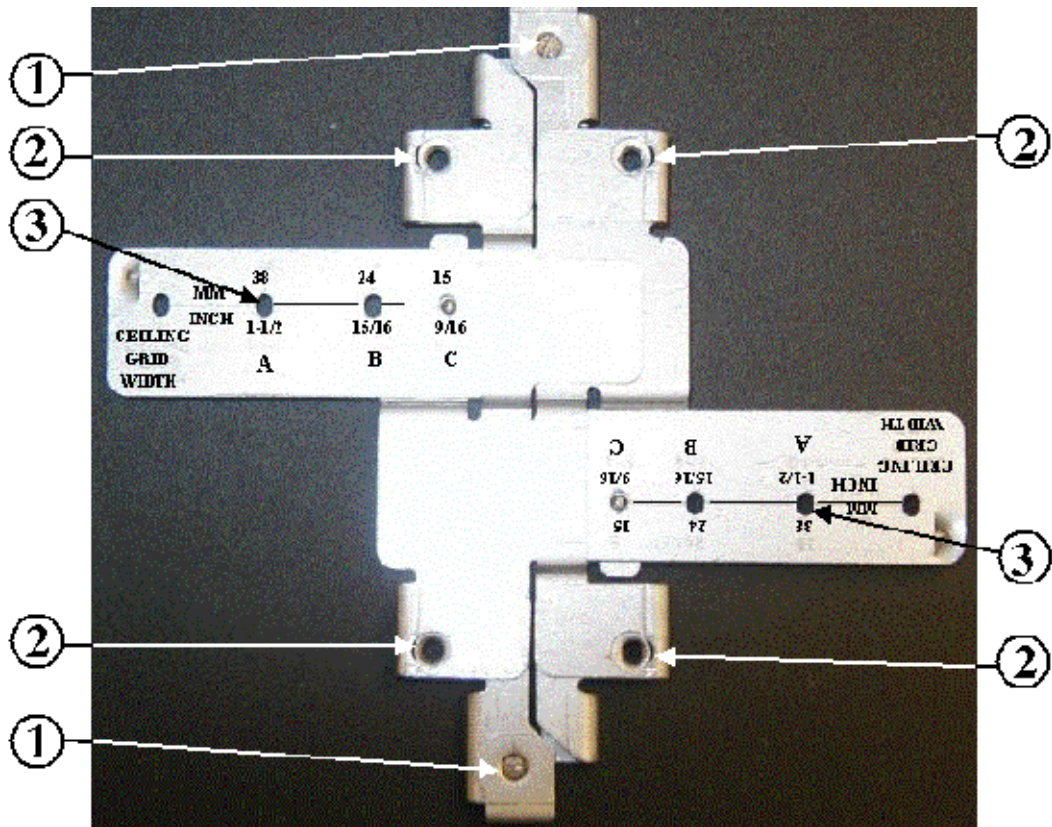
Step 6 Insert two 8x32x1inch pan head screws in the X mounting holes and tightening.

To attach the access point to the mounting plate, see “Attaching the Access Point to the Mounting Plate” section on page 2-16.

Mounting Below a Suspended Ceiling

You should review [Figure 2-8](#) before beginning the mounting process.

Figure 2-8 Adjustable T-Rail Clips



1	T-rail locking set screw	3	T-rail width detents (A, B, or C)
2	Mounting plate screw holes		

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

Step 1 Decide where you want to mount the access point on your suspended ceiling.

Step 2 Select the appropriate adjustable T-rail clip for your suspended ceiling and open the clip to the maximum (see [Figure 2-4](#)).

Step 3 Unscrew the two T-rail locking set screws to enable placing the clip over a T-rail.

CISCO CONFIDENTIAL - Draft 2

- Step 4** Place the T-rail clip over the T-rail and close the T-rail clip (see [Figure 2-4](#)).
- Step 5** Tighten the two T-rail locking set screws to prevent the T-rail clip from moving.
- Step 6** Observe the T-rail width detent letter (A, B, or C) that corresponds to the T-rail width.
- Step 7** Align the corresponding (A, B, or C) holes on the mounting plate over the T-rail mounting plate holes.
- Step 8** Hold the mounting plate and insert a 6x32x1/4 flat head screw into each of the corresponding (A, B, or C) holes and tighten.
- Step 9** If needed, drill or cut a cable access hole (see [Figure 2-7](#)) large enough for the access point cables and pull the cables through the access hole until you have about 1 foot of exposed cables protruding from the hole.

To attach the access point to the mounting plate, see [“Attaching the Access Point to the Mounting Plate” section on page 2-16](#).

CISCO CONFIDENTIAL - Draft 2

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. The access point uses a T-bar box hanger (not supplied) such as the Erico Caddy 512 or B-Line BA12 and should be oriented just above the top surface of a standard 5/8-in. (1.59 cm) ceiling tile. You may need to modify a thicker tile to allow room for the access point.

**Caution**

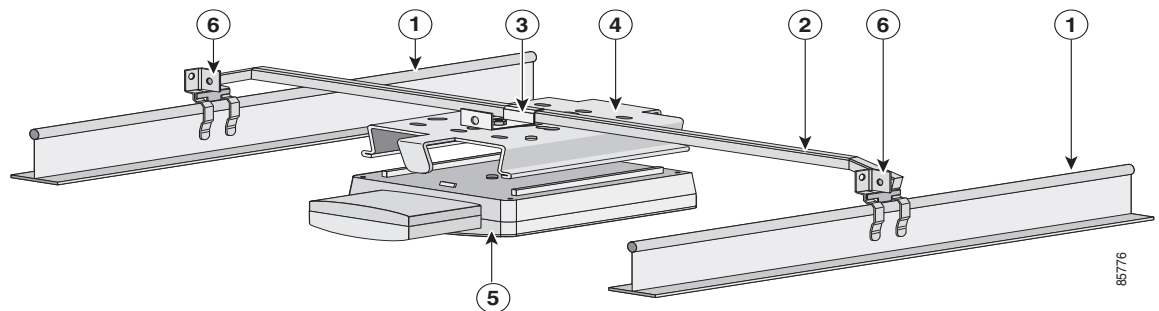
Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space, the AIR-PWRINJ3 power injector and the power module are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

**Caution**

Cisco does not sell Ethernet cable rated for use in a building environmental air space, such as above suspended ceilings. You must obtain special Ethernet cable with the appropriate rating.

Follow these steps to mount the access point above a suspended ceiling. Refer [Figure 2-9](#) before proceeding.

Figure 2-9 T-Bar Grid Mounting Bracket Parts



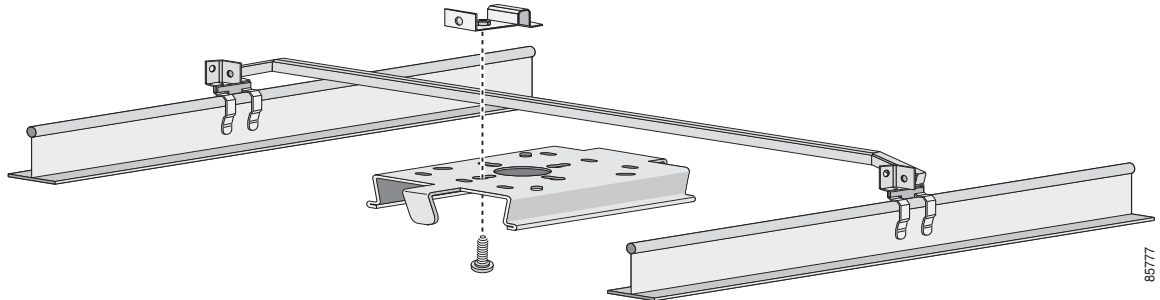
1	Suspended ceiling T-rail	4	Access point mounting bracket
2	T-bar box hanger	5	Access point
3	Bracket mounting clip	6	T-rail clip

Step 1 Insert the bracket mounting clip's tab into the rectangular hole on the access point mounting bracket.

CISCO CONFIDENTIAL - Draft 2

- Step 2** Place the clip over the T-bar box hanger (refer to [Figure 2-10](#)) and secure it to the access point mounting bracket with the 1/4-20 fastener (supplied with the T-bar hanger).

Figure 2-10 T-Bar and Mounting Bracket - TBD



Note [Figure 2-10](#) 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** Remove a ceiling tile adjacent to the mounting location.
- Step 4** Configure the ends of the T-bar box hanger to allow for maximum clearance above the ceiling tile. See the illustration above.
- Step 5** Open the access point cover and connect the Ethernet cable to the access point (see the [“Connecting to an Ethernet Network with an Inline Power Source”](#) section on page 2-18).
- Step 6** Attach the access point to the access point mounting bracket (see the [“Attaching the Access Point to the Mounting Plate”](#) section on page 2-16).
- Step 7** Attach the T-rail clips on the 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 8** Connect a drop wire to a building structural element and 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 9** If you need additional security, you can secure the access point to a nearby immovable object using a Kensington lock and security cable (see the [“Securing the Access Point”](#) section on page 2-19).
- Step 10** Verify that the access point is operating before replacing the ceiling tile.

Mounting on a Network Cable Box

Follow these steps to mount the access point on a network cable box.

- Step 1** Position the mounting plate over the network cable box and align the two mounting holes (labeled with a X) with the network cable box holes.
- Step 2** Hold the mounting plate and insert a 6x32x1/4 flat head screw into each of the X mounting holes and tighten.
- Step 3** Pull the access point cables out of the network box until there is about 1 foot of exposed cables protruding from the box.

CISCO CONFIDENTIAL - Draft 2

To attach the access point to the mounting plate, see [“Attaching the Access Point to the Mounting Plate” section on page 2-16](#).

Mounting on a Desktop or Shelf

When placing the access point on a desktop or shelf, you do not need the mounting plate. The access point has four rubber pads on the bottom to help prevent sliding or scratching the surface of your desktop or shelf. For information on connecting the access point cables, see the [“Connecting the Ethernet and Power Cables” section on page 2-17](#).

Rotating the Cisco Logo

The Cisco logo on the top of the unit can be rotated to correctly position the logo for any mounting arrangement, such as when the unit is mounted on a vertical wall, the logo should be oriented with the Cisco Systems positioned on top. The logo should always be oriented to ease reading.

To rotate the Cisco logo, perform these steps:

-
- Step 1** Place the end of an opened paper clip into one of the holes on the logo assembly (see [Figure 2-11](#)).

Figure 2-11 Cisco Logo Holes

1	Cisco logo	2	Status LED
3	Logo assembly holes		

- Step 2** Using the paper clip as a handle, rotate the logo until you reach the desired orientation.

- Step 3** Remove the paper clip.
-

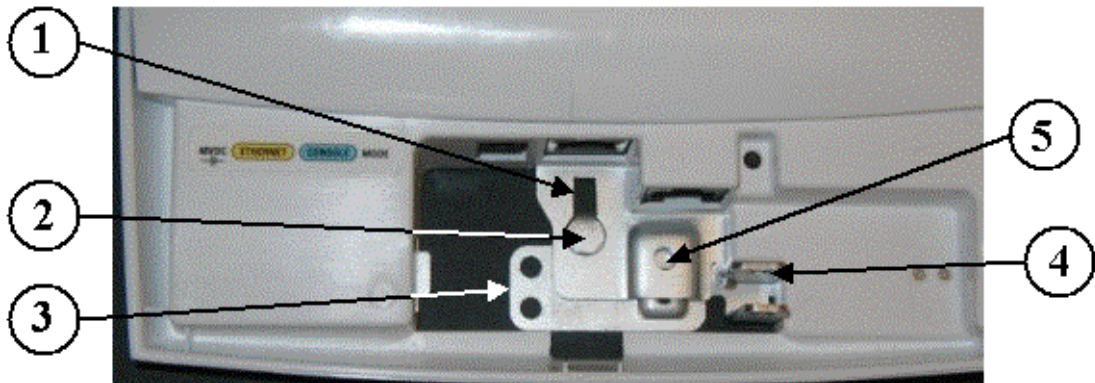
CISCO CONFIDENTIAL - Draft 2

Attaching the Access Point to the Mounting Plate

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

-
- Step 1** Open the access point cover (see the [“Opening the Access Point Cover”](#) section on page 2-8).
 - Step 2** In the cable bay area, pull the cables through one of the access point cable openings (see [Figure 2-6](#)).
 - Step 3** In the cable bay area, line up the visible access point keyhole with the mounting plate keyhole clip located near the security padlock hole (see [Figure 2-12](#)).

Figure 2-12 *Aligning the Keyhole Clip to the Access Point Keyhole*



1	Access point keyhole	4	Security screw hole
2	Mounting plate keyhole clip	5	Padlock hole
3	Mounting plate		

- Step 4** Insert the keyhole clip into the keyhole and maintain a slight pressure to hold the access point in place.
- Step 5** Slightly rotate the access point from side-to-side until you hear the second keyhole clip falling into the other keyhole (not visible).
- Step 6** Slide the access point back over the keyhole clips. You will hear a click when the locking detent contacts the access point and locks it into place.

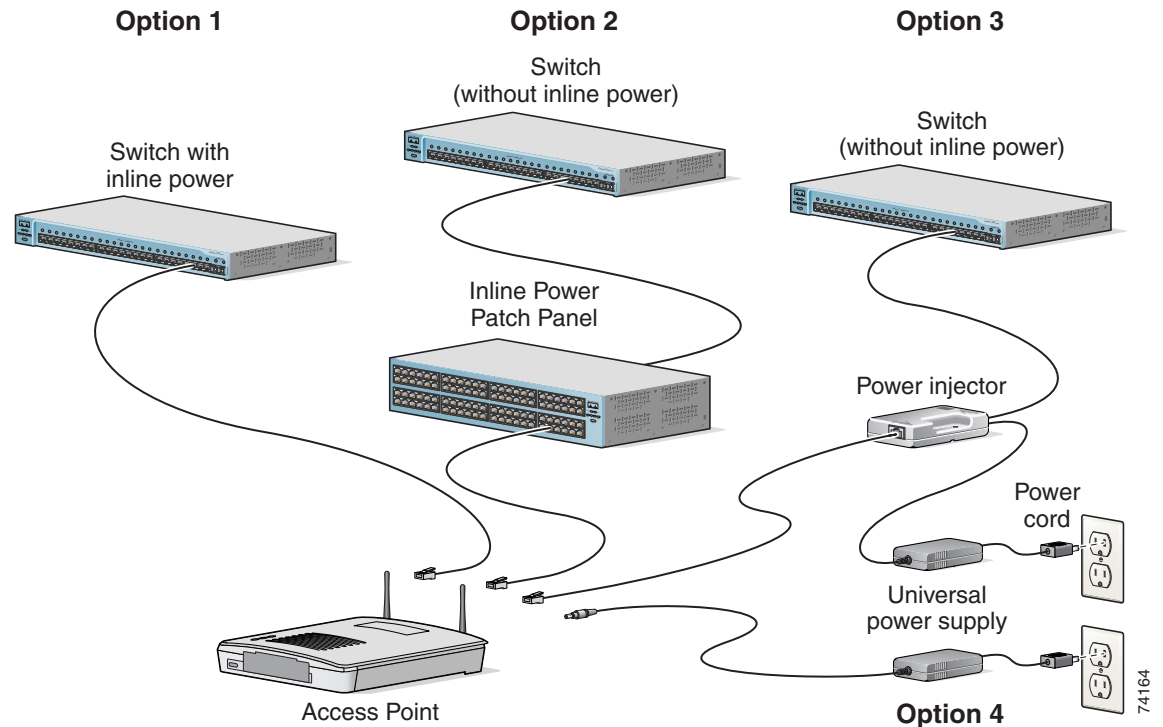
For instructions on connecting your cables, refer to the [“Connecting the Ethernet and Power Cables”](#) section on page 2-17.

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 2-13 shows the power options for the access point.

Figure 2-13 Access Point Power Options - need new picture with Ajax



Warning

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

The access point supports the following power sources:

- Power module (supplied)
- Inline power:
 - Cisco Aironet Power Injector (AIR-PWRINJ3 or AIR-PWRINJ-FIB)
 - An inline power capable switch, such as the Cisco Catalyst 3524 PWR XL, 3560-48PS, 3570-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
 - Other inline power switches supporting the IEEE 802.3af inline power standard



Note

Some switches and patch panels might not provide enough power to operate the access point when configured with both 2.4-GHz and 5-GHz radios. On power-up if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point also activates a Status LED low power error indication and creates an error log entry (refer to the [“Checking the Access Point LEDs”](#) section on page 6-2 and the [“Low Power Condition”](#) section on page 6-5).

CISCO CONFIDENTIAL - Draft 2**Connecting to an Ethernet Network with an Inline Power Source****Caution**

The Cisco Aironet Power Injectors are 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** If necessary, open the access point cover (see the [“Opening the Access Point Cover”](#) section on page 2-8).
- Step 2** Pull the Category 5 Ethernet cable out of the access point cable bay area approximately 1 foot.
- Step 3** Loop the cable back towards the Ethernet connector (see [Figure 2-14](#))

Figure 2-14 Looping the Ethernet Cable



- Step 4** Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point (see [Figure 2-1](#)).
- Step 5** Push or pull the excess cable length (the loop) back through the access point cable bay area.
- Step 6** Close the access point cover by sliding it over the cable bay area until a click is heard.
- Step 7** Connect the other end of the Ethernet cable to one of the following:
- A switch with inline power (see the [“Connecting the Ethernet and Power Cables”](#) section on page 2-17).
 - The end of a Cisco Aironet power injector labeled *To AP/Bridge*. Connect the other end labeled *To Network* to your 10/100 Ethernet LAN.
-

CISCO CONFIDENTIAL - Draft 2

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** If necessary, open the access point cover (see the [“Opening the Access Point Cover”](#) section on page 2-8).
 - Step 2** Pull the Category 5 Ethernet cable and the power module cable out of the access point cable bay area approximately 1 foot.
 - Step 3** Loop the Ethernet cable back towards the access point Ethernet connector (see [Figure 2-14](#)).
 - Step 4** Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point (see [Figure 2-1](#)).
 - Step 5** Loop the power cable back towards the access point 48-VDC power port (see [Figure 2-1](#) for the location of the power port).
 - Step 6** Connect the power module output connector to the access point power port.
 - Step 7** Push or pull the excess cable lengths (both loops) back through the access point cable bay area.
 - Step 8** Close the access point cover by sliding it over the cable bay area until a click is heard.
 - Step 9** Plug the other end of the Ethernet cable into an unpowered Ethernet port on your LAN network.
 - Step 10** Plug the other end of the power module into an approved 100- to 240-VAC outlet.

For information on securing your access point, see the [“Securing the Access Point”](#) section on page 2-19.

Securing the Access Point

The access point supports two methods of restricting the removal of the access point.

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

Using a Security Cable

The access point housing provides a security cable slot to secure the access point using a standard security cable, such as those used on laptop computers. The access point security cable slot is located on one side of the unit.

CISCO CONFIDENTIAL - Draft 2**Securing the Access Point to the Mounting Plate**

The mounting plate contains a security padlock hole and a security screw hole to enable you to secure your access point to the mounting plate to restrict its removal. You can use a security-type screw (that you provide) to attach the access point to the mounting plate using the security screw hole (see [Figure 2-12](#)).

**Note**

Using a security-type screw to secure the access point to the mounting plate does not prevent someone from inserting or removing the access point cables or pressing the mode button.

You can use the security hasp adapter (supplied) and a padlock (that you provide) to secure your access point to the mounting plate. Compatible padlocks are Master Lock models 120T or 121T.

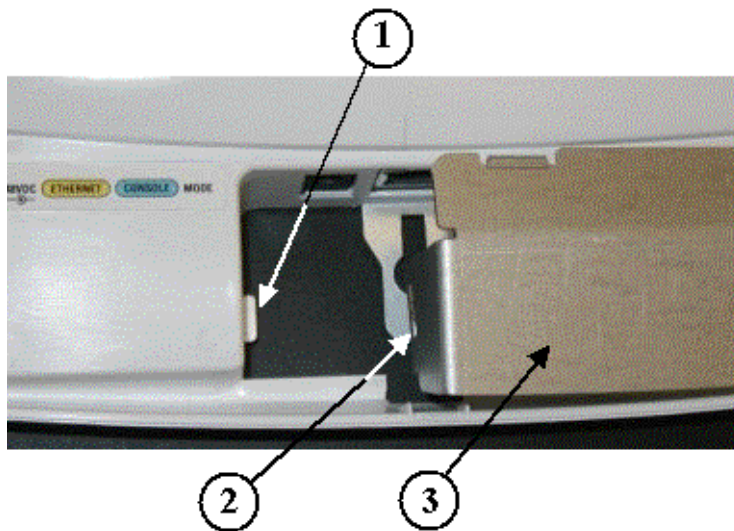
**Note**

The security hasp adapter covers the cable bay area (including the power port, Ethernet port, console port, and the mode button) to prevent the installation or removal of the cables or the activation of the mode button.

Follow these instructions to install the security hasp adapter:

- Step 1** Open the access point cover (see the [“Opening the Access Point Cover”](#) section on page 2-8).
- Step 2** Carefully insert the access point security hasp tab into the notch on the security hasp adapter (see [Figure 2-15](#)).

Figure 2-15 Installing the Security Hasp Adapter



1	Access point security hasp tab	3	Security hasp adapter
2	Security hasp notch		

- Step 3** Push down on the security hasp adapter to ensure the padlock hole is not blocked.
- Step 4** Insert a padlock into the padlock hole and lock the padlock.

CISCO CONFIDENTIAL - Draft 2

- Step 5** Position the padlock into the padlock area.
- Step 6** Close the access point cover by sliding it over the security hasp adapter until you hear a click.
-

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 Status LED on top of the access point. On initial power-up the LED changes colors indicating various POST activities, such as the Status LED turns dark green for about 30 seconds to indicate loading of the Cisco IOS operating system. After a successful power-up sequence, the LED turns light green to signify there are no client devices associated or it turns light blue to signify that there are client devices associated. Refer to [Chapter 6, “Troubleshooting,”](#) for complete LED descriptions.

When the Status LED turns light green or light blue, you are ready to obtain the access point’s IP address and perform an initial configuration. For instructions on assigning basic settings to the access point, refer to [Chapter 3, “Configuring the Access Point for the First Time,”](#)

CISCO CONFIDENTIAL - Draft 2



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 3-9](#)
- [Using the IP Setup Utility, page 3-9](#)
- [Assigning an IP Address Using the CLI, page 3-11](#)
- [Using a Telnet Session to Access the CLI, page 3-11](#)

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 identifiers (SSIDs) for your 802.11g and 02.11a radio networks
- 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

Using the Mode Button

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** Open the access point cover (refer to the [“Opening the Access Point Cover”](#) section on page 2-8).
 - Step 2** Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.
 - Step 3** Press and hold the MODE button while you reconnect power to the access point until the Ethernet LED turns an amber color, approximately 2 to 3 seconds, and release the button. All access point settings return to factory defaults.
-

Using the Web-Browser Interface

Prior to using the web-browser interface, you must have the access point IP address (see the [“Obtaining and Assigning an IP Address”](#) section on page 3-3).

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.

CISCO CONFIDENTIAL - Draft 2

- 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.

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:



Note The access point does not have a default IP address.

- To assign a static IP address to the access point, connect to the access point console port (see the [“Connecting to the Access Point Locally”](#) section on page 3-3) and follow the steps in the [“Assigning an IP Address Using the CLI”](#) section on page 3-11.
- 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 a Cisco IOS CLI command to display the IP address, such as **show interface bvi1**. 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. 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:

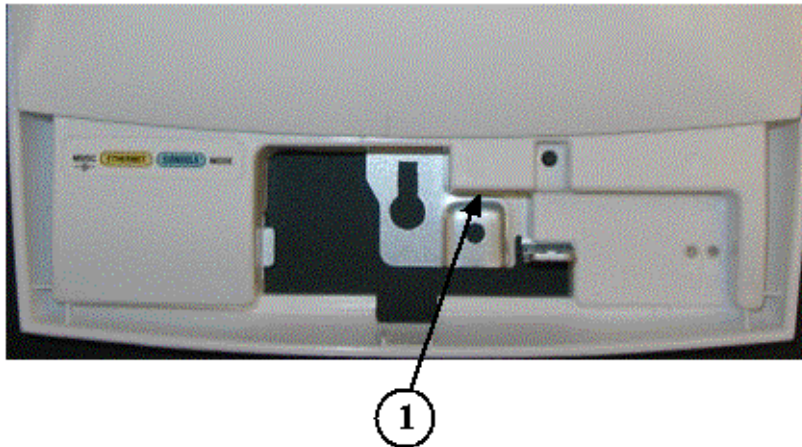
- Step 1** Open the access point cover (refer to [“Opening the Access Point Cover”](#) section on page 2-8).
- Step 2** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 console port on the access point and to the COM port on a computer.

CISCO CONFIDENTIAL - Draft 2**Tip**

If your serial cable enters from the lower cable bay area, you should loop the cable as shown in Figure 2-14.

Figure 3-1 shows the console port location.

Figure 3-1 Console Port Location



1	Console port
---	--------------

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

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.

CISCO CONFIDENTIAL - Draft 2

Figure 3-2 shows the Summary Status page.

Figure 3-2 Summary Status Page

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY +
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

Hostname **ap** ap uptime is 1 day, 56 minutes

Home: Summary Status

Association

Clients: 1	Repeaters: 0
----------------------------	------------------------------

Network Identity

IP Address	10.91.105.48
MAC Address	000b.fcfb.7ce3

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	000b.fcfb.7ce3	100Mb/s
Radio0-802.11G	000b.fcfb.7ee3	54.0Mb/s
Radio1-802.11A	000b.fcfb.7ae3	54.0Mb/s

Event Log

Time	Severity	Description
Mar 1 02:27:29.253	Information	Interface Dot11Radio0, Station KLUMB-LAB1 0040.96a0.b4e0 Associated KEY_MGMT[NONE]
Mar 1 02:27:28.649	Information	Interface Dot11Radio0, Deauthenticating Station 0040.96a0.b4e0 Reason: Disassociated because sending station is leaving (or has left) BSS
Mar 1 02:26:30.173	Information	Interface Dot11Radio0, Station KLUMB-LAB1 0040.96a0.b4e0 Associated KEY_MGMT[NONE]
Mar 1 02:26:19.548	Error	Interface Dot11Radio0, changed state to up
Mar 1 02:26:19.501	Notification	Interface Dot11Radio0, changed state to reset
Mar 1 02:26:19.384	Error	Interface Dot11Radio0, changed state to down
Mar 1 02:26:19.383	Information	Interface Dot11Radio0, Deauthenticating Station 0040.96a0.b4e0 Reason: Previous authentication no longer valid
Mar 1 02:17:04.93...	Information	Interface Dot11Radio0, Station KLUMB-LAB1 0040.96a0.b4e0 Associated KEY_MGMT[NONE]
Mar 1 02:17:03.608	Notification	Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 02:17:02.608	Error	Interface Dot11Radio0, changed state to up

Refresh

OL-6226-01

Cisco Aironet 1130AG Series Access Point Hardware Installation Guide

3-5

CISCO CONFIDENTIAL - Draft 2

Step 5 Click **Express Setup**. The Express Setup screen appears. [Figure 3-3](#) shows the Express Setup page.

Figure 3-3 Express Setup Page

The screenshot displays the Express Setup page for an access point. On the left is a navigation menu with options: HOME, EXPRESS SET-UP (highlighted), EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Express Set-Up' and shows the following configuration details:

- Hostname:** ap (with status: ap uptime is 1 day, 1 hour, 0 minutes)
- System Name:** ap
- MAC Address:** 000b.fcfb.7ce3
- Configuration Server Protocol:** DHCP Static IP
- IP Address:** 10.91.105.48
- IP Subnet Mask:** 255.255.255.0
- Default Gateway:** 0.0.0.0
- Web Server:** Standard (HTTP) Secure (HTTPS)
- SNMP Community:** defaultCommunity
 - Read-Only Read-Write
- Radio0-802.11G:**
 - Role in Radio Network:** Access Point Root Repeater Non-Root
 - Optimize Radio Network for:** Throughput Range Default Custom
 - Aironet Extensions:** Enable Disable
- Radio1-802.11A:**
 - Role in Radio Network:** Access Point Root Repeater Non-Root
 - Optimize Radio Network for:** Throughput Range Default Custom
 - Aironet Extensions:** Enable Disable

At the bottom right, there are 'Apply' and 'Cancel' buttons.

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).

CISCO CONFIDENTIAL - Draft 2

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.



Note You can restore the access point to its factory defaults by unplugging the power jack and plugging it back in while holding the Mode button down until the Ethernet LED turns an amber color (approximately 2 to 3 seconds).

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 Note The access point does not have a default IP address.
IP Subnet Mask	Assigned by DHCP
Default Gateway	Assigned by DHCP
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.

CISCO CONFIDENTIAL - Draft 2

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*)
- 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. The access point must have an IP address before IPSU can be used. This section explains how to install the utility and how to use it to find the access point's IP address.

**Note**

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

**Note**

IPSU can not be used to set the access point IP address or SSID.

**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 1130AG Series (Cisco IOS Software)**.
- Step 4** Click **IPSUvxxxxxx.exe**. The *xxxxxx* 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.

CISCO CONFIDENTIAL - Draft 2

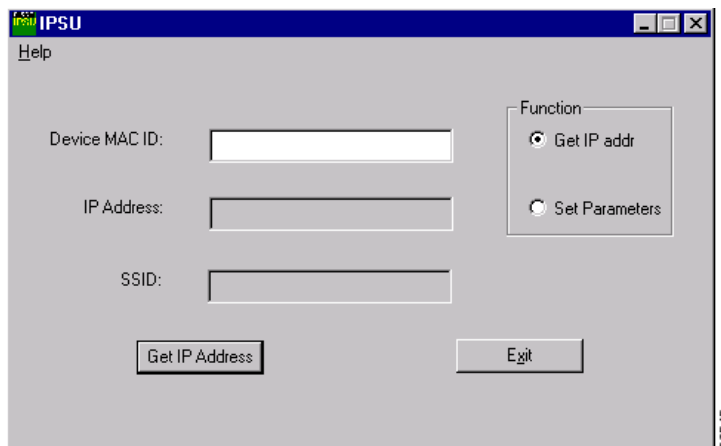
- Step 8** Select the file again to download it.
- Step 9** Download and save the file to a temporary directory on your hard drive and then exit the Internet browser.
- Step 10** Double-click **IPSUvxxxxxx.exe** in the temporary directory to expand the file.
- Step 11** Double-click **Setup.exe** and follow the steps provided by the installation wizard to install IPSU. The IPSU icon appears on your computer desktop.

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 and the access point must have an IP address. 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.

CISCO CONFIDENTIAL - Draft 2

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 <i>address</i> <i>mask</i>	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**.
-

CISCO CONFIDENTIAL - Draft 2



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 your Internet browser.
 - Step 2** Enter the access point's IP address in the browser **Location** field (Netscape Navigator) or **Address** field (Internet Explorer) and press **Enter**. An Enter Network Password screen 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 access point 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.

CISCO CONFIDENTIAL - Draft 2

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

Figure 4-1 Web-Browser Interface Home Page

Hostname **ap** ap uptime is 1 day, 56 minutes

Home: Summary Status

Association

Clients: 1	Repeaters: 0
----------------------------	------------------------------

Network Identity

IP Address	10.91.105.48
MAC Address	000b.fcfb.7ce3

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	000b.fcfb.7ce3	100Mb/s
Radio0-802.11G	000b.fcfb.7ee3	54.0Mb/s
Radio1-802.11A	000b.fcfb.7ae3	54.0Mb/s

Event Log

Time	Severity	Description
Mar 1 02:27:29.253	◆ Information	Interface Dot11Radio0, Station KLUMB-LAB1 0040.96a0.b4e0 Associated KEY_MGMT[NONE]
Mar 1 02:27:28.649	◆ Information	Interface Dot11Radio0, Deauthenticating Station 0040.96a0.b4e0 Reason: Disassociated because sending station is leaving (or has left) BSS
Mar 1 02:26:30.173	◆ Information	Interface Dot11Radio0, Station KLUMB-LAB1 0040.96a0.b4e0 Associated KEY_MGMT[NONE]
Mar 1 02:26:19.548	◆ Error	Interface Dot11Radio0, changed state to up
Mar 1 02:26:19.501	◆ Notification	Interface Dot11Radio0, changed state to reset
Mar 1 02:26:19.384	◆ Error	Interface Dot11Radio0, changed state to down
Mar 1 02:26:19.383	◆ Information	Interface Dot11Radio0, Deauthenticating Station 0040.96a0.b4e0 Reason: Previous authentication no longer valid
Mar 1 02:17:04.93 Dot11Radio0, Station KLUMB-LAB1 0040.96a0.b4e0 Associated KEY_MGMT[NONE]
Mar 1 02:17:03.608	◆ Notification	Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 02:17:02.608	◆ Error	Interface Dot11Radio0, changed state to up

[Refresh](#)

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 is used to quickly configure basic access point settings such as system name, IP address, SNMP community, radio roles, and radio activation or deactivation.
Express Security	Displays the Express Security page that is used to quickly setup basic security settings for both radios such as SSID, VLAN, and the type of security.
Network Map	Displays a list of infrastructure devices on your wireless LAN.
Association	Displays a list of wireless devices associated to your access point, listing their system names, IP address, MAC address, parent-client relationships, and the VLAN.
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 that are used to configure all security options for each radio interface.
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.
Wireless Services	Displays a summary of wireless services used with CCKM and provides links to WDS configuration pages.
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.
Cancel	Discards changes to the page and remains on the page.
Clear	Clears the selected options on the page.
Refresh	Updates status information or statistics displayed on a page.

CISCO CONFIDENTIAL - Draft 2

Character Restrictions in Entry Fields

Because the 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 help and print 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:

- [Cisco 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

Cisco 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. Refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for a list of the supported Cisco IOS commands.

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: <ul style="list-style-type: none"> 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.
<i>abbreviated-command-entry?</i>	Obtains a list of commands that begin with a particular character string. For example: <pre>ap# di? dir disable disconnect</pre>
<i>abbreviated-command-entry<Tab></i>	Completes a partial command name. For example: <pre>ap# sh conf<tab> ap# show configuration</pre>
?	Lists all commands available for a particular command mode. For example: <pre>ap> ?</pre>
<i>command ?</i>	Lists the associated keywords for a command. For example: <pre>ap> show ?</pre>
<i>command keyword ?</i>	Lists the associated arguments for a keyword. For example: <pre>ap(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet</pre>

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.	Return	Scroll down one line.
	Space	Scroll down one screen.
Note The <code>More</code> prompt appears for output that has more lines than can be displayed on the terminal screen, including <code>show</code> command output. You can use the Return and Space bar keystrokes whenever you see the <code>More</code> prompt.		
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



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:

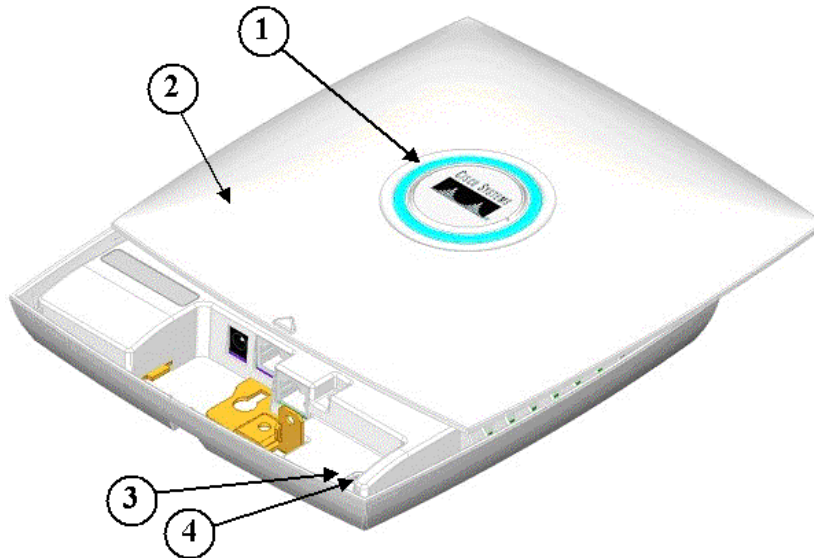
- [Checking the Access Point LEDs, page 6-2](#)
- [Checking Basic Settings, page 6-4](#)
- [Resetting to the Default Configuration, page 6-9](#)
- [Reloading the Access Point Image, page 6-10](#)
- [Obtaining the Access Point Image File, page 6-13](#)
- [Obtaining the TFTP Server Software, page 6-13](#)
- [Running the Carrier Busy Test, page 6-8](#)
- [Running the Ping/Link Test, page 6-8](#)

CISCO CONFIDENTIAL - Draft 2

Checking the Access Point LEDs

If your access point is not working properly, check the Status LED on the top panel or the Ethernet and Radio LEDs in the cable bay area. You can use the LED indications to quickly assess the unit's status. [Figure 6-1](#) shows the access point LEDs.

Figure 6-1 Access Point LEDs



1	Status LED	3	Ethernet LED
2	Access point cover	4	Radio LED

**Note**

To view the Ethernet and Radio LEDs you must open the access point cover (refer to the [“Opening the Access Point Cover”](#) section on page 2-8).

**Note**

When the access point cover is opened, the Status LED colors are not visible.

CISCO CONFIDENTIAL - Draft 2

The LED signals are listed in Table 6-1.

Table 6-1 LED Signals

Message type	Cable Bay Area		Top of Unit	Meaning
	Ethernet LED	Radio LED	Status LED	
Boot loader status	Green	Green	Green	DRAM memory test ok.
	Off	Blinking green	Light Blue	Initialize Flash file system.
	Off	Green	Pink	Flash memory test ok.
	Green	Off	Blue	Ethernet test ok.
	Green	Green	Green	Starting Cisco IOS.
Association status	n/a	n/a	Light green	Normal operating condition, but no wireless client devices are associated with the unit.
	n/a	n/a	Sky blue	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	n/a	n/a	Ethernet link is operational.
	Blinking green	n/a	n/a	Transmitting or receiving Ethernet packets.
	n/a	Blinking green	n/a	Transmitting or receiving radio packets.
	n/a	n/a	Blinking dark blue	Software upgrade in progress
Boot loader warnings	Off	Off	Yellow	Ethernet link not operational.
	Red	Off	Yellow	Ethernet failure.
	Amber	Off	Yellow	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Pink	Image recovery (Mode button pressed for 20 to 30 seconds)
	Blinking green	Blinking red	Blinking pink	Image recovery in progress and Mode button is released.

CISCO CONFIDENTIAL - Draft 2

Message type	Cable Bay Area		Top of Unit	Meaning
	Ethernet LED	Radio LED	Status LED	
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Red	Blinking red and blue	Flash file system failure.
	Off	Amber	Blinking red and light blue	Environment variable (ENVAR) failure.
	Amber	Off	Blinking red and yellow	Bad MAC address.
	Red	Off	Blinking red and off	Ethernet failure during image recovery.
	Amber	Amber	Blinking red and off	Boot environment error.
	Red	Amber	Blinking red and off	No Cisco IOS image file.
	Amber	Amber	Blinking red and off	Boot failure.
Cisco IOS errors	Blinking amber	n/a	n/a	Transmit or receive Ethernet errors.
	n/a	Blinking amber	n/a	Maximum retries or buffer full occurred on the radio.
	Red	Red	Orange	Software failure; try disconnecting and reconnecting unit power.
	n/a	n/a	Orange	General warning, insufficient inline power.
	Blinking green	Blinking green	Blinking green	User activation of location indicator.

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*.

CISCO CONFIDENTIAL - Draft 2

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.

Low Power Condition

The access point can be powered from the 48 VDC power module or from an in-line power source. The access point supports the IEEE 802.3af power standard and the Cisco CDP Power Negotiation protocol for in-line power sources. The access point requires more power (13 watts) than some legacy in-line power sources can supply. On power-up if the access point is unable to determine that the power source can supply sufficient power, the access point automatically enters low power mode and deactivates both radios to prevent an over-current condition. The access point also activates a Status LED low power error indication and creates an error log entry (see the [“Checking the Access Point LEDs”](#) section on page 6-2 and [“Inline Power Status Messages”](#) section on page 6-6).

**Warning**

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

On power up, the access point boots up in low power mode, Cisco IOS software loads and runs, CDP power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on, otherwise the radios remain disabled.

When the access point is in low power mode, the Cisco IOS *show interfaces dot11radio 0* command produces the following results:

```
Dot11Radio0 is up, line protocol is down.
```

CISCO CONFIDENTIAL - Draft 2**CDP Inline Power Negotiation**

The access point uses CDP (Cisco Discovery Protocol) to negotiate with the in-line power source for sufficient power. The results of these negotiations will either be a decision to enter full power mode or to remain in low power mode. Independent of the CDP negotiations, the access point hardware uses the 802.3af classification scheme to report maximum power is required by the access point.

Currently, Cisco switches (802.3af capable) do not support CDP in-line power negotiation. The access point automatically enters normal power mode if a Cisco Catalyst 3550, 3560, or 3570 switch is detected in the received CDP ID field.

When the access point determines that sufficient power is not available for normal power mode an error message is logged and the Status LED turns orange to indicate the low power mode ((see the [“Checking the Access Point LEDs”](#) section on page 6-2 and the [“Inline Power Status Messages”](#) section on page 6-6) .

Inline Power Status Messages

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

- `%CDP_PD-4-POWER_OK: Full power - AC_ADAPTOR inline power source`—This message indicates the access point is using the power module and can support full power.
- `%CDP_PD-4-POWER_OK: Full power - NO_CDP_NON_CISCO inline power source`—This message indicates the access point is operating at full power but is connected to a non-Cisco in-line power source. To prevent possible over-current conditions, this must be an IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.
- `%CDP_PD-4-POWER_OK: Full power - HIGH_POWER_CLASSIC inline power source`—This message indicates the access point is operating at full power and has detected a Cisco switch capable of supplying sufficient power.
- `%CDP_PD-4-POWER_OK: Full power - MIDSPAN inline power source`—This message indicates the access point is operating at full power and the Cisco IOS power in-line negotiation command has been used to indicate a power injector is being used to supply power.
- `%CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source`—This message indicates the access point is operating at full power and power is being supplied by a Cisco switch capable of power negotiation.
- `%CDP_PD-2-POWER_LOW: All radios disabled - LOW_POWER_CLASSIC inline power source platform=AIR-AP1120B-A-K9 MAC address=xxxx.xxxx.xxxx`—This message indicates the access point is in low power mode with all radios disabled and the power source is not capable of in-line power negotiations. The `xxxx.xxxx.xxxx` indicates the MAC address of the power source.
- `%CDP_PD-2-POWER_LOW: All radios disabled - NEGOTIATED inline power source platform=AIR-AP1120B-A-K9 MAC address=xxxx.xxxx.xxxx`—This message indicates the access point is in low power mode with all radios disabled and the power source is incapable of supplying sufficient power. The `xxxx.xxxx.xxxx` indicates the MAC address of the power source.

CISCO CONFIDENTIAL - Draft 2

Inline Power Exception

CDP in-line power negotiation is dependent on similar code being resident in the Cisco switch that is providing power. However, not every switch supports this CDP power negotiation code. As a work around for such pre-standard switches the following Cisco IOS CLI command is required:

```
(config)# [no] power inline negotiation {prestandard source | injector H.H.H}
```

You can use this Cisco IOS CLI command to inform the access point that the power source is an 802.3af compliant Cisco switch or that a power injector is being used to supply sufficient power. Refer to [Table 6-2](#) for information on when to use this special Cisco IOS command.

**Caution**

If the access point receives power through Power-over-Ethernet (PoE), the output current of the power sourcing equipment (PSE) cannot exceed 400 mA or 1500 V per port, whichever is smaller. The power source must comply with IEEE802.3af or IEC60950 for limited power sources.

Table 6-2 Special Cisco IOS Command

Power Source	Cisco IOS Command
AC power module	None required
Power injector ¹	For Cisco non-802.3af compliant switches and Cisco switches without inline power, use this Cisco IOS command: power inline negotiation injector xxxx.xxxx.xxxx (where xxxx.xxxx.xxxx is the MAC address of the switch port to which the access point is connected.)
Cisco 802.3af compliant switch ²	Use this Cisco IOS command: power inline negotiation prestandard source

1. Power injector must be AIR-PWRINJ3 or AIR-PWRINJ-FIB.

2. If command 2 is not issued when powered only by a Cisco non-802.3af compliant switch, the access point powers up with both radio interfaces down.

Issuing the Cisco IOS Command

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

-
- Step 1** Connect a PC to the access point console port and use a terminal emulator to establish a session with the access point (refer to the [“Connecting to the Access Point Locally”](#) section on page 3-3).
- Step 2** From the Privileged EXEC mode (refer to the [“Cisco IOS Command Modes”](#) section on page 5-2), enter one of these commands that applies to your power configuration (see [Table 6-2](#)):
- **power inline negotiation injector xxxx.xxxx.xxxx**
(where xxxx.xxxx.xxxx is the MAC address of the switch port to which the access point is connected.)
 - **power inline negotiation prestandard source**
- Step 3** Enter the **write memory** command to save the setting to the access point memory.
- Step 4** Enter the **quit** command to exit the terminal session.
-

CISCO CONFIDENTIAL - Draft 2

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 over several days to obtain the best results and to avoid temporary activity spikes.

**Note**

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

**Note**

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

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 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 link to and from 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.

CISCO CONFIDENTIAL - Draft 2

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**.

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

Resetting to the Default Configuration

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

**Note**

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

Using the MODE Button

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

Step 1 Open the access point cover (refer to the [“Opening the Access Point Cover”](#) section on page 2-8).

Step 2 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 3 Press and hold the **MODE** button while you reconnect power to the access point.

Step 4 Hold the **MODE** button until the Ethernet LED turns an amber color (approximately 2 to 3 seconds), and release the button.

Step 5 After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.

**Note**

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

CISCO CONFIDENTIAL - Draft 2

Using the Web Browser Interface

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

-
- Step 1** Open your Internet browser. 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.
 - Step 7** Click the **Reset to Defaults** button.



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

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

Reloading the Access Point Image

If your access point has a firmware failure, you must reload the complete access point image file using the Web browser interface or by 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.

CISCO CONFIDENTIAL - Draft 2

Using the MODE Button

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

**Note**

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

**Note**

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

Follow these steps to reload the access point image file:

- Step 1** The PC you intend to use must be configured with a static IP address between 10.0.0.2 and 10.0.0.30.
- Step 2** Place a copy of the access point image file (such as c1130-k9w7-tar.122-15.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 **c1130-k9w7-tar.default**.
- Step 4** Activate the TFTP server.
- Step 5** If using in-line power, use a Category 5 (CAT5) Ethernet cable to connect your PC to the **To Network** Ethernet connector on the power injector.
- Step 6** Open the access point cover (refer to the [“Opening the Access Point Cover”](#) section on page 2-8).
- Step 7** Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.
- Step 8** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 9** Hold the **MODE** button until the Radio LED turns a red color (approximately 20 to 30 seconds), and release the **MODE** button.
- Step 10** After the access point reboots, you must reconfigure the access point by using the Web interface, the Telnet interface, or Cisco IOS commands.

CISCO CONFIDENTIAL - Draft 2

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 these instructions 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 c1130-k9w7-tar.122-15.JA.tar) on your PC.
 - Step 7** Click the **Upload** button.

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

Browser TFTP Interface

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

-
- Step 1** Open your Internet browser. 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.

CISCO CONFIDENTIAL - Draft 2

- Step 8** Enter the file name for the access point image file (such as c1130-k9w7-tar.122-15.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

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**.
- Step 3** Find the access point firmware and utilities section and click **Cisco Aironet 1130 Series (Cisco IOS Software)**.
- Step 4** Click on the access point image file, such as c1130-k9w7-tar.122-15.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.
-

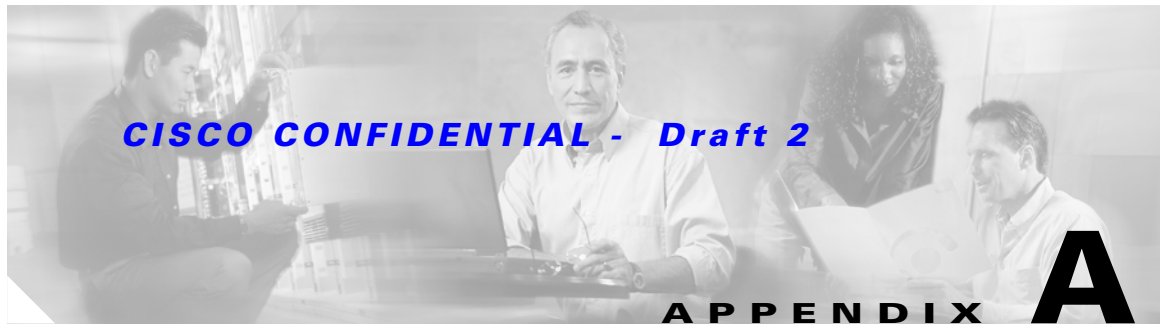
Obtaining the TFTP Server Software

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.

CISCO CONFIDENTIAL - Draft 2



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 onbeschermden 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 frequência 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 közbén 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 oikosulkusuojuuksesta (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 verneenheter 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 1130 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****Model:**

AIR-AP1131AG-A-K9

FCC Certification number:

LDK102054

Manufacturer:

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

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

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

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

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

**Caution**

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

**Caution**

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

CISCO CONFIDENTIAL - Draft 2**Department of Communications—Canada****Model:**

AIR-AP1131AG-A-K9

Certification number:

2461B-102054

Canadian Compliance Statement

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

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

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

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

Cisco Aironet 2.4-GHz Access Points are certified to the requirements of RSS-210 for 2.4-GHz spread spectrum devices, and Cisco Aironet 54-Mbps, 5-GHz Access Points are certified to the requirements of RSS-210 for 5-GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

European Community, Switzerland, Norway, Iceland, and Liechtenstein**Model:**

AIR-AP1131AG-E-K9

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 entprecheneden 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.

CISCO CONFIDENTIAL - Draft 2

Español:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/EC.
Ελληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιαστικές απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes 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-direktiv 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.

For 2.4 GHz radios, the following standards were applied:

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

**Note**

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

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

CISCO CONFIDENTIAL - Draft 2

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



Declaration of Conformity for RF Exposure

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

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

**Note**

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

CISCO CONFIDENTIAL - Draft 2

Guidelines for Operating Cisco Aironet Access Points in Japan

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

Model:

AIR-AP1131AG-J-K9

Japanese Translation

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

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

連絡先 : 03-5549-6500

43768

English Translation

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

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

Contact Number: 03-5549-6500

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>

CISCO CONFIDENTIAL - Draft 2




Access Point Specifications

This appendix provides technical specifications for the Cisco Aironet 1130AG Series Access Point. [Table C-1](#) lists the technical specifications for the access point.

Table C-1 Access Point Specifications

Category	802.11b Radio Specifications	802.11g Radio Specifications	802.11a Radio Specifications
Size	7.53 in. W x 7.53 in. D x 1.31 in. H 19.13 cm W x 19.13 cm D x 3.33 cm H		
Indicators	Tri-color Status LED indicator on the top panel and two bi-color LED indicators (radio and Ethernet) in the cable bay		
Connectors	Cable bay (left to right) 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.		
Input Voltage	48 VDC (nominal)		
Input Power	12.95 W (typical)		
Operating Temperature	Base unit: 32 to 104°F (0 to 40°C) 1130 series power injector: 32 to 104°F (0 to 40°C) 1130 series power module: 32 to 104°F (0 to 40°C)		
Storage Temperature	TBD to TBD°F (TBD to TBD°C)		
Weight	Without mounting hardware: 1.48 lbs (0.67 kg)		

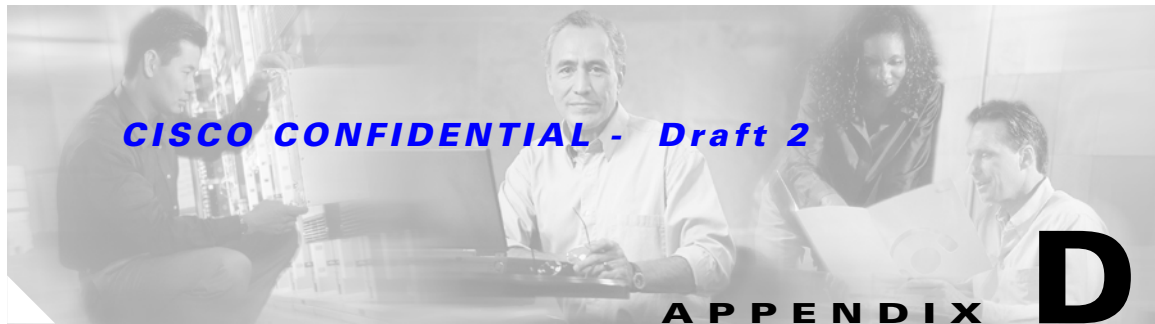
CISCO CONFIDENTIAL - Draft 2**Table C-1 Access Point Specifications (continued)**

Category	802.11b Radio Specifications	802.11g Radio Specifications	802.11a Radio Specifications
Power Output	100 mW (20 dBm) 50 mW (17 dBm) 25 mW (14 dBm) 10 mW (11 dBm) 5 mW (8 dBm) 3 mW (5 dBm) 1 mW (2 dBm) 0.5 mW (-1 dBm) (Depending on the regulatory domain in which the access point is installed)	50 mW (17 dBm) 25 mW (14 dBm) 10 mW (11 dBm) 5 mW (8 dBm) 3 mW (5 dBm) 1 mW (2 dBm) 0.5 mW (-1 dBm) (Depending on the regulatory domain in which the access point is installed)	50 mW (17 dBm) 30 mW (15 dBm) 25 mW (14 dBm) 10 mW (11 dBm) 5 mW (8 dBm) 3 mW (5 dBm) 1 mW (2 dBm) 0.5 mW (-1 dBm) (Depending on the regulatory domain in which the access point is installed)
Antenna	A diversity system with two integrated 4-dBi antennas.		A diversity system with two integrated 4-dBi antennas.
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)		5.15 to 5.25 GHz 5.25 to 5.35 GHz 5.725 to 5.85 GHz (Depending on the regulatory domain in which the access point is installed)
Modulation	Complementary Code Keying (CCK)	Orthogonal Frequency Division Multiplex (OFDM)	
Subcarrier modulation	BPSK (1 Mbps) QPSK (2 Mbps) CCK (5.5 and 11 Mbps)	BPSK (6 and 9 Mbps) QPSK (12 and 18 Mbps) 16-QAM (24 and 36 Mbps) 64-QAM (48 and 54 Mbps)	BPSK (6 Mbps and 9 Mbps) QPSK (12 Mbps and 18 Mbps) 16-QAM (24 and 36 Mbps) 64-QAM (48 and 54 Mbps)
Data rates	1, 2, 5.5, and 11 Mbps	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	
Typical indoor range	320 ft at 1 Mbps 130 ft at 11 Mbps	170 ft at 6 Mbps 80 ft at 54 Mbps	175 ft at 6 Mbps 50 ft at 54 Mbps
Compliance	Complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings.		
	 <p>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; the AIR-PWRINJ3 power injector and the power module are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.</p>		
Safety	Designed to meet: <ul style="list-style-type: none"> • CSN/CSA 22.2 No. 60950 • UL 2043 (Plenum rating) • UL 60950 Third Edition • IEC 60950 Second Edition, including Amendments 1-4 with all deviations • EN 60950 Second Edition, including Amendments 1-4 		

CISCO CONFIDENTIAL - Draft 2**Table C-1 Access Point Specifications (continued)**

Category	802.11b Radio Specifications	802.11g Radio Specifications	802.11a Radio Specifications
Radio Approvals	FCC Parts 15.247 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 301.489-1 EN 301.489-17		
RF Exposure	OET-65C RSS-102 ANSI C95.1		

CISCO CONFIDENTIAL - Draft 2



Channels and Power Levels

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

The following topic is covered in this appendix:

- [Channels and Maximum Power Levels, page D-2](#)

CISCO CONFIDENTIAL - Draft 2**Channels and Maximum Power Levels****IEEE 802.11b/g (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-1](#) indicates the channel identifiers, channel center frequencies, and maximum power levels for each channel allowed by the regulatory domains:

Table D-1 Channels and Maximum Conducted Power for the 802.11b/g Radio

Channel Identifier	Center Frequency (MHz)	Maximum Conducted Power Levels (dBm) in the Regulatory Domains									
		Americas (-A)		China (-C)		EMEA (-E)		Japan (-J)		North American (-N)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	20	17	14	14	14	14	14	14	20	17
2	2417	20	17	14	14	14	14	14	14	20	17
3	2422	20	17	14	14	14	14	14	14	20	17
4	2427	20	17	14	14	14	14	14	14	20	17
5	2432	20	17	14	14	14	14	14	14	20	17
6	2437	20	17	14	14	14	14	14	14	20	17
7	2442	20	17	14	14	14	14	14	14	20	17
8	2447	20	17	14	14	14	14	14	14	20	17
9	2452	20	17	14	14	14	14	14	14	20	17
10	2457	20	17	14	14	14	14	14	14	20	17
11	2462	20	17	14	14	14	14	14	14	20	17
12	2467	–	–	14	14	14	14	14	14	–	–
13	2472	–	–	14	14	14	14	14	14	–	–
14	2484	–	–	–	–	–	–	14	–	–	–

CISCO CONFIDENTIAL - Draft 2**IEEE 802.11a (5-GHz Band)**

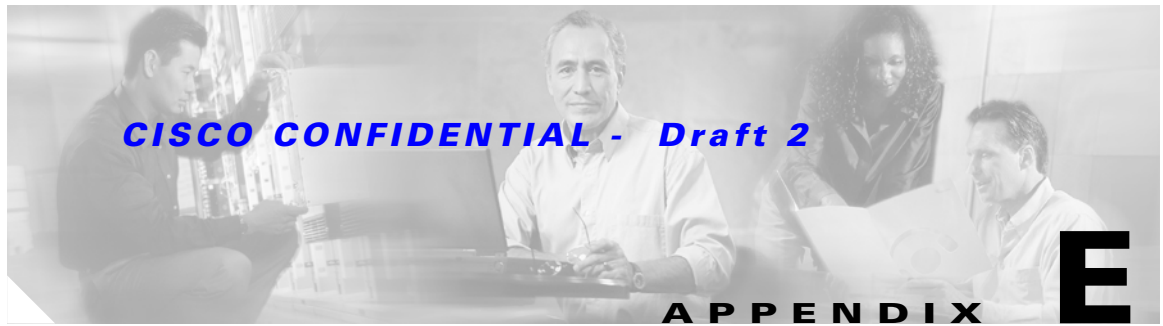
An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. All channel sets are restricted to indoor usage except the Americas (-A), which allows for indoor and outdoor use on channels 52 through 64 in the United States.

Table D-2 indicates the channel identifiers, channel center frequencies, and maximum power levels for each IEEE 802.11a 20-MHz-wide channel allowed by the regulatory domains:

Table D-2 Channels for IEEE 802.11a Radio

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

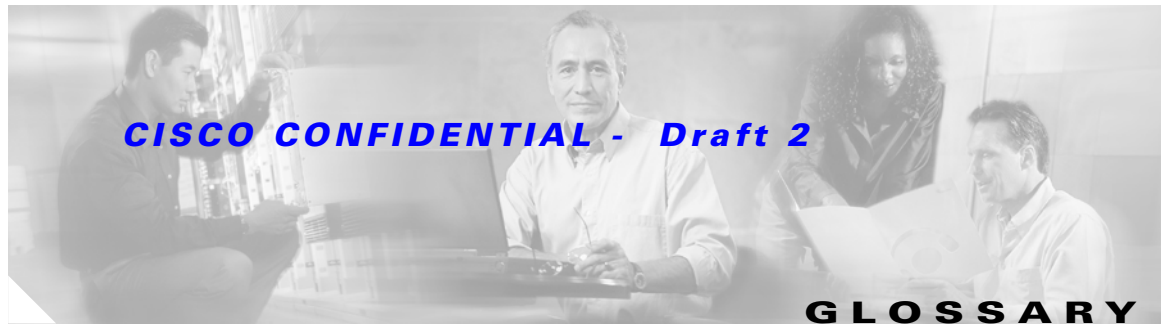
Both the Ethernet and console ports use RJ-45 connectors. Be careful to avoid accidentally connecting the serial cable to the Ethernet port connector.

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.
-----------------------	--

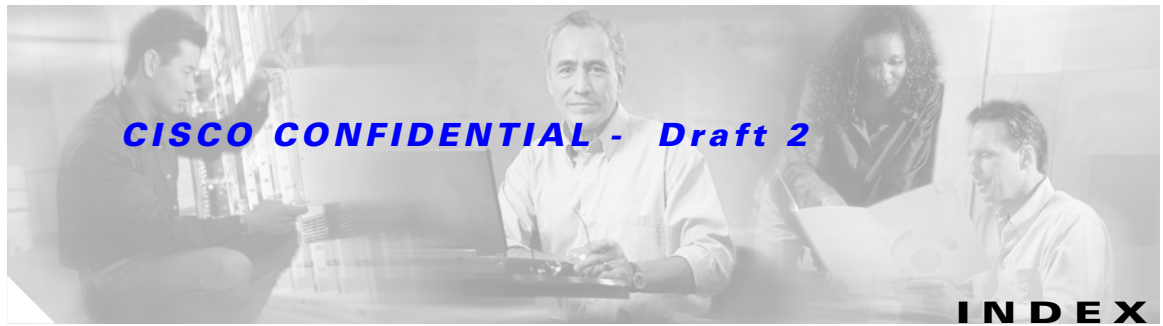
U

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 client adapter.

CISCO CONFIDENTIAL - Draft 2



A

- abbreviating commands [5-3](#)
- access point image [6-10](#)
- antenna
 - connectors [C-2](#)
- Apply button [4-4](#)

B

- basic settings, checking [6-4](#)

C

- Cancel button [4-4](#)
- Cisco TAC [6-1](#)
- CLI
 - abbreviating commands [5-3](#)
 - command modes [5-2](#)
 - editing features
 - enabling and disabling [5-6](#)
 - keystroke editing [5-7](#)
 - 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-2](#)
- declarations of conformity [B-1](#)
- default, configuration, resetting [6-9](#)
- default commands [5-3](#)

E

- editing features
 - enabling and disabling [5-6](#)
 - keystrokes used [5-6](#)
 - wrapped lines [5-7](#)
- EIRP, maximum [D-2 to ??, D-3 to ??](#)
- error messages, during command entry [5-4](#)
- extended temperature range [2-3, 2-4](#)

F

- FCC Declaration of Conformity [B-2](#)
- FCC Safety Compliance [2-2](#)
- filtering
 - show and more command output [5-8](#)
- frequencies [D-2, D-3](#)

CISCO CONFIDENTIAL - Draft 2

frequency range [C-2](#)

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 [6-2](#)

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](#)

M

MAC [3-10](#)

management options, CLI [5-1](#)

Mode button [6-11](#)

modulation [C-2](#)

N

no commands [5-3](#)

O

OK button [4-4](#)

operating temperature [C-1](#)

P

package contents [2-3](#)

password reset [6-9](#)

pinouts, serial cable [E-2](#)

power

- connecting [2-17](#)

- input [C-1](#)

- output [C-2](#)

power level, maximum [D-2](#)

privileged EXEC mode [5-2](#)

R

range, radio [C-2](#)

regulatory

- domains [D-2, D-3](#)

regulatory information [B-1](#)

reloading access point image [6-10](#)

RF exposure [B-5](#)

S

safety warnings, translated [A-1](#)

serial

- cable [E-2](#)

- Cisco cable [E-2](#)

size [C-1](#)

SSH Communications Security, Ltd. [5-9](#)

CISCO CONFIDENTIAL - Draft 2

status indicators **C-1**
storage temperature **C-1**

T

TAC **6-1**
Telnet **3-11**
temperature
 operating **C-1**
 storage **C-1**
terminal emulator **3-4**
TFTP server **6-11**
troubleshooting **6-1**

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, 6-13**
weight **C-1**
WEP key **6-5**

CISCO CONFIDENTIAL - Draft 2