



## **Cisco Aironet 1130AG Series Access Point Hardware Installation Guide**

April 2005

### **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

Text Part Number: OL-6226-02



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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

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

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

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

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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, 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, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, 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, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)



## **Preface ix**

Audience	ix
Purpose	ix
Organization	ix
Conventions	x
Related Publications	xii
Obtaining Documentation	xii
Cisco.com	xii
Documentation DVD	xiii
Ordering Documentation	xiii
Documentation Feedback	xiii
Cisco Product Security Overview	xiv
Reporting Security Problems in Cisco Products	xiv
Obtaining Technical Assistance	xv
Cisco Technical Support Website	xv
Locating the Product Serial Number	xvi
Submitting a Service Request	xvii
Definitions of Service Request Severity	xvii
Obtaining Additional Publications and Information	xvii

## **Overview 1-1**

Hardware Features	1-2
Dual-Radio Operation	1-3
Ethernet Port	1-3
Console Port	1-3
LEDs	1-3
Power Sources	1-4
UL 2043 Certification	1-4
Anti-Theft Features	1-5
Network Configuration Examples	1-7
Root Unit on a Wired LAN	1-7
Repeater Unit that Extends Wireless Range	1-8
Central Unit in an All-Wireless Network	1-9

<b>Installing the Access Point</b>	<b>2-1</b>
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	2-7
Installation Summary	2-8
Opening the Access Point Cover	2-9
Mounting the Access Point on a Horizontal or Vertical Surface	2-10
Mounting the Access Point Below a Suspended Ceiling	2-12
Mounting the Access Point Above a Suspended Ceiling	2-13
Mounting Access Point on a Network Cable Box	2-15
Mounting Access Point on a Desktop or Shelf	2-15
Attaching the Access Point to the Mounting Plate	2-15
Securing the Access Point	2-17
Using a Security Cable	2-17
Securing the Access Point to the Mounting Plate	2-18
Connecting the Ethernet and Power Cables	2-20
Connecting to an Ethernet Network with an Inline Power Source	2-21
Connecting to an Ethernet Network with Local Power	2-22
Rotating the Cisco Logo	2-23
Powering Up the Access Point	2-24
<b>Configuring the Access Point for the First Time</b>	<b>3-1</b>
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	3-3
Default IP Address Behavior	3-3
Default SSID and Radio Behavior	3-3

Obtaining and Assigning an IP Address	3-4
Connecting to the Access Point Locally	3-4
Assigning Basic Settings	3-5
Default Settings on the Express Setup Page	3-9
Enabling the Radio Interfaces	3-9
Configuring Basic Security Settings	3-10
Understanding Express Security Settings	3-11
Using VLANs	3-11
Express Security Types	3-11
Express Security Limitations	3-12
Using the Express Security Page	3-13
Finding the IP Address Using the CLI	3-13
Assigning an IP Address Using the CLI	3-14
Using a Terminal Emulator to Access the CLI	3-14
Using a Telnet Session to Access the CLI	3-15
<b>Using the Web-Browser Interface</b>	<b>4-1</b>
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	4-3
Character Restrictions in Entry Fields	4-5
Using Online Help	4-5
<b>Using the Command-Line Interface</b>	<b>5-1</b>
Cisco IOS Command Modes	5-2
Getting Help	5-3
Abbreviating Commands	5-3
Using no and default Forms of Commands	5-4
Understanding CLI Messages	5-4
Using Command History	5-4
Changing the Command History Buffer Size	5-5
Recalling Commands	5-5
Disabling the Command History Feature	5-5
Using Editing Features	5-6
Enabling and Disabling Editing Features	5-6

- Editing Commands with Keystrokes 5-6
- Editing Command Lines That Wrap 5-7
- Searching and Filtering Output of show and more Commands 5-8
- Accessing the CLI 5-9
  - Opening the CLI with Telnet 5-9
  - Opening the CLI with Secure Shell 5-9

**Troubleshooting 6-1**

- Checking the Access Point LEDs 6-2
- Checking Basic Settings 6-4
  - Default IP Address Behavior 6-4
  - Default SSID and Radio Behavior 6-5
  - Enable Radio Interfaces 6-5
  - SSID 6-5
  - WEP Keys 6-6
  - Security Settings 6-6
- Low Power Condition 6-6
  - Intelligent Power Management 6-7
    - Inline Power Status Messages 6-7
  - Configuring Power Using the CLI 6-9
    - Issuing the Cisco IOS Command Using the CLI 6-11
  - Configuring the Access Point System Power Settings Using a Browser 6-11
- Running the Carrier Busy Test 6-14
- Running the Ping Test 6-14
- Resetting to the Default Configuration 6-15
  - Using the MODE Button 6-15
  - Using the Web Browser Interface 6-16
- Reloading the Access Point Image 6-16
  - Using the MODE Button 6-17
  - Web Browser Interface 6-17
    - Browser HTTP Interface 6-18
    - Browser TFTP Interface 6-18
- Obtaining the Access Point Image File 6-19
- Obtaining the TFTP Server Software 6-19

**Translated Safety Warnings** A-1

- Statement 245B—Explosive Device Proximity Warning A-2
- Statement 332—Antenna Installation Warning A-3
- Statement 353—Power Source Warning A-3
- Statement 1001—Work During Lightning Activity Warning A-5
- Statement 1004—Installation Instructions Warning A-6
- Statement 1005—Circuit Breaker (20A) Warning A-7

**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-4
  - Declaration of Conformity for RF Exposure B-5
  - 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
  - Declaration of Conformity Statements for European Union Countries 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-2

**Console Cable Pinouts** E-1

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

---

**GLOSSARY**


---

**INDEX**







## Preface

---

### Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1130AG Series Access Point, hereafter referred to as the *access point*. To use this guide, you should have experience working with 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 Cisco IOS commands, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS Release 12.3 commands, refer to the Cisco 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 12.3** from the Cisco IOS Software drop-down menu.

This guide also includes an overview of the access point web-based interface (APWI) but does not provide field-level descriptions of all the APWI windows nor does it provide the procedures for configuring all access point options from the APWI. For all APWI window descriptions, 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.

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.

**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].)**

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

## Related Publications

These documents provide complete information about the access point:

- *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 1130 Series Access Point documentation:

[http://www.cisco.com/en/US/products/ps6087/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6087/tsd_products_support_series_home.html)

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto: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 Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



### Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

---

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



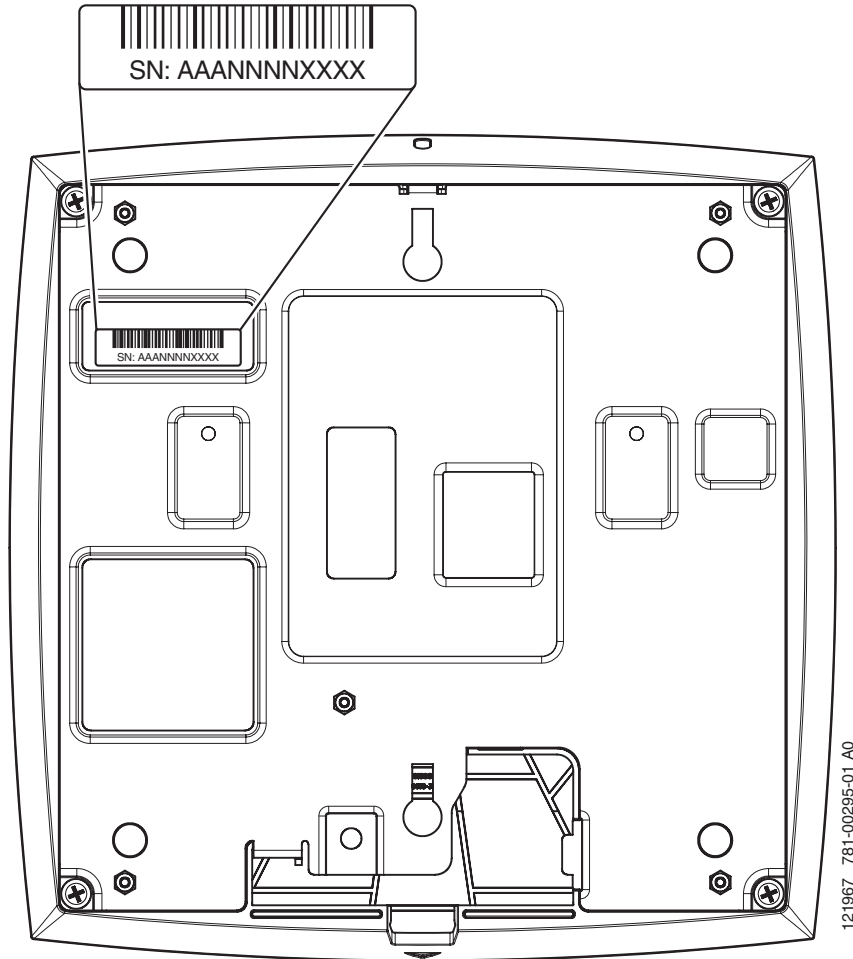
### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Locating the Product Serial Number

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

**Figure 1** Location of Serial Number Label



The access point serial number label contains the following information:

- Model number, such as *AIR-AP1130AG-x-k9*
- Serial number, such as *VDF0636XXXX* (11 alphanumeric digits)
- MAC address, such as *00abc65094d3* (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.



## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



## Overview

---

Cisco Aironet 1130AG Series Access Points combine mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, the 1130AG 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.

The access point connects wireless and wired networks or is the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

You can configure and monitor the access point using the command-line interface (CLI), the browser-based management system, Simple Network Management Protocol (SNMP), or Cisco Structured Wireless-Aware Network (SWAN).

This chapter provides information on the following topics:

- [Hardware Features, page 1-2](#)
- [Network Configuration Examples, page 1-7](#)

# Hardware Features

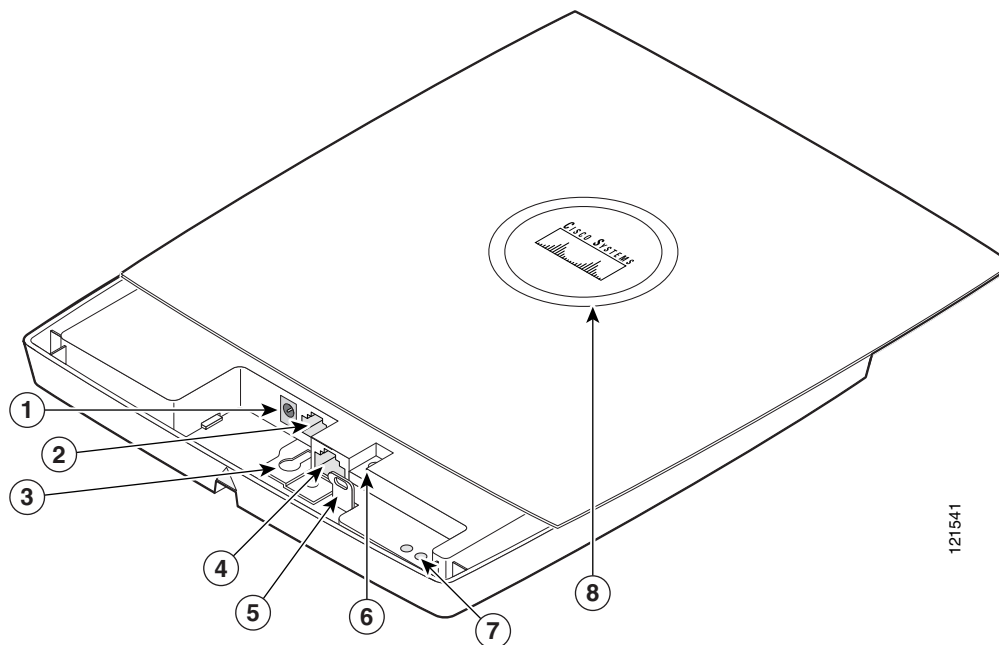
Key hardware features of the access point include:

- Dual-radio operation (see [page 1-3](#))
- Ethernet port (see [page 1-3](#))
- Console port (see [page 1-3](#))
- LEDs, (see [page 1-3](#))
- Multiple power sources (see [page 1-4](#))
- UL 2043 certification (see [page 1-4](#))
- Anti-theft features (see [page 1-5](#))

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

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

**Figure 1-1 Access Point Hardware Features**



<b>1</b>	48-VDC power port	<b>5</b>	Padlock post
<b>2</b>	Ethernet port (RJ-45)	<b>6</b>	Mode button
<b>3</b>	Keyhole slot	<b>7</b>	Ethernet (E) and radio (R) LEDs
<b>4</b>	Console port (RJ-45)	<b>8</b>	Status LED

121541

## 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 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*.

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

**Note**

Do not attempt to connect a cable with a protective boot to the access point Ethernet port. Because of limited space in the connection area, booted connectors will not fit.

## 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**

Do not attempt to connect a cable with a protective boot to the access point console port. Because of limited space in the connection area, booted connectors will not fit.

## LEDs

The access point has three LEDs to indicate Ethernet activity, radio activity, and 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 (top cover closed).
- 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 is located in the cable bay area under the access point top cover. This LED signals that wireless packets are being transmitted or received over the radio interface and provides radio error indications.

**Note**

The access point cover must be closed to view the Status LED but the cover must be open to view the Ethernet and the Radio LEDs.

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

## Power Sources

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



### Warning

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



### Caution

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

The access point supports the following power sources:

- Power module
- Inline power:
  - Cisco Aironet Power Injector (AIR-PWRINJ3 or AIR-PWRINJ-FIB)
  - An inline power capable switch, such as the Cisco Catalyst 3550 PWR XL, 3560-48PS, 3570-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
  - Other inline power switches supporting the IEEE 802.3af inline power standard



### Note

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. At power-up, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point 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 6-6).

## 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.

## Anti-Theft Features

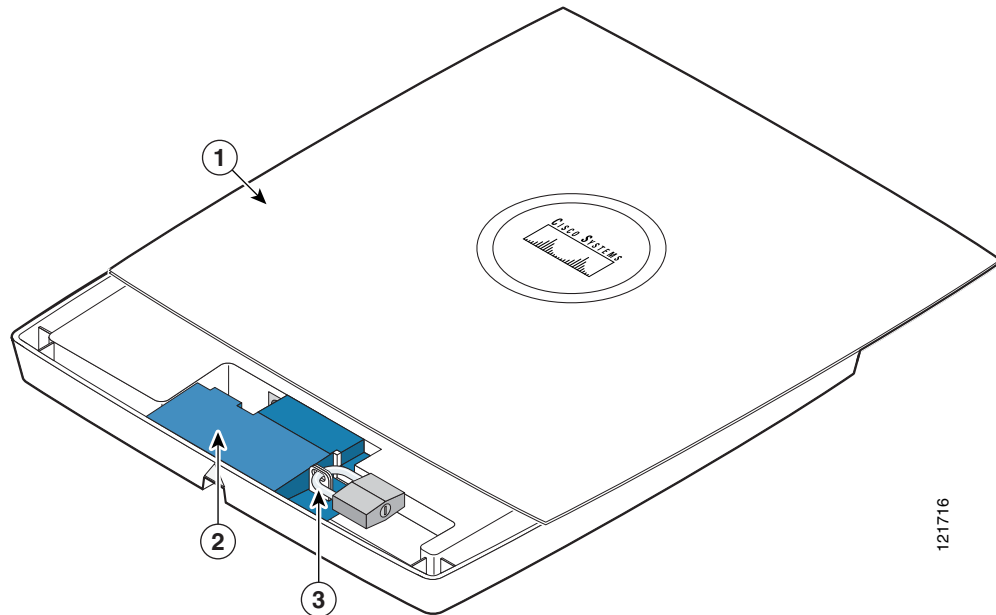
There are three methods of securing the access point:

- Security cable keyhole—You can use the security cable slot to secure the access point using a standard security cable, like those used on laptop computers (refer to the [“Using a Security Cable” section on page 2-17](#)).
- Security hasp adapter—When you mount the access point on a wall or ceiling using the mounting plate and the security hasp adapter, 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.

**Figure 1-2** Access Point with Security Hasp Adapter



<b>1</b>	Access point cover in open position	<b>3</b>	Security padlock
<b>2</b>	Security hasp adapter		

- Security screw—The access point contains a security screw hole (see [Figure 1-3](#)) that can be used to secure the access point to the mounting plate.
  - When the supplied #8 Philips head screw is used, the access point is prevented from accidentally detaching from the mounting plate in vertical and over-head mounting positions.



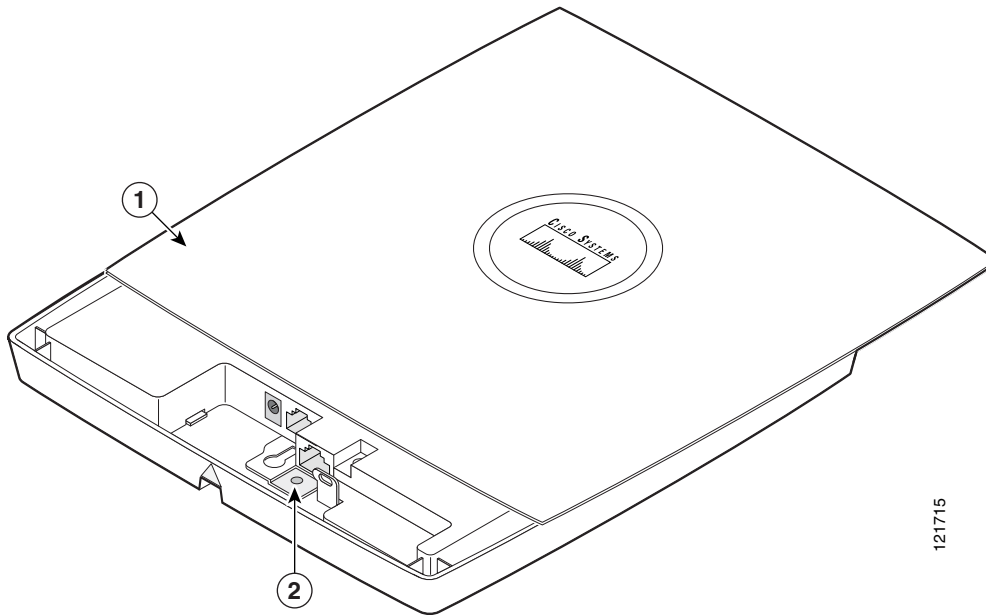
**Note** The supplied #8 Philips head screw provides minimal anti-theft protection.

- When a tamper-resistant head screw (user supplied) is used, access to the mounting screws that attach the mounting plate is greatly restricted.



**Note** The use of a tamper-resistant head screw does not restrict access to the access point cables or the mode button.

**Figure 1-3** Access Point Security Screw Hole



<b>1</b>	Access point cover in open position	<b>2</b>	Security screw hole
----------	-------------------------------------	----------	---------------------



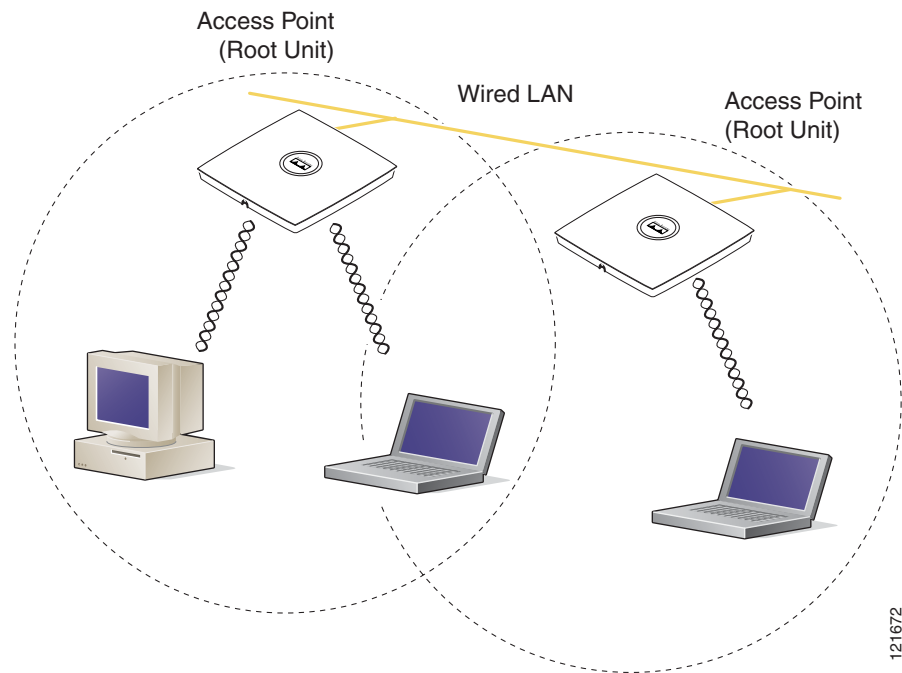
# Network Configuration Examples

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

**Figure 1-4** Access Points as Root Units on a Wired LAN



## Repeater Unit that Extends Wireless Range

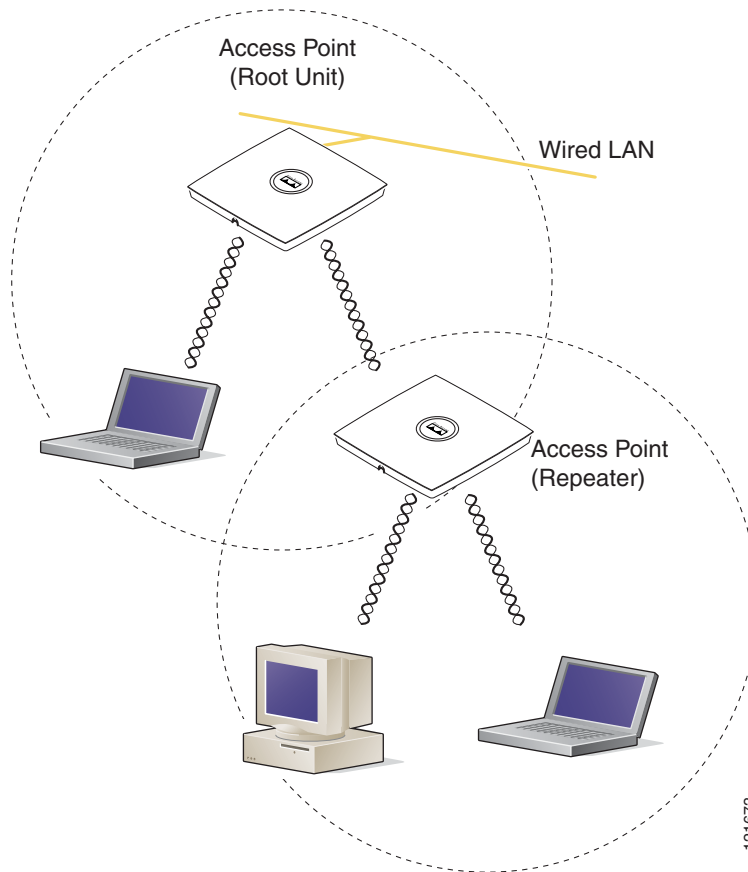
An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point 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.

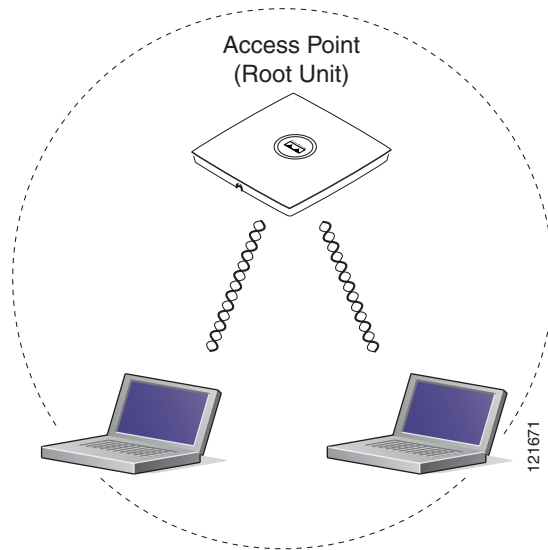
**Figure 1-5** Access Point as Repeater



## 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







## 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 2-8](#)
- [Opening the Access Point Cover, page 2-9](#)
- [Mounting the Access Point on a Horizontal or Vertical Surface, page 2-10](#)
- [Mounting the Access Point Below a Suspended Ceiling, page 2-12](#)
- [Mounting the Access Point Above a Suspended Ceiling, page 2-13](#)
- [Mounting Access Point on a Network Cable Box, page 2-15](#)
- [Mounting Access Point on a Desktop or Shelf, page 2-15](#)
- [Attaching the Access Point to the Mounting Plate, page 2-15](#)
- [Securing the Access Point, page 2-17](#)
- [Connecting the Ethernet and Power Cables, page 2-20](#)
- [Powering Up the Access Point, page 2-24](#)

# Safety Information

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

## FCC Safety Compliance Statement

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

## General Safety Guidelines

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

## Warnings

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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

# 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 module)—optional
- Mounting hardware kit
  - One mounting plate
  - Two suspended ceiling adjustable T-rail clips (accommodates standard and recessed T-rails)
  - One security hasp adapter
  - Four 6 x 32 x ¼ in. flat head Phillips machine screws
  - One 8 x 32 x 3/16 in. pan head Phillips machine screw
  - 2 #8 plastic wall anchors
  - 2 #8 x 32 x 1 in. pan head screws
- *Quick Start Guide: Cisco Aironet 1130AG Series Access Point*
- *Safety Warnings for Cisco Aironet 1130AG Series Access Points*
- Cisco product registration and Cisco documentation feedback cards

## Basic Installation Guidelines

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

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

## Before Beginning the Installation

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

- “Access Point Layout and Connectors” section on page 2-4
- “Mounting Plate” section on page 2-5
- “Suspended Ceiling Adjustable T-Rail Clips” section on page 2-7



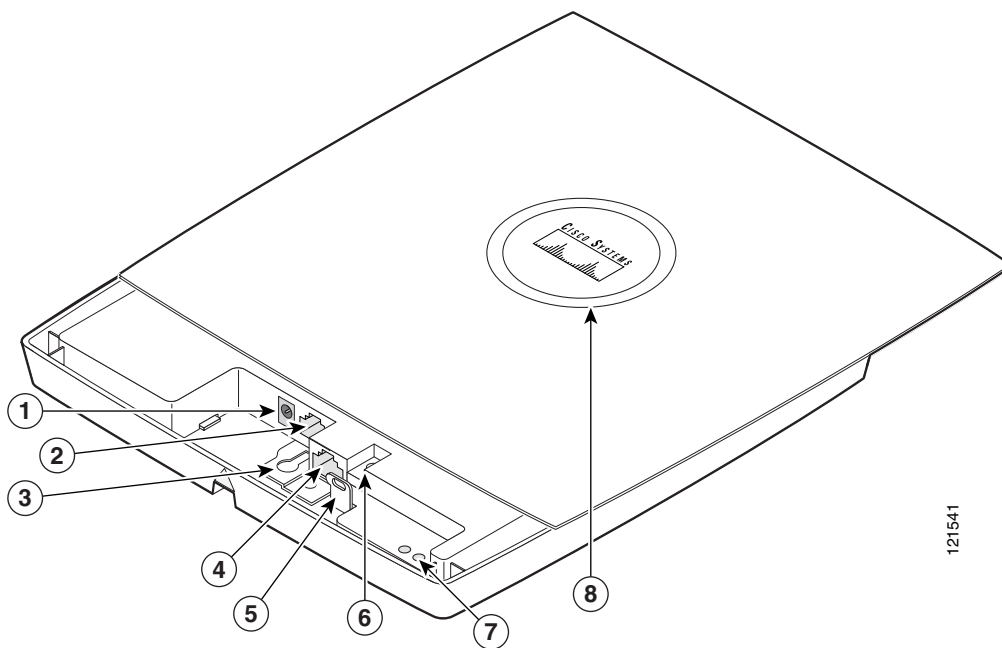
**Caution**

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

## Access Point Layout and Connectors

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

**Figure 2-1** Access Point Hardware Features



1	48-VDC power port	5	Padlock post
2	Ethernet port (RJ-45)	6	Mode button
3	Keyhole slot	7	Ethernet (E) and radio (R) LEDs
4	Console port (RJ-45)	8	Status LED



**Note**

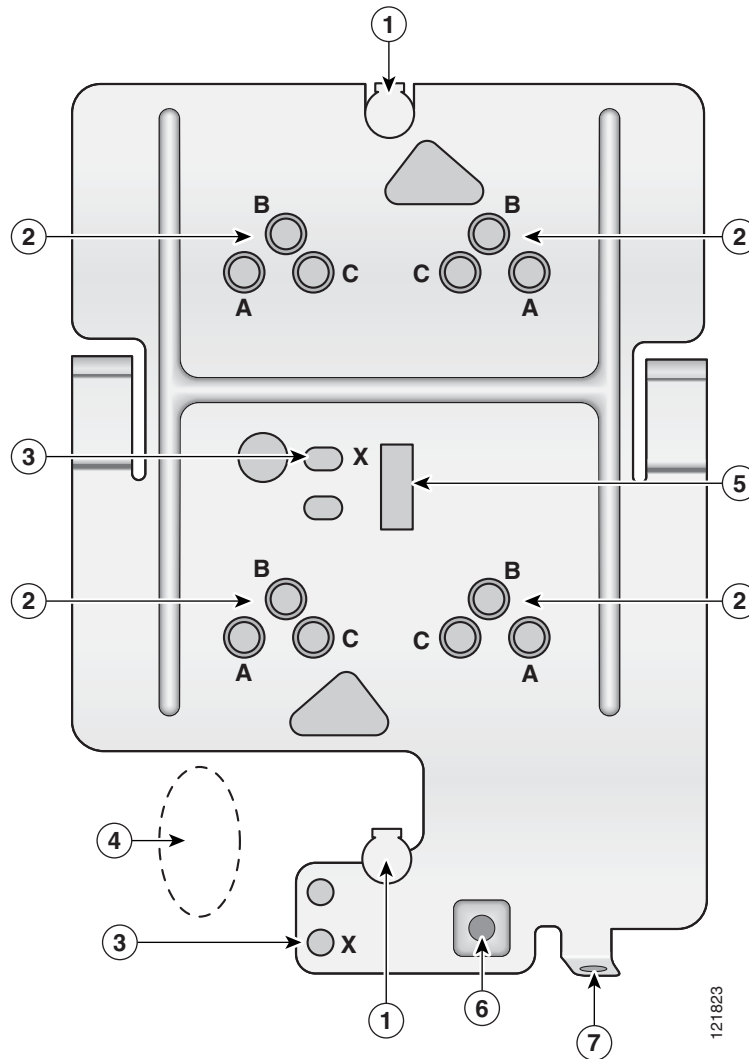
There is a second keyhole slot located on the bottom of the unit near the security slot.



## Mounting Plate

The access point mounting plate is designed to accommodate multiple mounting methods. The mounting holes on the plate are marked so that 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



<b>1</b>	Keyhole clips	<b>5</b>	T-bar hanger clip hole
<b>2</b>	Screw holes (A, B, C)	<b>6</b>	Security screw hole
<b>3</b>	Screw hole (X)	<b>7</b>	Padlock hole
<b>4</b>	Location for cable access 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 keyhole slots on the bottom of the access point.
- Screw holes (A, B, C)—used to attach the suspended ceiling adjustable T-rail clips.
- Screw hole (X)—used to attach the mounting plate to a network cable box, wall, or ceiling. The mounting kit contains two 8 x 32 x 1 inch pan head screws and wall anchors for wall or ceiling mounting.
- T-bar hanger clip hole—used to attach a T-bar hanger clip.
- Security screw hole—used to secure the access point to the mounting plate.
- Padlock hole—used to attach a padlock (user provided) 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**

---

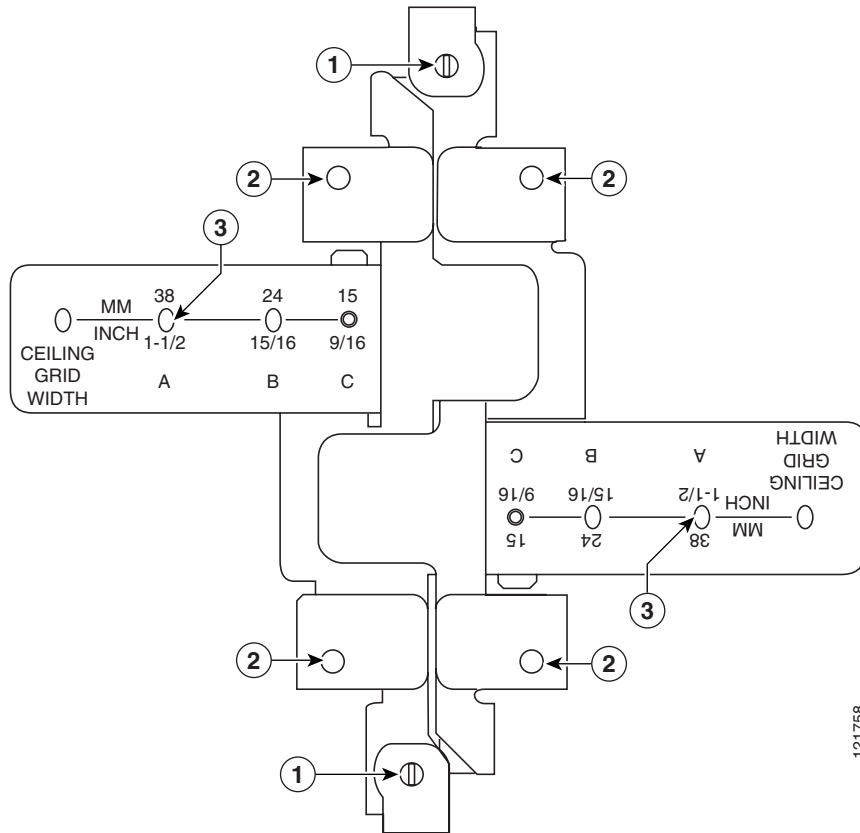
The security hasp covers the cable bay area ( including the power port, Ethernet port, console port, and the mode button) to prevent the installation or removal of the cables or the activation of the mode button.

---

## 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



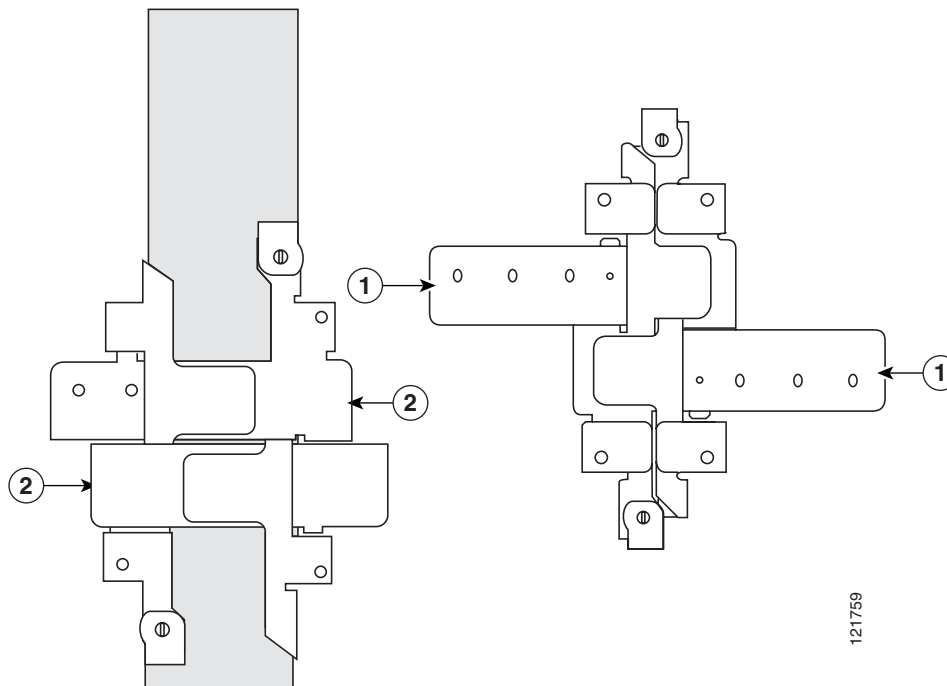
<p><b>1</b> T-rail locking screws</p>	<p><b>3</b> T-rail width adjustment detents (A, B, C) correspond to the A, B, and C holes on the mounting plate</p>
<p><b>2</b> Mounting plate screw holes (8 x 32 flat head screw)</p>	

The adjustable T-rail clip attaches to the mounting plate using four 6 x 32 x 1/4 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*



<b>1</b>	Push here to open	<b>2</b>	Push here to close
----------	-------------------	----------	--------------------

## Installation Summary

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

- Open the access point cover (see [“Opening the Access Point Cover”](#) section on page 2-9).
- Mount the mounting plate on a convenient flat horizontal or vertical surface, such as a desktop, book shelf, file cabinet, wall, ceiling, or suspended ceiling T-rail. See these sections:
  - [“Mounting the Access Point on a Horizontal or Vertical Surface”](#) section on page 2-10
  - [“Mounting the Access Point Below a Suspended Ceiling”](#) section on page 2-12
  - [“Mounting the Access Point Above a Suspended Ceiling”](#) section on page 2-13
  - [“Mounting Access Point on a Network Cable Box”](#) section on page 2-15
  - [“Mounting Access Point on a Desktop or Shelf”](#) section on page 2-15).
- Attach the access point to the mounting plate (see the [“Attaching the Access Point to the Mounting Plate”](#) section on page 2-15).
- Secure the access point (see the [“Securing the Access Point”](#) section on page 2-17).
- Connect Ethernet and power cables (see the [“Connecting the Ethernet and Power Cables”](#) section on page 2-20).
- 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*).

## Opening the Access Point Cover

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

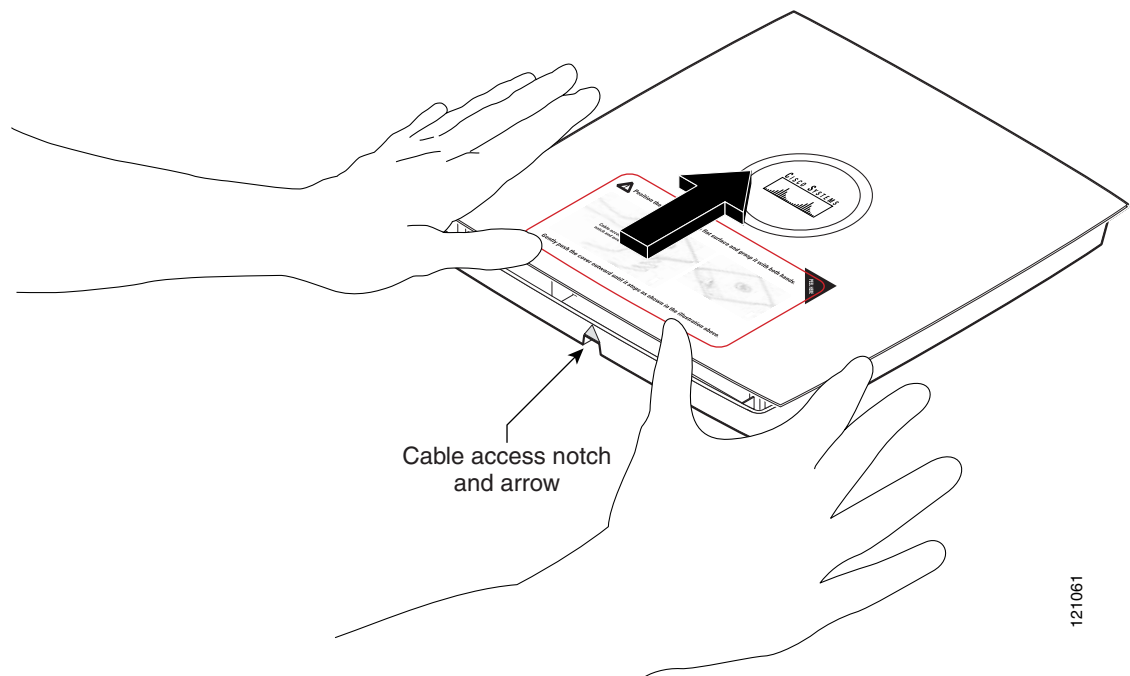
**Caution**

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** Find the cable access notch on the end of the unit (see [Figure 2-5](#)).

**Figure 2-5** Opening the Access Point Cover



- Step 2** Place your thumbs on the edge of top cover and gently push towards the Status LED.

- Step 3** Continue to slowly slide the cover back until you reach the cover stop.

# Mounting the Access Point on a Horizontal or Vertical Surface

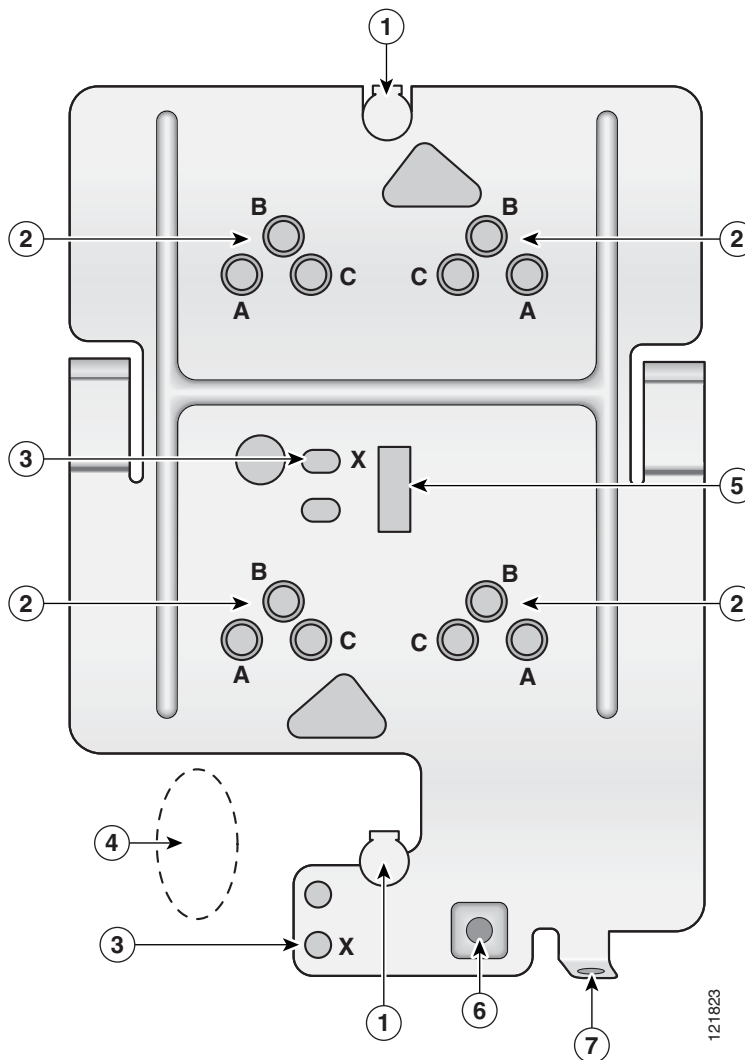
Follow these steps to mount the access point on a horizontal or vertical surface:

- 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 2-6](#)).



**Note** The mounting plate can be installed upside-down on a vertical surface for upper cable entry.

**Figure 2-6** Mounting Plate



<b>1</b>	Keyhole clip	<b>5</b>	T-bar hanger clip hole
<b>2</b>	Screw holes (A, B, C)	<b>6</b>	Security screw hole
<b>3</b>	Screw hole (X)	<b>7</b>	Padlock hole
<b>4</b>	Location for cable access hole		

- Step 2** Drill a 3/16 in. (4.7 mm) hole at the X mounting hole locations you marked.
- Step 3** Insert the wall anchors into the mounting holes.
- Step 4** If needed, drill or cut a cable access hole (see [Figure 2-6](#)) large enough for the Ethernet and possibly the power cables and pull the cables through the access hole until you have about 1 foot of exposed cables protruding from the hole.



---

**Note** You can optionally insert the Ethernet cable and the power cable (if used) through the cable access notch in access point housing (see [Figure 2-5](#)).

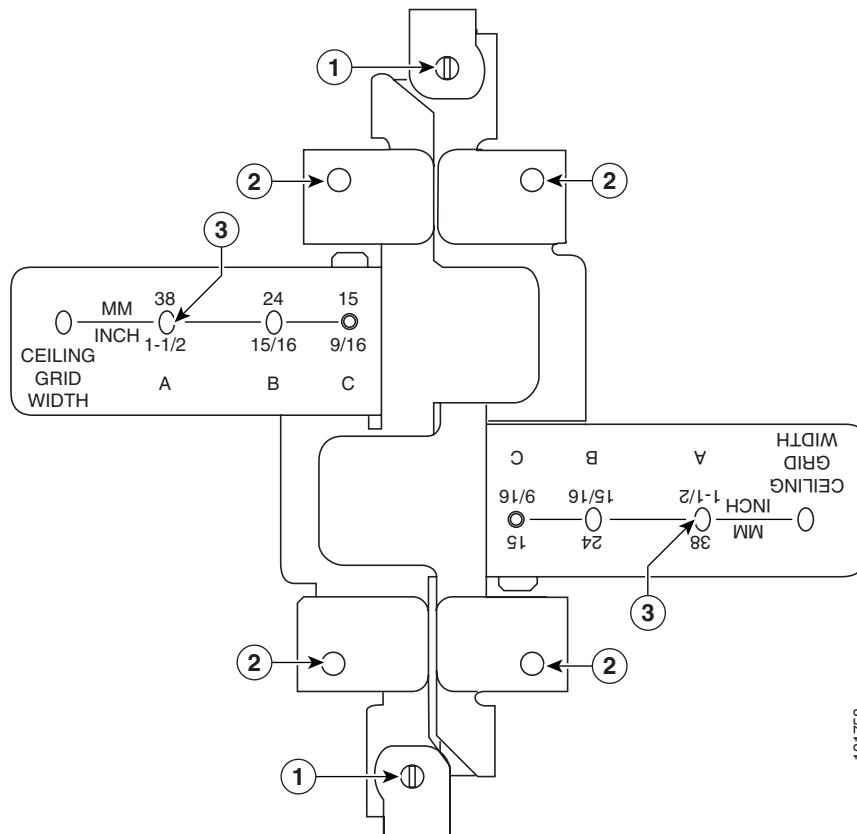
---

- Step 5** Position the mounting plate over the wall anchors or the drilled holes.
- Step 6** Insert two 8 x 32 x 1 inch pan head screws in the X mounting holes and tighten.
- To attach the access point to the mounting plate, see [“Attaching the Access Point to the Mounting Plate” section on page 2-15](#).
-

# Mounting the Access Point Below a Suspended Ceiling

You should review [Figure 2-7](#) before beginning the mounting process.

**Figure 2-7** Adjustable T-Rail Clips



<b>1</b>	T-rail locking screws	<b>3</b>	T-rail width detents (A, B, or C)
<b>2</b>	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** Place the T-rail clip over the T-rail and close it (see [Figure 2-4](#)) to the appropriate (A, B, or C) detent.
- Step 4** Tighten the two T-rail locking screws to prevent the T-rail clip from sliding along the T-rail.
- Step 5** Observe the T-rail width detent letter (A, B, or C) that corresponds to the T-rail width.
- Step 6** Align the corresponding (A, B, or C) holes on the mounting plate over the T-rail mounting plate holes.
- Step 7** Hold the mounting plate and insert a 6 x 32 x 1/4 in. flat head screw into each of the four corresponding (A, B, or C) holes and tighten.



**Step 8** If needed, drill or cut a cable access hole (see [Figure 2-6](#)) 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 2-15](#).

---

## Mounting the Access Point 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.

---

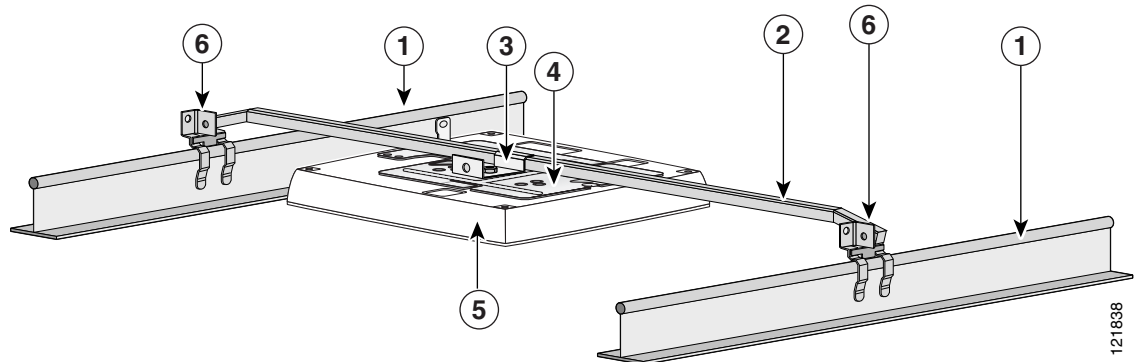
**Caution**

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 to [Figure 2-8](#) before proceeding.

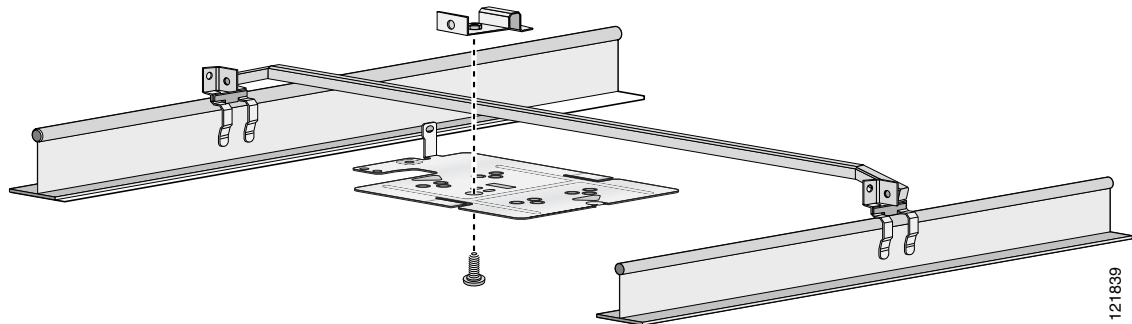
**Figure 2-8 T-Bar Grid Mounting Bracket Parts**



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.
- Step 2** Place the clip over the T-bar box hanger (refer to [Figure 2-9](#)) and secure it to the access point mounting bracket with the 1/4-20 fastener (supplied with the T-bar hanger).

**Figure 2-9 T-Bar and Mounting Bracket**



- 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 2-21).
- 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 2-15).
- 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 2-17).
  - Step 10** Verify that the access point is operating before replacing the ceiling tile.
- 

## Mounting Access Point 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 6 x 32 x 1/4 in. pan head screw into each of the two 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.

To attach the access point to the mounting plate, see the [“Attaching the Access Point to the Mounting Plate”](#) section on page 2-15.

## Mounting Access Point 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 2-20.

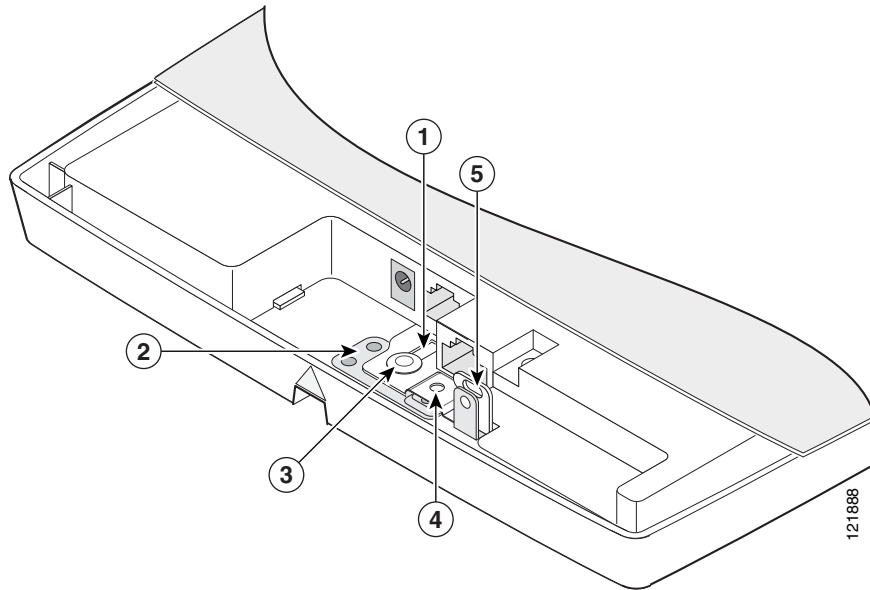
## Attaching the Access Point to the Mounting Plate

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 2-9).
- Step 2** In the cable bay area, pull the cables through the access point cable opening (see [Figure 2-5](#)).

- 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 2-10](#)).

**Figure 2-10** *Aligning the Keyhole Clip to the Access Point Keyhole*



<b>1</b>	Access point keyhole	<b>4</b>	Security screw hole
<b>2</b>	Mounting plate	<b>5</b>	Padlock hole
<b>3</b>	Mounting plate keyhole clip		

- 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 that is located on the opposite end of the access point and is 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 2-20.

For instructions on securing your access point, refer to the [“Securing the Access Point”](#) section on page 2-17.

# Securing the Access Point

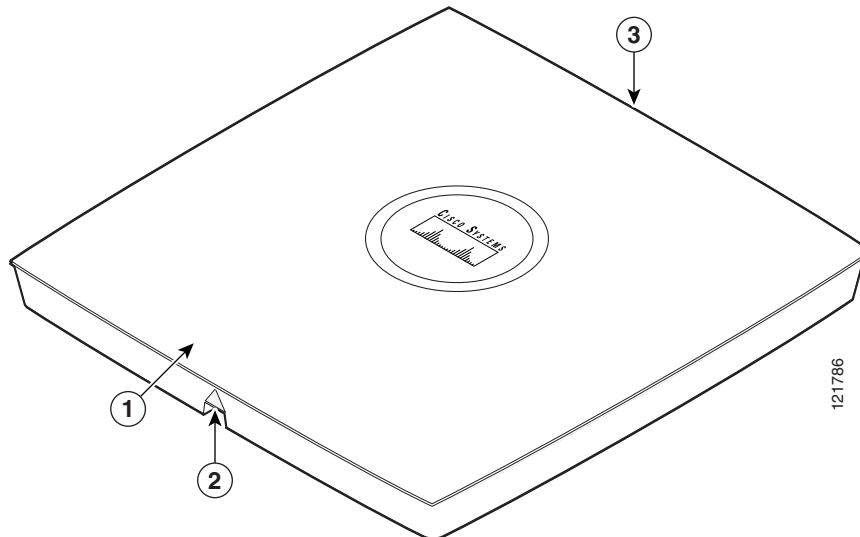
There are two ways to secure your access point:

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

## Using a Security Cable

You can secure the access point by installing a standard security cable (such as the Kensington Notebook MicroSaver, model number 64068) into the access point security cable slot (see [Figure 2-5](#)). The security cable can be used with any of the mounting methods described in this guide.

**Figure 2-11 Security Cable Slot**



<b>1</b>	Access point cover	<b>3</b>	Security cable slot
<b>2</b>	Cable access notch		

Follow these steps to install the security cable.

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

## Securing the Access Point to the Mounting Plate

The mounting plate provides two methods of securing your access point to restrict its removal:

- You can use the security hasp adapter (supplied) and a padlock (that you provide) to secure your access point to the mounting plate (refer to [Figure 1-3 on page 1-6](#)). 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.

- You can use the 8 x 32 x 3/16 in. pan head screw (provided) or a tamper-resistant head screw (that you provide) to attach the access point to the mounting plate using the security screw hole (see [Figure 2-10](#)).

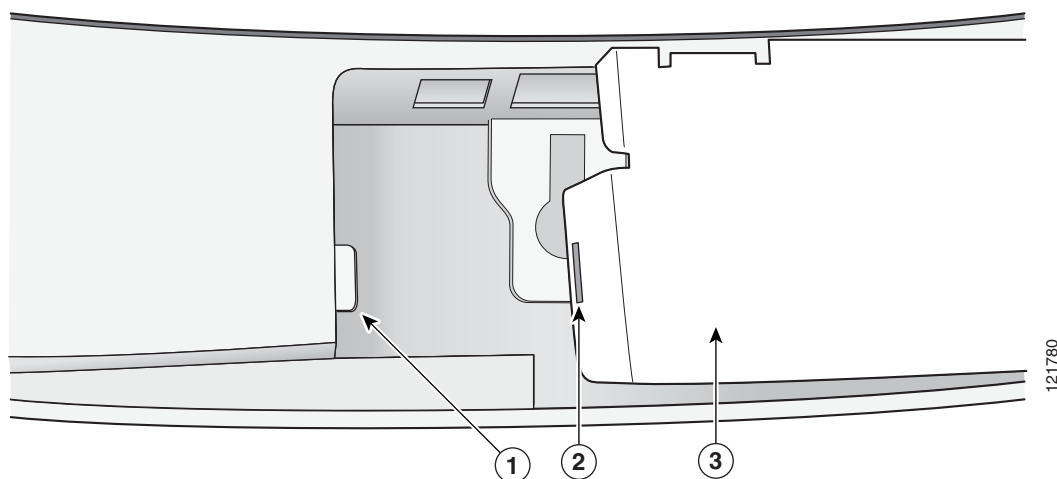


**Note** Using a tamper-resistant head screw to secure the access point to the mounting plate does not prevent someone from inserting or removing the access point cables or pressing the mode button.

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 2-9).
- Step 2** Carefully tilt the security hasp adapter and insert the access point security hasp tab into the notch on the security hasp adapter (see [Figure 2-12](#)).

**Figure 2-12** Installing the Security Hasp Adapter

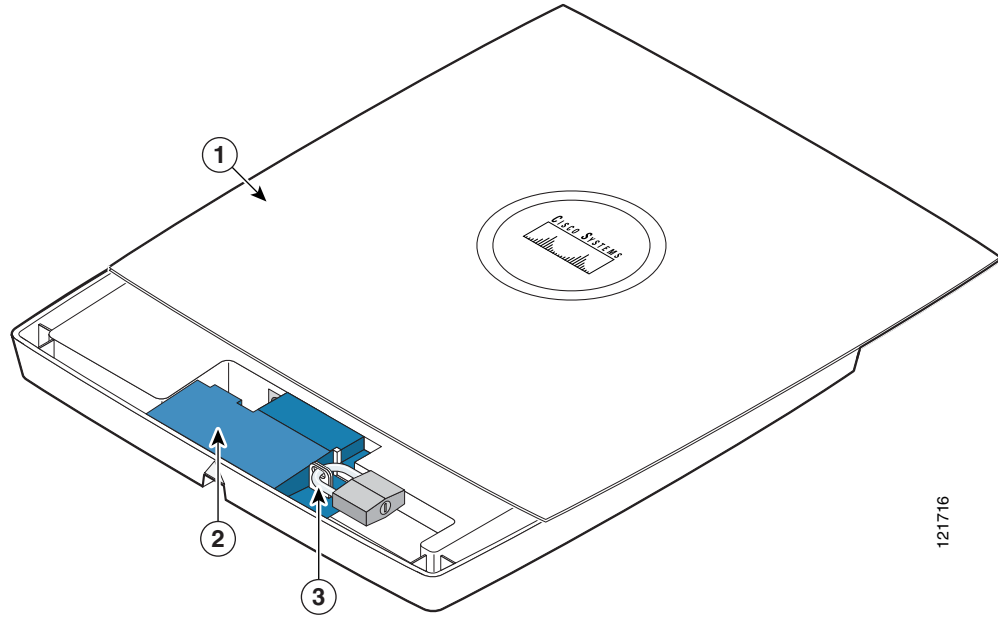


<b>1</b>	Access point security hasp tab	<b>3</b>	Security hasp adapter
<b>2</b>	Security hasp notch		

- Step 3** Push down on the security hasp adapter to expose the padlock post hole.

- Step 4** Insert a padlock into the padlock post hole and lock the padlock.
- Step 5** Position the padlock into the padlock area (see [Figure 2-13](#))

**Figure 2-13 Padlock**



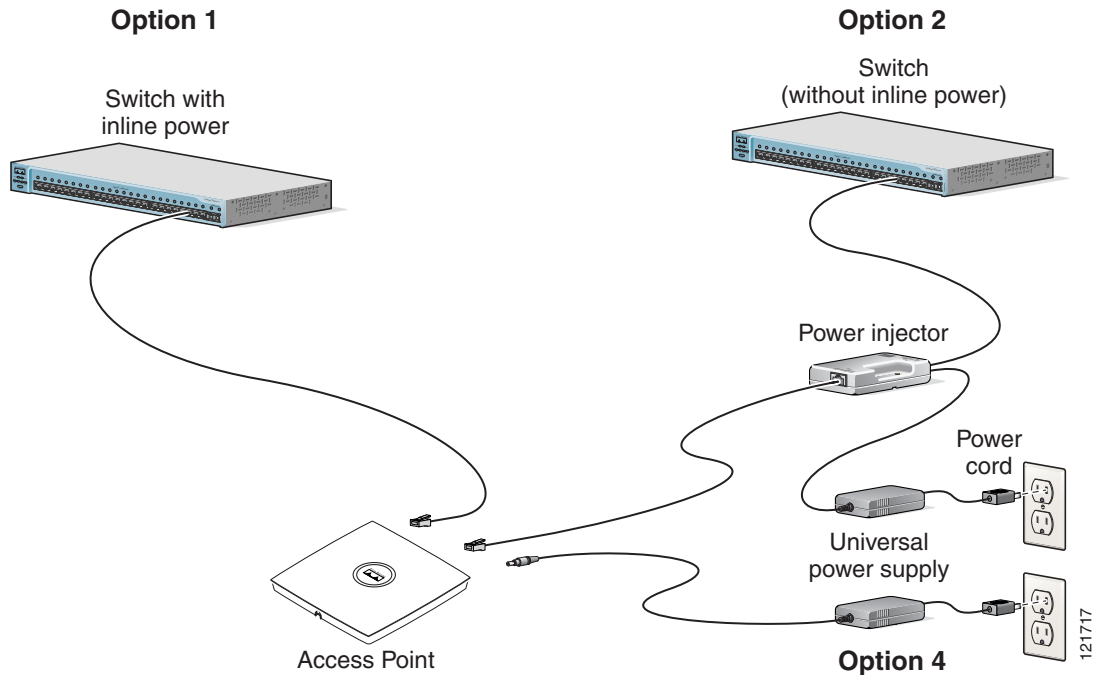
<b>1</b>	Access point cover in open position	<b>3</b>	Security padlock
<b>2</b>	Security hasp adapter		

- Step 6** Push down on the padlock to ensure the padlock is held by the security hasp adapter clips.
- Step 7** Close the access point cover by sliding it over the security hasp adapter until you hear a click.

# Connecting the Ethernet and Power Cables

The access point receives power through the Ethernet cable or an external power module. Figure 2-14 shows the power options for the access point.

**Figure 2-14** Access Point Power Options



## Warning

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

The access point supports the following power sources:

- Power module
- Inline power:
  - Cisco Aironet Power Injector (AIR-PWRINJ3 or AIR-PWRINJ-FIB)
  - An inline power capable switch, such as the Cisco Catalyst 3550 PWR XL, 3560-48PS, 3570-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
  - Other inline power switches supporting the IEEE 802.3af inline power standard



## Note

Some older switches and patch panels might not provide enough power to operate the access point. At power-up, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. 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 6-6).



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



### Caution

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



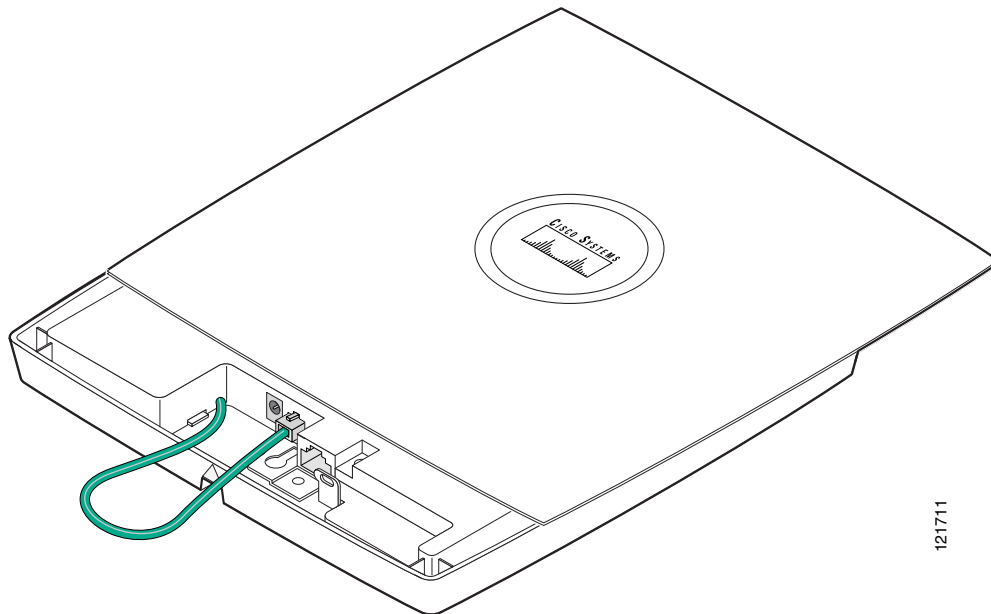
### Note

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

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

- Step 1** If necessary, open the access point cover (see the [“Opening the Access Point Cover”](#) section on page 2-9).
- 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 2-15](#))

**Figure 2-15**     *Looping the Ethernet Cable*



- Step 4** Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point.
- 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 you hear a click.

- 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 2-20).
  - 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.

## Connecting to an Ethernet Network with Local Power



### Caution

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



### Note

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

Follow these steps to connect the access point to 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 2-9).
- 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 2-15](#)).
- 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 you hear a click.
- 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 2-17.

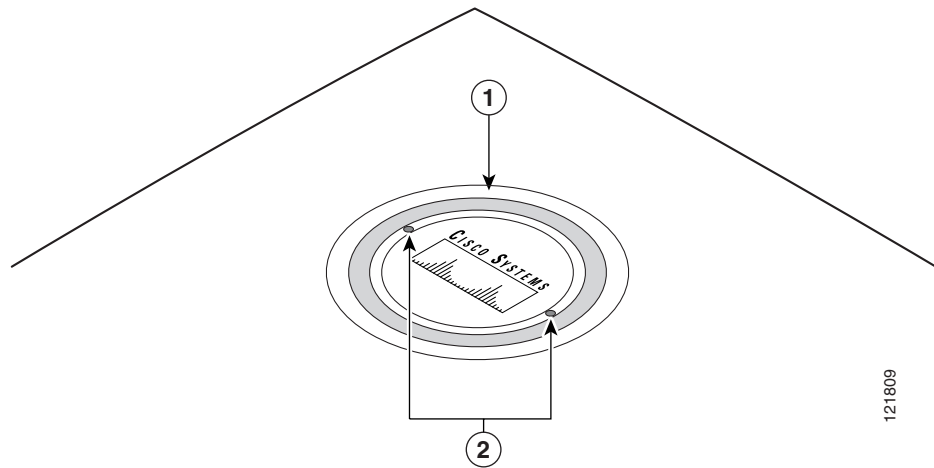
# Rotating the Cisco Logo

The Cisco logo on the top of the unit can be rotated to correctly position the logo for any mounting arrangement; for example, when the unit is mounted on a vertical wall. The logo should always be easy to read.

To rotate the Cisco logo, follow these steps:

- Step 1** Place the end of an opened paper clip into each of the holes on the logo assembly (see [Figure 2-16](#)).

**Figure 2-16** Cisco Logo Holes



121809

1	Status LED	2	Logo assembly holes
---	------------	---	---------------------

- Step 2** Using the paper clips, rotate the logo until you reach the desired orientation. Detents are provided to help you align the logo for 90 degree rotations.
- Step 3** Remove the paper clips.

# Powering Up the Access Point

When you apply power 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 Power-On Self-Test (POST) activities; for example, 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 that there are no client devices associated, or it turns blue to signify that there are client devices associated. Refer to [Chapter 6, “Troubleshooting,”](#) for complete LED descriptions.

When the Status LED turns light blue or medium blue, you can 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.”](#)

**Caution**

---

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

---

**Note**

---

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

---



## 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 3-4](#)
- [Connecting to the Access Point Locally, page 3-4](#)
- [Assigning Basic Settings, page 3-5](#)
- [Configuring Basic Security Settings, page 3-10](#)
- [Finding the IP Address Using the CLI, page 3-13](#)
- [Assigning an IP Address Using the CLI, page 3-14](#)
- [Using a Terminal Emulator to Access the CLI, page 3-14](#)
- [Using a Telnet Session to Access the CLI, page 3-15](#)

## 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 Cisco IP Setup Utility (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 2-9).
  - 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 3-4).

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

---

**Step 1** Open your Internet browser.



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



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

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

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

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

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

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

**Step 7** To return to factory default settings, click **Reset to Defaults**.

**Step 8** To retain the IP address and return all other settings to factory default values, click **Reset to Defaults (Except IP)**.

---

## Default IP Address Behavior

When you connect an 1130AG access point running Cisco IOS Release 12.3(2)JA or later software with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an IP address, continues to send requests indefinitely.

## Default SSID and Radio Behavior

In Cisco IOS Release 12.3(2)JA2 and earlier, the access point radios are enabled by default and the default SSIDs are *tsunami*.

In Cisco IOS Release 12.3(4)JA, the access point radios are disabled by default, and there are no default SSIDs. You must create an SSID and enable the radio before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the [“Configuring Basic Security Settings”](#) section on page 3-10 for instructions on configuring the SSID and the [“Enabling the Radio Interfaces”](#) section on page 3-9 for instructions on enabling the radio interfaces.

## 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:

- 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 3-4) and follow the steps in the “Assigning an IP Address Using the CLI” section on page 3-14.
- 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 3-4 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 CLI to identify the IP address assigned to your access point (refer to the Finding the IP Address Using the CLI, page 3-13).

## Connecting to the Access Point Locally

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



### Caution

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



### Note

The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/en/US/ordering/index.shtml> to order a serial cable.



### Note

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

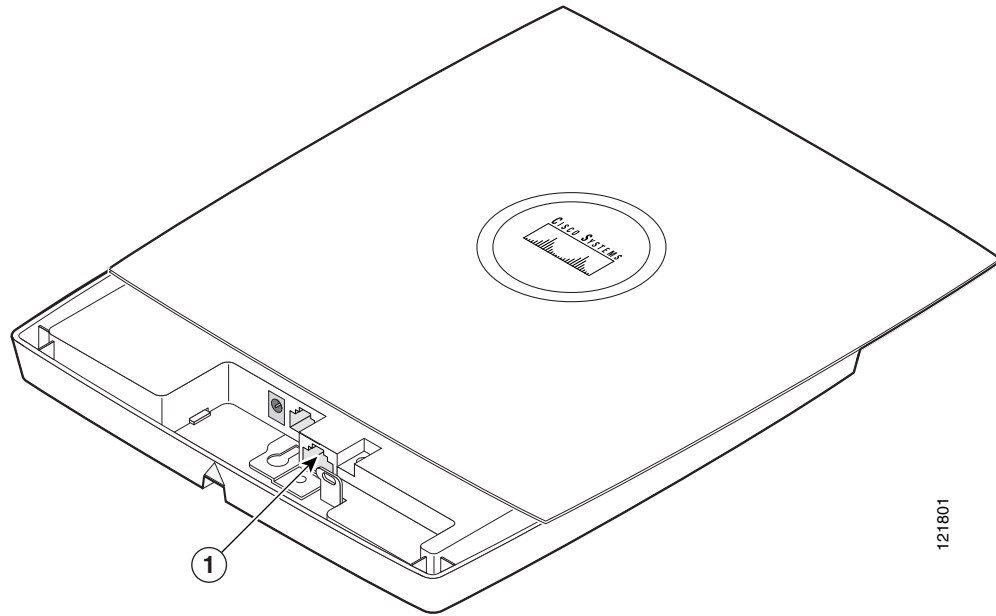
Follow these steps to open the CLI by connecting to the access point console port:

- Step 1** Open the access point cover (refer to “Opening the Access Point Cover” section on page 2-9).
- 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. To connect to the access point console port, you should loop the cable as shown in Figure 2-15.



Figure 3-1 shows the console port location.

**Figure 3-1 Console Port Location**



<b>1</b>	Console port
----------	--------------

**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.



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



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

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

- Step 3** Enter *Cisco* in the username field and advance to the Password field.
- Step 4** Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears.

Figure 3-2 shows the Summary Status page.

**Figure 3-2 Summary Status Page**

**Cisco Aironet 1130AG Series Access Point**

Hostname **ap** ap uptime is 7 minutes

Home: Summary Status

**Association**

Clients: [0](#) Repeaters: [0](#)

**Network Identity**

IP Address	10.0.0.109
MAC Address	000b.fcf.1420

**Network Interfaces**

Interface	MAC Address	Transmission Rate
<a href="#">↑ FastEthernet</a>	000b.fcf.1420	100Mb/s
<a href="#">↑ Radio0-802.11G</a>	000b.fcf.1620	54.0Mb/s
<a href="#">↑ Radio1-802.11A</a>	000b.fcf.1220	54.0Mb/s

**Event Log**

Time	Severity	Description

Refresh

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

121705

**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 a Cisco Aironet 1130AG Series Access Point. The page title is "Cisco Aironet 1130AG Series Access Point". The hostname is set to "ap" and the access point has been up for 7 minutes. The configuration is as follows:

Field	Value
Host Name	ap
MAC Address	000b.fcfb.7d2f
Configuration Server Protocol	Static IP (selected)
IP Address	10.0.0.159
IP Subnet Mask	255.255.255.0
Default Gateway	
SNMP Community	defaultCommunity
SNMP Read-Only	Read-Only (selected)
SNMP Read-Write	Read-Write
<b>Radio0-802.11G</b>	
Role in Radio Network	Access Point Root (selected)
Optimize Radio Network for	Default (selected)
Aironet Extensions	Enable (selected)
<b>Radio1-802.11A</b>	
Role in Radio Network	Access Point Root (selected)
Optimize Radio Network for	Default (selected)
Aironet Extensions	Enable (selected)

Buttons for "Apply" and "Cancel" are located at the bottom right of the page.

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

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

- **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.
- **Web Server**—Choose the type of HTTP protocol used by your web browser to access the access point.
  - Standard (HTTP)—Uses encrypted traffic to transfer data.
  - Secure (HTTPS)—Uses Secure Socket Layer (SSL) encrypted traffic to transfer data.
- **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).
- **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.

**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 or Host Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP <sup>1</sup>
IP Subnet Mask	Assigned by DHCP
Default Gateway	Assigned by DHCP
Role in Radio Network	Access point (root)
Web Server	Standard (HTTP)
SNMP Community	defaultCommunity
Optimize Radio Network for	Throughput
Aironet Extensions	Enable

1. When you connect a 1130AG series access point running Cisco IOS Release 12.3(2)JA or later with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.

## Enabling the Radio Interfaces

In Cisco IOS Release 12.3(4)JA, the access point radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radios before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the “[Configuring Basic Security Settings](#)” section on page 3-10 for instructions on configuring the SSID.

To enable the radio interfaces, follow these instructions:

- 
- Step 1** Use your internet browser to access your access point.
  - Step 2** When the Summary Status page displays, click **Network Interfaces > Radio0-802.11g** and the radio status page displays.
  - Step 3** Click **Settings** and the radio settings page displays.
  - Step 4** Click **Enable** in the Enable Radio field.
  - Step 5** Click **Apply**.
  - Step 6** Click **Radio1-802.11A** and the radio status page displays.
  - Step 7** Repeat Steps 3 to 5.
  - Step 8** Close your internet browser.
-

# Configuring Basic Security Settings

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.

Just as you use the Express Setup page to assign basic settings, you can use the Express Security Set-Up page to create unique SSIDs and assign one of four security types to them. For detailed security information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Figure 3-4 shows the Express Security Set-Up page.

**Figure 3-4** Express Security Set-Up Page

Cisco Aironet 1130AG Series Access Point

Hostname ap ap uptime is 58 minutes

Express Security Set-Up

**SSID Configuration**

1. SSID   Broadcast SSID in Beacon

2. VLAN

No VLAN  Enable VLAN ID:  (1-4095)  Native VLAN

3. Security

No Security

Static WEP Key

Key 1  128 bit

EAP Authentication

RADIUS Server:  (Hostname or IP Address)

RADIUS Server Secret:

WPA

RADIUS Server:  (Hostname or IP Address)

RADIUS Server Secret:

**SSID Table**

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input type="button" value="⊗"/>	tsunami	none	none	open	none		<input checked="" type="checkbox"/>

121703

## Understanding Express Security Settings

When the access point configuration is at factory defaults, the first SSID that you create by using the Express Security page overwrites the default SSID (tsunami), which has no security settings. The SSIDs that you create appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the access point.



### Note

In Cisco IOS Release 12.3(4)JA and later, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

## Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs by using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because on the Express Security page encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

If any VLANs are defined on the access point, the trunk port on the switch must be limited to allow only the VLANs defined on the access point.

## Express Security Types

Table 3-2 describes the four security types that you can assign to an SSID.

**Table 3-2 Security Types on Express Security Setup Page**

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the bridge based on MAC address (refer to the <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i> ).	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the bridge key.

**Table 3-2 Security Types on Express Security Setup Page (continued)**

Security Type	Description	Security Features Enabled
EAP Authentication	This option enables 802.1x authentication (such as LEAP, PEAP, EAP-TLS, EAP-GTC, EAP-SIM, and others) and requires you to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1x authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1x authentication. Client devices that associate using this SSID must perform 802.1x authentication.
WPA	Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate using this SSID must be WPA-capable.

## Express Security Limitations

Because the Express Security page is designed for simple configuration of basic security, the options available are a subset of the bridge security capabilities. Keep these limitations in mind when using the Express Security page:

- If the **No VLAN** option is selected, the static WEP key can be configured once. If you select **Enable VLAN**, the static WEP key should be disabled.
- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the bridge. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (for example, MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.



### Note

For detailed information about security and security settings, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.



## Using the Express Security Page

Follow these steps to create an SSID using the Express Security page:

- 
- Step 1** Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.
- Step 2** To broadcast the SSID in the bridge beacon, check the Broadcast SSID in Beacon check box. When you broadcast the SSID, devices that do not specify an SSID can associate to the bridge. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the bridge unless their SSID matches this SSID. Only one SSID can be included in the bridge beacon.
- Step 3** (Optional) Check the Enable VLAN ID check box and enter a VLAN number (1 through 4095) to assign the SSID to a VLAN. You cannot assign an SSID to an existing VLAN.
- Step 4** (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.
- Step 5** Select the security setting for the SSID. The settings are listed in order of robustness, from No Security to WPA, which is the most secure setting.
- If you select Static WEP Key, choose the key number and encryption key size and enter the encryption key (10 hexadecimal characters for 40-bit keys or 26 hexadecimal characters for 128-bit keys).
  - If you select EAP Authentication or WPA, enter the IP address and shared secret for the authentication server on your network.



---

**Note** If you do not use VLANs on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for VLAN details.

---

- Step 6** Click **Apply**. The SSID appears in the SSID table at the bottom of the page.
- 

## Finding the 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.

To find the IP address of your access point using the console port, you can use the Cisco IOS CLI `show ip interface brief bvi1` from the privileged EXEC mode. For additional information on the CLI, refer to the [“Using the Command-Line Interface” section on page 5-1](#).

## Assigning an IP Address Using the CLI

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	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface bvi1</b>	Enter interface configuration mode for the BVI.
Step 3	<b>ip address</b> <i>address</i> <i>mask</i>	Assign an IP address and address mask to the BVI.  <b>Note</b> 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 Terminal Emulator to Access the CLI

Follow these steps to access the CLI using a terminal emulator program from the serial port. These steps are for a PC running Microsoft Windows with the Hyper Terminal application. Check your PC operating instructions for detailed instructions for your operating system.

- 
- Step 1** Connect a DB-9 to RJ-45 serial cable from your PC's serial port connector (COM3 or COM2) to the access point serial console port.
  - Step 2** Select **Start > Programs > Accessories > Communications > Hyper Terminal**.
  - Step 3** When the Hyper Terminal Connection Description window displays, enter a connection name in the Name field and click **OK**.
  - Step 4** When the Connect To window displays, click the drop-down arrow in the Connect using field and choose **COM3** or **COM2** for your PC serial port. Click **OK**.
  - Step 5** When the COM3 or COM2 Properties window displays, enter this information into the respective fields and then click **OK**:
    - Bits per second: **9600**
    - Data bits: **8**
    - Parity: **None**
    - Stop bits: **1**
    - Flow control: **None**
  - Step 6** Click **Enter** and the access point CLI page displays.
-

## 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** Choose **Start > Programs > Accessories > Telnet**.

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

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



---

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

---

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

---





## Using the Web-Browser Interface

---

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

- [Using the Web-Browser Interface for the First Time, page 4-2](#)
- [Using the Management Pages in the Web-Browser Interface, page 4-2](#)
- [Using Online Help, page 4-5](#)

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



**Note**

---

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

---

## 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 3-4 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.



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



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

**Step 2** Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password 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**. Always remember to click **Apply** before changing the page or clicking your browser's **Back** button. Clicking **Cancel** cancels any changes you made on the page and keeps you on that page.

---

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

**Figure 4-1** Web-Browser Interface Home Page

The screenshot displays the Cisco Aironet 1130AG Series Access Point web-browser interface. The page title is "Cisco Aironet 1130AG Series Access Point". The hostname is "ap" and the uptime is "7 minutes". The main content area shows "Home: Summary Status" with sections for Association (Clients: 0, Repeaters: 0), Network Identity (IP Address: 10.0.0.109, MAC Address: 000b.fcfc.1420), Network Interfaces (FastEthernet, Radio0-802.11G, Radio1-802.11A), and Event Log. A navigation menu on the left includes HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. A "Refresh" button is at the bottom right.

## 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
<b>Navigation Links</b>	
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.

**Table 4-1 Common Buttons on Management Pages (continued)**

<b>Button/Link</b>	<b>Description</b>
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.
<b>Configuration Action Buttons</b>	
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.



## 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.





## Using the Command-Line Interface

---

This chapter describes the IOS command-line interface (CLI), which you can use to configure your access point. This chapter 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 5-4](#)
- [Understanding CLI Messages, page 5-4](#)
- [Using Command History, page 5-4](#)
- [Using Editing Features, page 5-6](#)
- [Searching and Filtering Output of show and more Commands, page 5-8](#)
- [Accessing the CLI, page 5-9](#)

# Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on the mode you are currently using. 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. 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.

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

**Table 5-1** Command Mode Summary

Mode	Access Method	Prompt	Exit Method	Using This Mode
User EXEC	Begin a session with your access point.	ap>	Enter <b>logout</b> or <b>quit</b> .	Use this mode to: <ul style="list-style-type: none"> <li>• Change terminal settings</li> <li>• Perform basic tests</li> <li>• Display system information</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	ap#	Enter <b>disable</b> 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 <b>configure</b> command.	ap(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire access point.
Interface configuration	While in global configuration mode, enter the <b>interface</b> command (with a specific interface).	ap(config-if)#	To exit to global configuration mode, enter <b>exit</b> . To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	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.

# 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
<b>help</b>	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: ap# <b>di?</b> dir disable disconnect
<i>abbreviated-command-entry&lt;Tab&gt;</i>	Completes a partial command name. For example: ap# <b>sh conf&lt;tab&gt;</b> ap# show configuration
<b>?</b>	Lists all commands available for a particular command mode. For example: ap> <b>?</b>
<i>command ?</i>	Lists the associated keywords for a command. For example: ap> <b>show ?</b>
<i>command keyword ?</i>	Lists the associated arguments for a keyword. For example: ap(config)# <b>cdp holdtime ?</b> <10-255> Length of time (in sec) that receiver must keep this packet

## Abbreviating Commands

You have to enter only enough characters for the access point to recognize the command as unique. If you do not enter enough characters, the access point indicate an error (% Unknown command). 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.

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 5-5](#)
- [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]
```

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 <sup>1</sup>	Result
Press <b>Ctrl-P</b> 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 <b>Ctrl-N</b> or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.
<b>show history</b>	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 <b>terminal history</b> global configuration command and <b>history</b> 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 with Keystrokes, page 5-6](#)
- [Editing Command Lines That Wrap, page 5-7](#)

## 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 with Keystrokes

[Table 5-5](#) shows the keystrokes that you need to edit command lines.

**Table 5-5** *Editing Commands with Keystrokes*

Capability	Keystroke <sup>1</sup>	Purpose
Move around the command line to make changes or corrections.	<b>Ctrl-B</b> or the left arrow key	Move the cursor back one character.
	<b>Ctrl-F</b> or the right arrow key	Move the cursor forward one character.
	<b>Ctrl-A</b>	Move the cursor to the beginning of the command line.
	<b>Ctrl-E</b>	Move the cursor to the end of the command line.
	<b>Esc-B</b>	Move the cursor back one word.
	<b>Esc-F</b>	Move the cursor forward one word.
	<b>Ctrl-T</b>	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.	<b>Ctrl-Y</b>	Recall the most recent entry in the buffer.
	<b>Esc-Y</b>	Recall the next buffer entry.  The buffer contains only the last 10 items that you have deleted or cut. If you press <b>Esc Y</b> more than ten times, you cycle to the first buffer entry.



Table 5-5 Editing Commands with Keystrokes (continued)

Capability	Keystroke <sup>1</sup>	Purpose
Delete entries if you make a mistake or change your mind.	<b>Delete</b> or <b>Backspace</b>	Erase the character to the left of the cursor.
	<b>Ctrl-D</b>	Delete the character at the cursor.
	<b>Ctrl-K</b>	Delete all characters from the cursor to the end of the command line.
	<b>Ctrl-U</b> or <b>Ctrl-X</b>	Delete all characters from the cursor to the beginning of the command line.
	<b>Ctrl-W</b>	Delete the word to the left of the cursor.
	<b>Esc-D</b>	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	<b>Esc-C</b>	Capitalize at the cursor.
	<b>Esc-L</b>	Change the word at the cursor to lowercase.
	<b>Esc-U</b>	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	<b>Ctrl-V</b> or <b>Esc Q</b>	
Scroll down a line or screen on displays that are longer than the terminal screen can display.	<b>Return</b>	Scroll down one line.
	<b>Space</b>	Scroll down one screen.
<b>Note</b> 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 <b>Return</b> and <b>Space</b> 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.	<b>Ctrl-L</b> or <b>Ctrl-R</b>	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 wrap-around 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 move back to verify the syntax at the beginning of the command.

To move 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 moved 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
```

After you complete the entry, press **Ctrl-A** to verify 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 shifted 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 with 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 protocol** the lines that contain *protocol* are not displayed, but the lines that contain *Protocol* 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** Choose **Start > Programs > Accessories > Telnet**.

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

**Step 2** When the Telnet window appears, click **Connect** and choose **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**.

**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 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.





## Troubleshooting

---

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

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

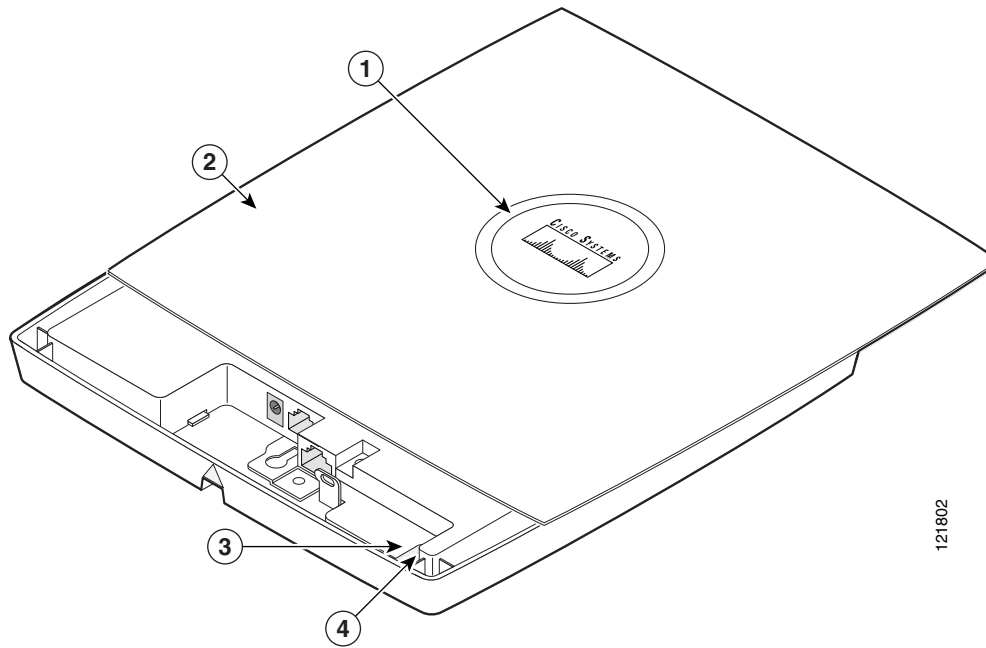
Sections in this chapter include:

- [Checking the Access Point LEDs, page 6-2](#)
- [Checking Basic Settings, page 6-4](#)
- [Low Power Condition, page 6-6](#)
- [Running the Carrier Busy Test, page 6-14](#)
- [Running the Ping Test, page 6-14](#)
- [Resetting to the Default Configuration, page 6-15](#)
- [Reloading the Access Point Image, page 6-16](#)
- [Obtaining the Access Point Image File, page 6-19](#)
- [Obtaining the TFTP Server Software, page 6-19](#)

## 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 (for additional information refer to the Event Log using the access point browser interface).

**Figure 6-1** Access Point LEDs



121802

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 2-9).

**Note**

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

**Note**

There can be slight color variations in the Status LED of each access point.

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	Blue-green	Initialize Flash file system.
	Off	Green	Pink	Flash memory test ok.
	Green	Off	Dark blue	Ethernet test ok.
	Green	Green	Green	Starting Cisco IOS.
Association status	—	—	Light green	Normal operating condition, but no wireless client devices are associated with the unit.
	—	—	Blue	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	—	—	Ethernet link is operational.
	Blinking green	—	—	Transmitting or receiving Ethernet packets.
	—	Blinking green	—	Transmitting or receiving radio packets.
	—	—	Blinking 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	Red	Blinking pink and off	Image recovery in progress and Mode button is released.

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 blue-green	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	—	—	Transmit or receive Ethernet errors.
	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio.
	Red	Red	Amber	Software failure; try disconnecting and reconnecting unit power.
	—	—	Amber	General warning, insufficient inline power (see the <a href="#">Low Power Condition</a> section).

## Checking Basic Settings

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

### Default IP Address Behavior

When you connect an 1130AG access point running Cisco IOS Release 12.3(2)JA or later software with a default configuration to your LAN, the access point requests an IP address from your DHCP server, and if it does not receive an IP address, it continues to send requests indefinitely.



## Default SSID and Radio Behavior

In Cisco IOS Release 12.3(2)JA2 and earlier, the access point radios are enabled by default and the default SSIDs are *tsunami*.

In Cisco IOS Release 12.3(4)JA, the access point radios are disabled by default, and there are no default SSIDs. You must create an SSID and enable the radio before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the [“Configuring Basic Security Settings” section on page 3-10](#) for instructions on configuring the SSID and the [“Enable Radio Interfaces” section on page 6-5](#) for instructions on enabling the radio interfaces.

## Enable Radio Interfaces

To enable the radio interfaces, follow these instructions:

- 
- Step 1** Use your web-browser to access your access point.
  - Step 2** When the Summary Status page displays, click **Network Interfaces > Radio0-802.11B** or **Radio0-802.11G** and the radio status page displays.
  - Step 3** Click **Settings** and the radio settings page displays.
  - Step 4** Click **Enable** in the Enable Radio field.
  - Step 5** Click **Apply**.
  - Step 6** Click **Network Interfaces > Radio0-802.11A** and the radio status page displays.
  - Step 7** Click **Settings** and the radio settings page displays.
  - Step 8** Click **Enable** in the Enable Radio field.
  - Step 9** Click **Apply**.
  - Step 10** Close your web-browser.
- 

## SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device’s SSID does not match the SSID of an access point in radio range, the client device will not associate. The access point default SSID is *tsunami*. Refer to the [“Using the Express Security Page” section on page 3-13](#) for instructions on how to configure an SSID.

**Note**

The default SSID (*tsunami*) is not supported in access points running Cisco IOS Release 12.3(4)JA. You must configure an SSID before client devices can associate to the access point.

## WEP Keys

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

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

## Security Settings

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

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



### Note

The access point MAC address that 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



### Warning

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

The access point can be powered from the 48-VDC power module or from an in-line power source. The access point supports the IEEE 802.3af power standard, Cisco Pre-Standard PoE protocol, and Cisco Intelligent Power Management for in-line power sources.

For full operation, the access point requires 12.95 W of power. The power module and Cisco Aironet power injectors are capable of supplying the required power for full operation, but some inline power sources are not capable of supplying 12.95 W. Also, some high-power inline power sources, might not be able to provide 12.95 W of power to all ports at the same time.



### Note

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



### Note

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

On power up, the access point is placed into low power mode (both radios are disabled), Cisco IOS software loads and runs, and power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on; otherwise, the access point remains in low power mode with the radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication, displays a low power message on the browser and serial interfaces, and creates an event log entry (see the [“Checking the Access Point LEDs”](#) section on page 6-2 and [“Inline Power Status Messages”](#) section on page 6-7).

## Intelligent Power Management

The access point requires 12.95 W of power for full power operation with both radios, but only needs 6.3 W of power when operating in low power mode with both radios disabled. To help avoid an over-current condition with low power sources and to optimize power usage on Cisco switches, Cisco developed Intelligent Power Management, which uses Cisco Discovery Protocol (CDP) to allow powered devices (such as your access point) to negotiate with a Cisco switch for sufficient power.

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



### Note

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

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

When the access point determines that sufficient power is not available for full power operation, an error message is logged and the Status LED turns amber to indicate low power mode (see the [“Checking the Access Point LEDs”](#) section on page 6-2 and the [“Inline Power Status Messages”](#) section on page 6-7).



### Tip

If your switch is capable of supplying sufficient power for full operation but the access point remains in low-power mode, your access point or your switch (or both) might be misconfigured (see [Table 6-2](#) and [Table 6-3](#)).

If your inline power source is not able to supply sufficient power for full operation, you should consider these options:

- Upgrade to a higher-powered switch
- Use a Cisco Aironet power injector on the switch port
- Use the 48-VDC power module to locally power the access point

## Inline Power Status Messages

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

- `%CDP_PD-4-POWER_OK: Full Power - AC_ADAPTOR inline power source—`This message indicates the access point is using the power module and can support full-power operation.

- `%CDP_PD-4-POWER_OK: Full Power - NEGOTIATED` inline power source—This message indicates the access point is operating at full power and has successfully negotiated for 12.95 W of power from a Cisco switch supporting Cisco Intelligent Power Management.
- `%CDP_PD-4-POWER_OK: Full Power - HIGH_POWER_CLASSIC` inline power source—This message indicates the access point is operating at full power because it has been configured for pre-standard compatibility mode and has detected a Cisco switch that does not support Intelligent Power Management but is able to supply sufficient power to the access point.
- `%CDP_PD-4-POWER_OK: Full Power - INJECTOR_CONFIGURED_ON_SOURCE` inline power source—This message indicates the access point is operating at full power because it is connected to a Cisco switch that supports Intelligent Power Management and the switch has been configured with *Power Inline Never*.
- `%CDP_PD-4-POWER_OK: Full power - INJECTOR_CONFIGURED_LOCAL` inline power source—This message indicates the access point is operating at full power because it has been configured to expect a power injector on this port.
- `%CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_PD` inline power source—This message indicates the access point is operating at full power because it has detected a CDP packet from another Cisco powerable device (PD). The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not transmit this type of CDP packet.
- `%CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_MULTIPLE_MACS_ON_HUB` inline power source—This message indicates the access point is operating at full power because it has detected multiple Cisco devices. The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not forward CDP packets.
- `%CDP_PD-4-POWER_OK: Full Power - NON_CISCO-NO_CDP_RECEIVED` inline power source—This message indicates the access point is operating at full power because it has not received any CDP packets within the timeout period. This condition indicates your access point is connected to a non-Cisco power source.




---

**Note** To prevent possible over-current conditions, the power source must be an IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.

---

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




---

**Note** A Cisco power injector might be required.

---

- `%CDP_PD-2-POWER_LOW: All radios disabled - LOW_POWER_CLASSIC` inline power source platform=<platform name> MAC address=<xxxx.xxxx.xxxx>—This message indicates the access point is in low power mode with all radios disabled and has detected a Cisco switch that is unable to supply sufficient power to the access point.

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




---

**Note** A Cisco power injector might be required. The MAC address of the switch port must be used when configuring a power injector to this port.

---

- `%CDP_PD-2-POWER_LOW: All radios disabled- HIGH_POWER_CLASSIC_NOT_CONFIGURED inline power source platform=<platform name> MAC address=<xxxx.xxxx.xxxx>`—This message indicates the access point is in low power mode with all radios disabled and has detected a Cisco switch that does not support Intelligent Power Management, but should be able to supply sufficient power. The access point must be configured for pre-standard compatibility.

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



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

## Configuring Power Using the CLI

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

```
[no] power inline negotiation {prestandard source | injector H.H.H}
(where H.H.H is the MAC address of the switch port to which the access point is connected)
```

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

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

Refer to [Table 6-2](#) for information on when to use this special Cisco IOS command and the corresponding Cisco switch power command.



### Caution

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



### Note

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


Table 6-2 Using Cisco IOS Commands

Power Source	Cisco IOS Commands	
	Access Point	Cisco Switch
AC power module	None required	<b>power inline never</b>
Cisco switch that supports Intelligent Power Management <sup>1</sup>	<b>no power inline negotiation prestandard source</b> <b>no power inline negotiation injector</b>	<b>power inline auto</b>
Cisco switch that does not support Intelligent Power Management <sup>1</sup>	<b>power inline negotiation prestandard source</b> <b>no power inline negotiation injector</b>	<b>power inline auto</b>
Power injector <sup>2</sup> used with a Cisco switch that supports Intelligent Power Management <sup>1</sup>	<b>no power inline negotiation prestandard source</b> <b>no power inline negotiation injector</b>	<b>power inline never<sup>3</sup></b>
Power injector <sup>2</sup> used with a Cisco switch that does not support Intelligent Power Management <sup>1</sup>	<b>no power inline negotiation prestandard source</b> <b>power inline negotiation injector xxxx.xxxx.xxxx</b> (where xxxx.xxxx.xxxx is the MAC address of the switch port to which the access point is connected) <b>Note</b> The MAC address might be available from the Inline Power Status message.	<b>power inline never</b>
Power injector used with a non-Cisco switch	None required	–
802.3af compliant non-Cisco switches	None required	–

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.
2. Power injector must be AIR-PWRINJ3 or AIR-PWRINJ-FIB.
3. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.

## Issuing the Cisco IOS Command Using the CLI

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

- Step 1** Connect a PC to the access point console port and use a terminal emulator to establish a session with the access point (refer to the “[Connecting to the Access Point Locally](#)” section on page 3-4).
- Step 2** From the privileged EXEC mode (refer to the “[Cisco IOS Command Modes](#)” section on page 5-2), enter the command below 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)
-  **Note** The MAC address might be available from the Inline Power Status message.
- **power inline negotiation prestandard source**
- Step 3** Enter the **write memory** command to save the setting to the access point memory.
- Step 4** Enter the **quit** command to exit the terminal session.

## Configuring the Access Point System Power Settings Using a Browser

You can also use your browser to set the access point System Power Settings.



**Note**

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



**Note**

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

[Figure 6-2](#) shows the system power setting options and indicates the power status of the access point.

**Figure 6-2 System Power Settings**

System Power Settings	
Power State:	<b>WARNING</b> ALL RADIOS DISABLED
Power Source:	LOW_POWER_CLASSIC (WS-C3524-PWR-XL on port 0009.7c05.200e)
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input checked="" type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="0040.9638.36b7"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	

121707

**Caution**

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

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

**Table 6-3 Access Point System Power Settings and Cisco Switch Commands**

Power Source	Access Point System Power Settings	Cisco Switch Power Command
AC power module	Configuration changes are not required	<b>power inline never</b>
Cisco switch that supports Intelligent Power Management <sup>1</sup>	Power Settings: <b>Power Negotiation</b> (selected) Power Injector: <b>Installed on Port with MAC Address</b> (unchecked)	<b>power inline auto</b>
Cisco switch that does not support Intelligent Power Management <sup>1</sup>	Power Settings: <b>Pre-standard Compatibility</b> (selected) Power Injector: <b>Installed on Port with MAC Address</b> (unchecked)	<b>power inline auto</b>
Power injector <sup>2</sup> used with a Cisco switch that supports Intelligent Power Management <sup>1</sup>	Power Settings: <b>Power Negotiation</b> (selected) Power Injector: <b>Installed on Port with MAC Address</b> (unchecked)	<b>power inline never<sup>3</sup></b>
Power injector <sup>2</sup> used with a Cisco switch that does not support Intelligent Power Management <sup>1</sup>	Power Settings: <b>Power Negotiation</b> (selected) Power Injector: <b>Installed on Port with MAC Address</b> (checked)	<b>power inline never</b>
Power injector used with a non-Cisco switch	Configuration changes are not required	–
802.3af compliant non-Cisco switches	Configuration changes are not required	–

1. You should check the release notes for your Cisco power source to determine which Cisco IOS release supports Intelligent Power Management. Support for Intelligent Power Management might not be currently available for your Cisco power source.
2. Power injector must be AIR-PWRINJ3 or AIR-PWRINJ-FIB.
3. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.



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

- 
- Step 1** Obtain the access point IP address and browse to your access point.
- Step 2** Perform one of these operations:
- When you browse to your access point operating in low-power mode, a Warning message appears indicating that all radios are disabled due to insufficient power. Click **OK** to jump to the System Power Settings located on the *System Software > System Configuration* page.
  - When you browse to your access point operating in full-power mode, choose **System Software > System Configuration**.
- Step 3** Choose one of these Power Settings options (see [Figure 6-2](#)):
- If your Cisco switch supports Intelligent Power Management negotiations, choose **Power Negotiation**.
  - If your Cisco switch does not support Intelligent Power Management negotiations, choose **Pre-standard Compatibility**.
  - If you are using a non-Cisco switch, changes to the power settings are not required.
- Step 4** If you are using a power injector with a Cisco switch, choose one of these Power setting options (see [Figure 6-2](#)):
- If your Cisco switch supports Intelligent Power Management negotiations, uncheck **Installed on Port with MAC address**.
  - If your Cisco switch does not support Intelligent Power Management, check **Installed on Port with MAC address** and ensure the MAC address for your switch port is displayed in the MAC address field. The HHHH.HHHH.HHHH indicates the MAC address contains 12 hexadecimal digits.



---

**Note** The MAC address field is not case-sensitive.

---

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



---

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

---

## Running the Carrier Busy Test

You can use the carrier busy test to determine the least congested channel for a radio interface (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 Test

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

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

Follow these steps to activate the ping test:

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

- c. Click **Start**.

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

- a. Enter the packet size in the Packet Size field.
- b. Click **Start** to activate the test.
- c. Click **Stop** to stop the test.

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

---

## Resetting to the Default Configuration

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



**Note**

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

---

For additional information on access point default behavior, refer to the [“Default IP Address Behavior” section on page 6-4](#) and the [“Default SSID and Radio Behavior” section on page 6-5](#).

## 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 2-9](#)).
- 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).

---

## Using the Web Browser Interface

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

**Step 1** Open your Internet browser.



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



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

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

## Using the MODE Button

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

**Note**

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

**Note**

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

Follow these steps to reload the access point image file:

- Step 1** The PC you intend to use must be configured with a static IP address in the same subnet as the access point.
- Step 2** Place a copy of the access point image file (such as *c1130-k9w7-tar.123-2.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 2-9).
- 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.

## 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.



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



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

**Step 2** Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password 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.123-2.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.



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



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

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

**Step 3** Enter your username in the User Name field.

- Step 4** Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.
  - Step 5** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
  - Step 6** Click the **TFTP Upgrade** tab.
  - Step 7** Enter the IP address for the TFTP server in the TFTP Server field.
  - Step 8** Enter the file name for the access point image file (such as *c1130-k9w7-tar.123-2.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 1130AG Series (Cisco IOS Software)**.
  - Step 4** Click on the access point image file, such as *c1130-k9w7-tar.123-2.JA.tar*.
  - Step 5** On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply.
  - Step 6** Click **Submit**.
  - Step 7** Read and accept the terms and conditions of the Software License Agreement.
  - Step 8** Select the image file again to download it.
  - Step 9** Download and save the image file to your hard drive and then exit the Internet browser.
- 

## Obtaining the TFTP Server Software

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

<http://tftpd32.jounin.net>

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







## Translated Safety Warnings

---

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

- [Statement 245B—Explosive Device Proximity Warning, page A-2](#)
- [Statement 332—Antenna Installation Warning, page A-3](#)
- [Statement 353—Power Source Warning, page A-3](#)
- [Statement 1001—Work During Lightning Activity Warning, page A-5](#)
- [Statement 1004—Installation Instructions Warning, page A-6](#)
- [Statement 1005—Circuit Breaker \(20A\) Warning, page A-7](#)

## Statement 245B—Explosive Device Proximity Warning


**Warning**

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

Statement 245B

**Waarschuwing**

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

**Varoitus**

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

**Attention**

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

**Warnung**

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

**Avvertenza**

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

**Advarsel**

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

**Aviso**

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

**¡Advertencia!**

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

**Varning!**

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

## Statement 332—Antenna Installation Warning



<b>Warning</b>	<b>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.</b> Statement 332
<b>Waarschuwing</b>	<b>Om te voldoen aan de FCC radiofrequentie (RF) blootstellingslimieten dienen antennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.</b>
<b>Varoitus</b>	<b>FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan antennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.</b>
<b>Attention</b>	<b>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.</b>
<b>Warnung</b>	<b>Um die in den FCC-Richtlinien festgelegten Expositionshöchstgrenzen für Radiofrequenzen (RF) nicht zu überschreiten, sollten Antennen mindestens 20 cm entfernt von Personen aufgestellt werden.</b>
<b>Avvertenza</b>	<b>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.</b>
<b>Advarsel</b>	<b>I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal antenner befinne seg på en avstand av minst 20 cm eller mer fra mennesker.</b>
<b>Aviso</b>	<b>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.</b>
<b>¡Advertencia!</b>	<b>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.</b>
<b>Varning!</b>	<b>För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör antenner placeras på minst 20 cm avstånd från alla människor.</b>

## Statement 353—Power Source Warning



<b>Warning</b>	<b>This product must be connected to a Power over Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.</b> Statement 353
<b>Waarschuwing</b>	<b>Dit product moet worden verbonden met een stroomvoorziening die compatibel is met PoE (Power over Ethernet) IEEE 802.3af of een beperkte stroomvoorziening die compatibel is met IEC60950.</b>

<b>Varoitus</b>	<b>Tämä tuote on liitettävä PoE (Power over Ethernet) IEEE 802.3af -yhteensopivaan virtalähteeseen tai IEC60950-yhteensopivaan rajoitettuun virtalähteeseen.</b>
<b>Attention</b>	<b>Ce produit doit être connecté à une source d'alimentation électrique par câble Ethernet (PoE) conforme à la norme IEEE 802.3af ou à une source d'alimentation limitée conforme à la norme IEC60950.</b>
<b>Warnung</b>	<b>Dieses Produkt muss entweder an eine Stromquelle angeschlossen sein, die mit dem IEEE 802.3af-Standard Power over Ethernet (PoE) kompatibel ist oder an eine Stromquelle für geringe Leistungen, die IEC60950-kompatibel ist.</b>
<b>Avvertenza</b>	<b>Questo prodotto deve essere connesso a una fonte di alimentazione di tipo PoE (Power over Ethernet) conforme a IEEE 802.3af o a una fonte di alimentazione conforme a IEC60950.</b>
<b>Advarsel</b>	<b>Dette produktet må være koblet til en Power over Ethernet (PoE) IEEE 802.3af-kompatibel strømkilde eller en IEC60950-kompatibel begrenset strømkilde.</b>
<b>Aviso</b>	<b>Este produto tem de estar ligado a uma fonte de alimentação compatível com a norma IEEE 802.3af, também conhecida pela sigla Power over Ethernet (PoE), ou a uma fonte de alimentação limitada compatível com a norma IEC60950.</b>
<b>¡Advertencia!</b>	<b>Debe conectar este producto a una fuente de alimentación sobre ethernet (PoE) conforme con el estándar IEEE 802.3af, o a una fuente limitada conforme con el estándar IEC60950.</b>
<b>Varning!</b>	<b>Denna produkt måste vara ansluten till en PoE IEEE 802.3af-kompatibel strömkälla eller en IEC60950-kompatibel begränsad strömkälla.</b>
<b>Figyelem</b>	<b>Ezt a készüléket vagy az IEEE 802.3af szabványnak megfelelő, a tápellátást Etherneten keresztül kapó (power-over-ethernet, PoE) tápforráshoz, vagy az IEC60950 szabványnak megfelelő, korlátozott tápforráshoz kell csatlakoztatni.</b>
<b>Предупреждение</b>	<b>Это устройство может быть подключено к источнику питания для подачи питания по сети Ethernet (PoE), удовлетворяющему требованиям стандарта IEEE 802.3af, или источнику питания ограниченного применения, удовлетворяющему требованиям стандарта IEC60950.</b>
<b>警告</b>	<b>本产品必须连接到以太网供电型 (Power-Over-Ethernet, 简称PoE) IEEE802.3af 电源或 IEC60950 限制型电源。</b>
<b>警告</b>	<b>この製品はPoE方式のIEEE 802.3af対応の電源またはIEC60950対応の制限電源に接続してください。</b>

# 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。**

# 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。**

## Statement 1005—Circuit Breaker (20A) Warning



<b>Warning</b>	<b>This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20A Statement 1005</b>
<b>Waarschuwing</b>	<b>Dit product is afhankelijk van de installatie van het gebouw voor beveiliging tegen kortsluiting (overstroom). Controleer of de beschermingsinrichting niet meer dan: 20A is.</b>
<b>Varoitus</b>	<b>Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että suojalaitteen mitoitus ei ole yli: 20A</b>
<b>Attention</b>	<b>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 : 20A</b>
<b>Warnung</b>	<b>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: 20A beträgt.</b>
<b>Avvertenza</b>	<b>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: 20A</b>
<b>Advarsel</b>	<b>Dette produktet er avhengig av bygningens installasjoner av kortslutnings (overstrøm)-beskyttelse. Påse at verneenheten ikke er merket høyere enn: 20A</b>
<b>Aviso</b>	<b>Este produto depende das instalações existentes para proteção contra curto-circuito (sobrecarga). Assegure-se de que o fusível ou disjuntor não seja superior a: 20A</b>
<b>¡Advertencia!</b>	<b>Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) del edificio. Asegúrese de que el dispositivo de protección no sea superior a: 20A</b>
<b>Varning!</b>	<b>Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att skyddsanordningen inte har högre märkvärde än: 20A</b>
<b>Figyelem</b>	<b>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: 20A</b>

## ■ Statement 1005—Circuit Breaker (20A) Warning

- Предупреждение**    Защита устройства от короткого замыкания (перегрузки) осуществляется с помощью оборудования, являющегося частью электропроводки здания. Убедитесь, что номинал защитного устройства не превышает:  
**20A**
- 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：  
**20A**
- 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。  
**20A**
-





## Declarations of Conformity and Regulatory Information

---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1130AG 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](#)

# 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.

## 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 entsprechedenen Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
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 ουσιώδεις 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

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



## Declaration of Conformity for RF Exposure

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

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

**Note**

---

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

---

# Guidelines for Operating Cisco Aironet Access Points in Japan

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

## Model:

AIR-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

# Declaration of Conformity Statements

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

<http://www.ciscofax.com>

## Declaration of Conformity Statements for European Union Countries

The Declaration of Conformity statement for the European Union countries is listed below:



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

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

Declare under our sole responsibility that the product,

*Product: AIR-AP1131AG-E-K9*  
*Cisco Aironet 1130AG Series IEEE802.11 a/b/g Access Point*

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

The following standards were applied:

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

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

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

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

The product carries the CE Mark:



Date & Place of Issue:            1 April 2005, San Jose

**Signature:**

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

Additional information:

*EMC Test Report:*                    *Cisco Systems EDCS-382866*  
*Safety Test Report:*                *CCS: 04U2603-8; UL: E-145532*  
*Radio Test Report:*                *CCS: 04U2603-4 (2.4 GHz) & 04U2603-11 (5 GHz)      DofC 441919*






## Access Point Specifications

Table C-1 lists the technical specifications for the Cisco Aironet 1130AG Series 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)  1130AG series power module: 32 to 104°F (0 to 40°C)		
Weight	Without mounting hardware: 1.48 lbs (0.67 kg)		
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 3-dBi antennas.		A diversity system with two integrated 4.5-dBi antennas.

Table C-1 Access Point Specifications (continued)

Category	802.11b Radio Specifications	802.11g Radio Specifications	802.11a Radio Specifications
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	450 ft at 1 Mbps 360 ft at 11 Mbps	400 ft at 6 Mbps 100 ft at 54 Mbps	325 ft at 6 Mbps 80 ft at 54 Mbps
Compliance	<p>The 1200 series access point complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings.</p> <p> <b>Caution</b> Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.</p>		
Safety	<p>Designed to meet:</p> <ul style="list-style-type: none"> <li>UL 60950-1</li> <li>CAN/CSA C22.2 No. 60950-1</li> <li>UL 2043</li> <li>EN 60950-1</li> <li>IEC 60950-1</li> </ul>		
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		



## 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](#)

# 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	–	–	–

## IEEE 802.11a (5-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain.

Table D-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 ID	Center Freq (MHz)	Maximum Conducted Power Levels (dBm) in the Regulatory Domains								
		Americas (-A)	China (-C)	EMEA (-E)	Japan (-J)	North America (-N)	-	-	-	-
<b>5150 to 5250 MHz</b>										
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	-	-	-	-
<b>5250 to 5350 MHz</b>										
52	5260	17	-	17	-	17	-	-	-	-
56	5280	17	-	17	-	17	-	-	-	-
60	5300	17	-	17	-	17	-	-	-	-
64	5320	17	-	17	-	17	-	-	-	-
<b>5450 to 5725 MHz</b>										
100	5500	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
104	5520	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
108	5540	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
112	5560	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
116	5580	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
120	5600	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
124	5620	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
128	5640	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
132	5660	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
136	5680	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
140	5700	17 <sup>1</sup>	-	17 <sup>1</sup>	-	-	-	-	-	-
<b>5725 to 5850 MHz</b>										
149	5745	17	17	-	-	17	-	-	-	-
153	5765	17	17	-	-	17	-	-	-	-
157	5785	17	17	-	-	17	-	-	-	-
161	5805	17	17	-	-	17	-	-	-	-
165	5825	-	-	-	-	-	-	-	-	-

1. Requires Cisco IOS Release 12.3(4)JA software.





## 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](#)

# 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 or can be built using the pinouts in this appendix.



**Note**

The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/en/US/ordering/index.shtml> to order a serial cable.

# Console Port Signals and Pinouts

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



**Note**

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



**Note**

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

Table E-1 lists the signals and pinouts for the console RJ-45 to DB-9 serial cable.

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

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

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





- 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.

- BPSK** Binary phase shift keying is 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.
- CCKM** Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
- 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.

---

## 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.

---

## 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.

**OFDM** Orthogonal frequency division multiplex is a modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

---

## P

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

---

## Q

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

---

## R

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

<b>receiver sensitivity</b>	A measurement of the weakest signal a receiver can receive and still correctly translate it into data.
<b>RF</b>	Radio frequency. A generic term for radio-based technology.
<b>roaming</b>	A feature of some Access Points that allows users to move through a facility while maintaining an unbroken connection to the LAN.
<b>RP-TNC</b>	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**

<b>spread spectrum</b>	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.
<b>SSID</b>	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**

<b>transmit power</b>	The power level of radio transmission.
-----------------------	--

---

**U**

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

---

**W**

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



---

## A

- abbreviating commands [5-3](#)
- access point image [6-16](#)
- antenna
  - connectors [C-1](#)
- Apply button [4-4](#)

---

## B

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

---

## C

- Cancel button [4-4](#)
- CLI
  - abbreviating commands [5-3](#)
  - command modes [5-2](#)
  - editing features
    - enabling and disabling [5-6](#)
    - keystroke editing [5-6](#)
    - wrapped lines [5-7](#)
  - error messages [5-4](#)
  - filtering command output [5-8](#)
  - getting help [5-3](#)
  - history
    - changing the buffer size [5-5](#)
    - described [5-4](#)
    - disabling [5-5](#)
    - recalling commands [5-5](#)
  - no and default forms of commands [5-4](#)
  - terminal emulator settings [3-5](#)
- command-line interface

See CLI

- command modes [5-2](#)
- commands
  - abbreviating [5-3](#)
  - no and default [5-4](#)
- connectors [C-1](#)
- console port [E-2](#)

---

## D

- data rates [C-2](#)
- declarations of conformity [B-1](#)
- default, configuration, resetting [6-15](#)
- default commands [5-4](#)

---

## E

- editing features
  - enabling and disabling [5-6](#)
  - keystrokes used [5-6](#)
  - wrapped lines [5-7](#)
- EIRP, maximum [D-2 to ??](#), [D-2 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](#)
- frequency range [C-2](#)

**G**

global configuration mode [5-2](#)

**H**

help, for the command line [5-3](#)

history

changing the buffer size [5-5](#)

described [5-4](#)

disabling [5-5](#)

recalling commands [5-5](#)

Home button [4-3](#)

**I**

indicators [6-2](#)

input power [C-1](#)

installation guidelines [2-3](#)

interface configuration mode [5-2](#)

**K**

key features [1-2](#)

**M**

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

Mode button [6-17](#)

modulation [C-2](#)

**N**

no commands [5-4](#)

**O**

OK button [4-4](#)

operating temperature [C-1](#)

**P**

package contents [2-3](#)

password reset [6-15](#)

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

power

connecting [2-20](#)

input [C-1](#)

output [C-1](#)

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 [6-16](#)

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](#)

status indicators [C-1](#)

**T**

Telnet [3-14, 3-15](#)

temperature

operating [C-1](#)



terminal emulator [3-5](#)

TFTP server [6-17](#)

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 [4-3](#)

    compatible browsers [4-1](#)

web site, Cisco Software Center [6-19](#)

weight [C-1](#)

WEP key [6-6](#)

Wi-Fi Protected Access (WPA) [3-12](#)

