



Cisco Aironet 1130AG Series Access Point Hardware Installation Guide

June 2008

Americas Headquarters

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

Text Part Number: OL-8369-05

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

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

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

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

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

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

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

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

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

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

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

CCSP, the Cisco Square Bridge logo, 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, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

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



CONTENTS

Preface ix

- Audience i-ix
- Purpose i-ix
- Organization i-ix
- Conventions i-x
- Related Publications i-xii
- Obtaining Documentation, Obtaining Support, and Security Guidelines i-xii
- Locating the Product Serial Number i-xiii

CHAPTER 1

Overview 1-1

- Product Terminology 1-1
- Autonomous Access Points 1-1
- Lightweight Access Points 1-1
- Guidelines for Using 1130AG Series Lightweight Access Points 1-2
- Hardware Features 1-3
 - Single or Dual-Radio Operation 1-4
 - Ethernet Port 1-4
 - Console Port 1-4
 - LEDs 1-4
 - Power Sources 1-5
 - UL 2043 Certification 1-5
 - Anti-Theft Features 1-6
- Network Examples with Autonomous Access Points 1-7
 - Root Unit on a Wired LAN 1-8
 - Repeater Unit that Extends Wireless Range 1-9
 - Central Unit in an All-Wireless Network 1-10
 - Workgroup Bridge Configuration 1-10
- Network Example with Lightweight Access Points 1-11

CHAPTER 2

Installing the Access Point 2-1

- Safety Information 2-2
 - FCC Safety Compliance Statement 2-2
 - General Safety Guidelines 2-2

Warnings	2-2
Unpacking the Access Point	2-3
Package Contents	2-3
Basic Installation Guidelines	2-4
Controller Discovery Process for Lightweight Access Points	2-4
Deploying the Access Points on the Wireless Network	2-5
Access Point Layout and Connectors	2-6
Mounting Plate	2-7
Suspended Ceiling Adjustable T-Rail Clips	2-8
Opening the Access Point Cover	2-11
Mounting the Access Point on a Horizontal Surface	2-12
Mounting the Access Point Below a Suspended Ceiling	2-13
Mounting the Access Point Above a Suspended Ceiling	2-14
Mounting Access Point on a Network Cable Box	2-16
Mounting Access Point on a Desktop or Shelf	2-16
Attaching the Access Point to the Mounting Plate	2-16
Securing the Access Point	2-18
Using a Security Cable	2-18
Securing the Access Point to the Mounting Plate	2-19
Connecting the Ethernet and Power Cables	2-21
Connecting to an Ethernet Network with an Inline Power Source	2-22
Connecting to an Ethernet Network with Local Power	2-23
Rotating the Cisco Logo	2-24

CHAPTER 3

Troubleshooting Autonomous Access Points	3-1
Checking the Autonomous Access Point LEDs	3-2
Checking Basic Settings	3-4
Default IP Address Behavior	3-4
Default SSID and Radio Behavior	3-4
Enable Radio Interfaces	3-5
SSID	3-5
WEP Keys	3-5
Security Settings	3-5
Low Power Condition for Autonomous Access Points	3-6
Intelligent Power Management	3-6
Inline Power Status Messages	3-7
Configuring Power Using the CLI	3-10
Issuing the Cisco IOS Command Using the CLI	3-11

Configuring the Access Point System Power Settings Using a Browser	3-12
Running the Carrier Busy Test	3-14
Running the Ping Test	3-15
Resetting to the Default Configuration	3-15
Using the MODE Button	3-16
Using the Web Browser Interface	3-16
Reloading the Access Point Image	3-17
Using the MODE Button	3-17
Web Browser Interface	3-18
Browser HTTP Interface	3-18
Browser TFTP Interface	3-19
Obtaining the Access Point Image File	3-19
Connecting to the Access Point Console Port	3-20
Obtaining the TFTP Server Software	3-21

CHAPTER 4

Troubleshooting Lightweight Access Points	4-1
Guidelines for Using 1130AG Series Lightweight Access Points	4-2
Using DHCP Option 43	4-2
Checking the Lightweight Access Point LEDs	4-2
Low Power Condition for Lightweight Access Points	4-6
Intelligent Power Management	4-6
Configuring Power Using Controller CLI Commands	4-7
Manually Configuring Controller Information Using the Access Point CLI	4-8
Configuring Controller Information	4-9
Clearing Manually Entered Controller Information	4-9
Manually Resetting the Access Point to Defaults	4-9
Returning the Access Point to Autonomous Mode	4-9
Using a WLAN Controller to Return the Access Point to Autonomous Mode	4-10
Using the MODE Button to Return the Access Point to Autonomous Mode	4-10
MODE Button Setting	4-11
Obtaining the Autonomous Access Point Image File	4-11
Connecting to the Access Point Console Port	4-12
Obtaining the TFTP Server Software	4-13

APPENDIX A

Translated Safety Warnings A-1

APPENDIX B

Declarations of Conformity and Regulatory Information B-1

Manufacturers Federal Communication Commission Declaration of Conformity Statement	B-2
VCCI Statement for Japan	B-3
Industry Canada	B-4
Canadian Compliance Statement	B-4
European Community, Switzerland, Norway, Iceland, and Liechtenstein	B-4
Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive)	B-5
Declaration of Conformity for RF Exposure	B-7
Guidelines for Operating Cisco Aironet Access Points in Japan	B-8
Japanese Translation	B-8
English Translation	B-8
Administrative Rules for Cisco Aironet Access Points in Taiwan	B-9
Access Points with IEEE 802.11a Radios	B-9
Chinese Translation	B-9
English Translation	B-9
All Access Points	B-10
Chinese Translation	B-10
English Translation	B-10
Declaration of Conformity Statements	B-11
Declaration of Conformity Statements for European Union Countries	B-11

APPENDIX C

Access Point Specifications C-1

APPENDIX D

Channels and Maximum Power Levels D-1

APPENDIX E

Console Cable Pinouts E-1

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

APPENDIX F

Priming Lightweight Access Points Prior to Deployment F-1

APPENDIX G

Configuring DHCP Option 43 for Lightweight Access Points G-1

Overview	G-2
Configuring Option 43 for 1000 and 1500 Series Access Points	G-3
Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Lightweight Access Points	G-4

GLOSSARY

INDEX



Preface

Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1130AG Series Access Point. The 1130AG series access point is available in autonomous and lightweight configurations.

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

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

Purpose

This guide provides the information you need to install your autonomous or lightweight access point.

For detailed information about Cisco IOS commands used with autonomous access points, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS Release 12.3 commands, refer to the Cisco IOS documentation set available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Cisco IOS Software > Cisco IOS Software Releases 12.3 Mainline**.

For information about Cisco Wireless LAN Controllers, refer to the Cisco documentation sets available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Wireless** and the documentation is listed under the “Wireless LAN Controllers” section.

Organization

This guide is organized into these chapters:

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

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

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

[Chapter 4, “Troubleshooting Lightweight Access Points,”](#) provides troubleshooting procedures for basic problems with the lightweight 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 Maximum 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.

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

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

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

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

Interactive examples use these conventions:

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

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



Tip

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



Note

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

**Caution**

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

**Warning**

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

Waarschuwing

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

Varoitus

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

Attention

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

Warnung

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

Avvertenza

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

Advarsel

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

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

¡Advertencia! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado “Translated Safety Warnings.”)

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix “Translated Safety Warnings” [Översatta säkerhetsvarningar].)

Related Publications

These documents provide complete information about the autonomous access point:

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

These documents provide complete information about the lightweight access point:

- *Release Notes for Cisco Aironet Access Points*
- *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 Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the 1130AG series access point documentation, click **Cisco Aironet 1130AG Series** listed under “Access Points.”

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

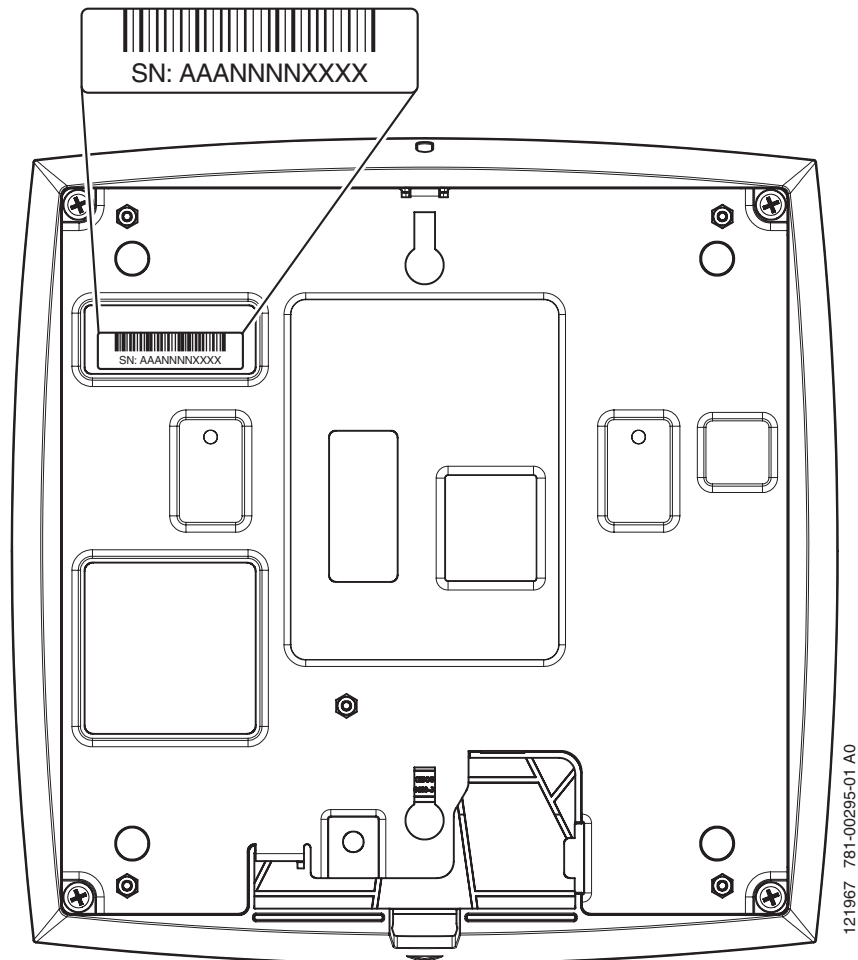
For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation,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

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

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-AP1131AG-A-k9* or *AIR-LAP1131AG-A-k9*
- Serial number, such as *VDF0636XXXX* (11 alphanumeric digits)
- MAC address, such as *00abc65094f3* (12 hexadecimal digits)
- Location of manufacture, such as *Made in Singapore*

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



CHAPTER 1

Overview

The Cisco Aironet 1130AG Series Access Point is available in autonomous and lightweight configurations. The autonomous access points can support standalone network configurations with all configuration settings maintained within the access points. The lightweight access points operate in conjunction with a Cisco wireless LAN controller with all configuration information maintained within the controller.

Product Terminology

The following terms refer to the autonomous and lightweight products:

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

Autonomous Access Points

Cisco Aironet 1130AG Series Access Point (models: AIR-AP1131AG and AIR-AP1131G) supports a management system based on Cisco IOS software. The 1130AG series access point is a Wi-Fi certified, wireless LAN transceiver. The 1131AG access point uses dual integrated radios (IEEE 802.11g and IEEE-802.11a). The 1131G access point uses a single integrated radio (IEEE 802.11g).

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

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

Lightweight Access Points

The Cisco Aironet 1130AG Series Access Point (models: AIR-LAP1131AG and AIR-LAP1131G) is part of the Cisco Integrated Wireless Network Solution and requires no manual configuration before they are mounted. The lightweight access point is automatically configured by a Cisco wireless LAN controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

The lightweight 1131AG access point contains two integrated radios: a 2.4-GHz radio (IEEE 802.11g) and a 5-GHz radio (IEEE 801.11a). The lightweight 1131G access point contains one integrated radio: a 2.4-GHz radio (IEEE 802.11g). Using a controller, you can configure the radio settings.

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

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

In an LWAPP environment, a lightweight access point discovers a controller by using LWAPP discovery mechanisms and then sends it an LWAPP join request. The controller sends the lightweight access point an LWAPP join response allowing the access point to join the controller. When the access point is joined, the access point downloads its software if the versions on the access point and controller do not match. After an access point joins a controller, you can reassign it to any controller on your network.

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

This chapter provides information on the following topics:

- [Guidelines for Using 1130AG Series Lightweight Access Points, page 1-2](#)
- [Hardware Features, page 1-3](#)
- [Network Examples with Autonomous Access Points, page 1-7](#)

Guidelines for Using 1130AG Series Lightweight Access Points

You should keep these guidelines in mind when you use a 1130AG series lightweight access point:

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

Hardware Features

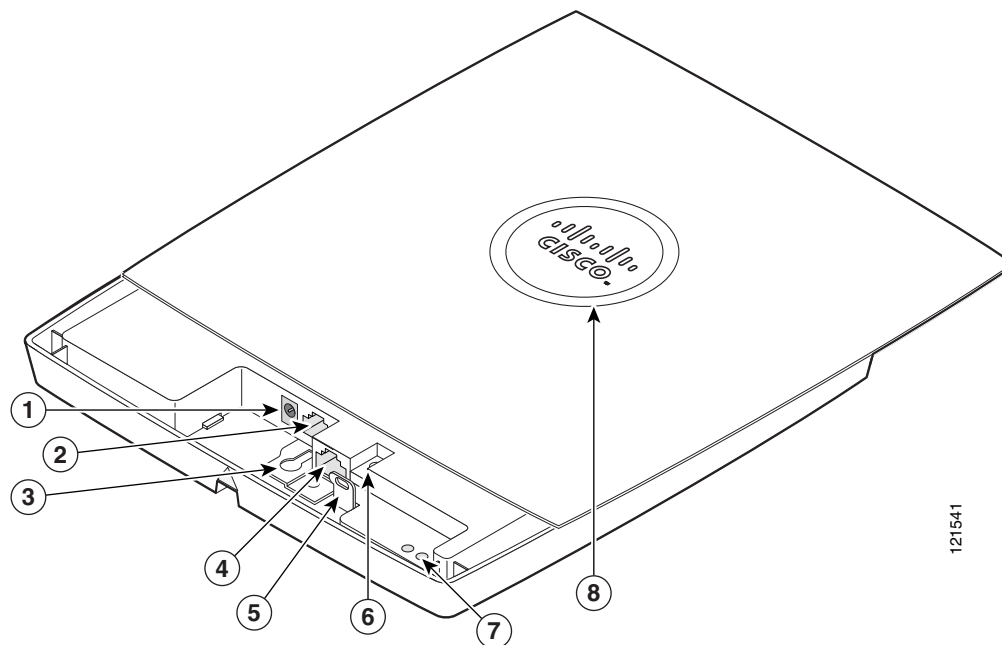
Key hardware features of the access point include:

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

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



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

Single or Dual-Radio Operation

The 1131AG access point supports simultaneous radio operation using a 2.4-GHz 802.11g radio and a 5-GHz 802.11a radio. The 1131G access point supports a single 2.4-GHz 802.11g 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 the [“Locating the Product Serial Number”](#) section on page xiii). 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 might not fit.

Console Port

The serial console port can be used to monitor the access point power-up sequences 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 might not fit.

LEDs

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

- 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.

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 (refer to the [“Low Power Condition for Autonomous Access Points”](#) section on page 3-6 or the [“Low Power Condition for Lightweight Access Points”](#) section on page 4-6).

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

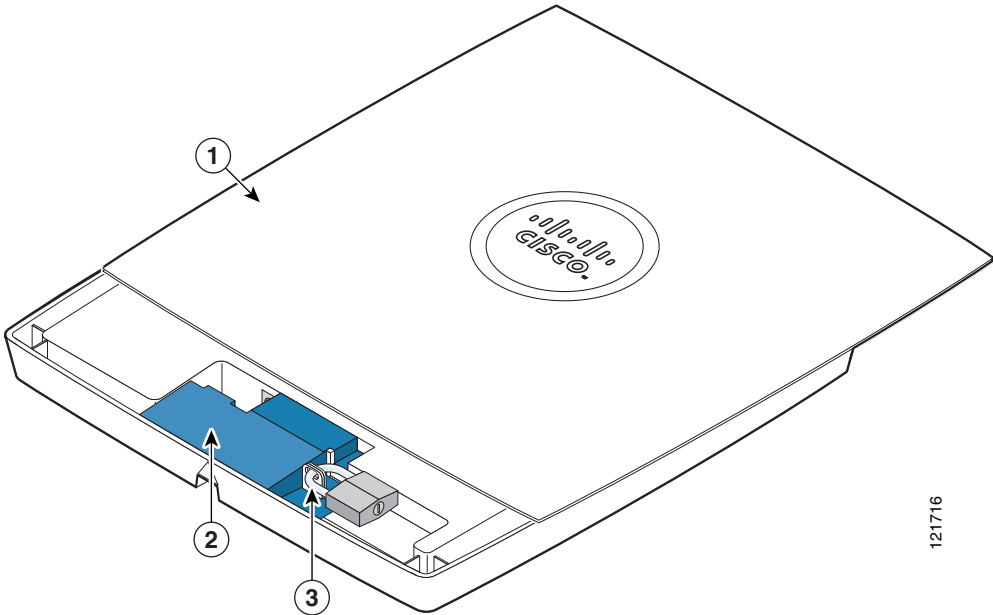
There are three methods of securing the access point:

- 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 2-18).
- Security hasp adapter—When you mount the access point 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



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

- Security screw—The access point contains a security screw hole (see Figure 1-3) that can be used to 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 over-head mounting positions.



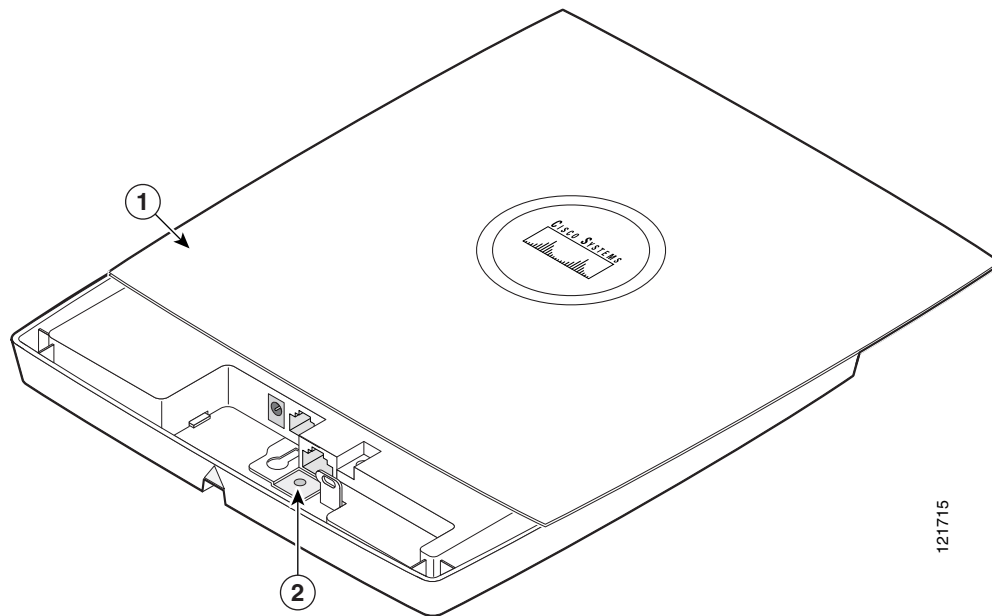
Note The supplied #8 Philips head screw provides minimal anti-theft protection.

- 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



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

Network Examples with Autonomous Access Points

This section describes the autonomous access point's role in three common wireless network configurations. The autonomous 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 or workgroup bridge roles require a specific configuration setting.

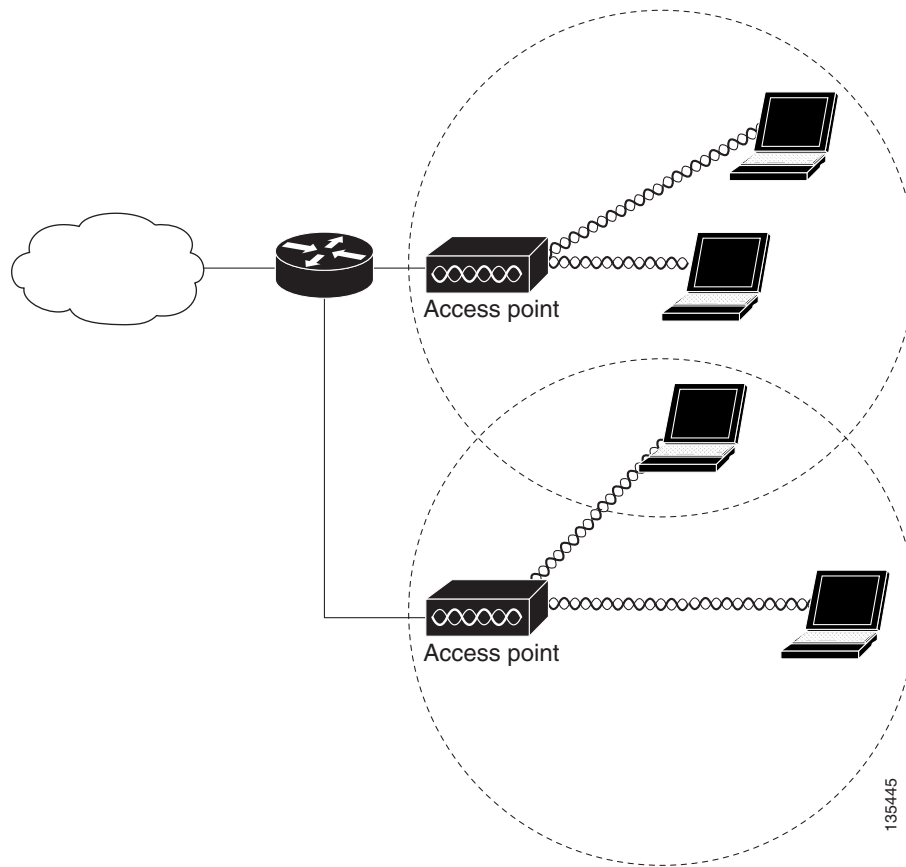
The autonomous 1130AG series access point supports these operating wireless modes:

- Root access point—Connected to a wired LAN and supports wireless clients.
- Repeater access point—Not connected to a wired LAN, associates to a root access point, and supports wireless clients
- Workgroup bridge—Not connected to a wired LAN, associates to a root access point or bridge, and supports wired network devices.

Root Unit on a Wired LAN

An autonomous access point connected directly to a wired LAN provides a connection point for wireless users. If more than one autonomous access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. [Figure 1-4](#) shows access points acting as root units on a wired LAN.

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



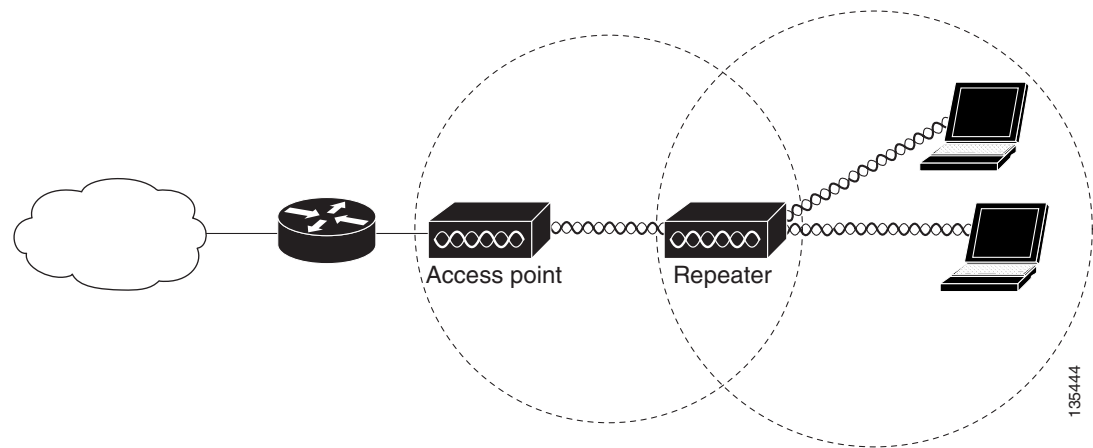
Repeater Unit that Extends Wireless Range

An autonomous 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 autonomous 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.

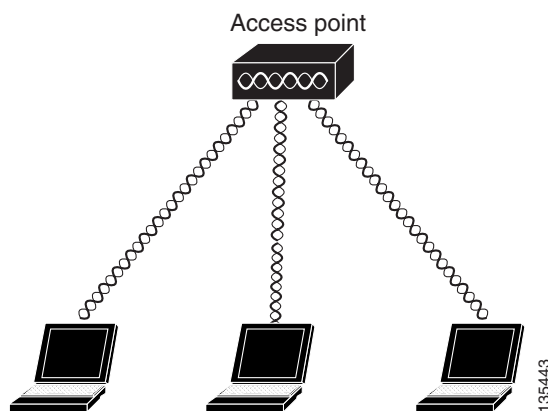
Figure 1-5 Access Point as Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an autonomous access point acts as a stand-alone root unit. The autonomous 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 autonomous access point in an all-wireless network.

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

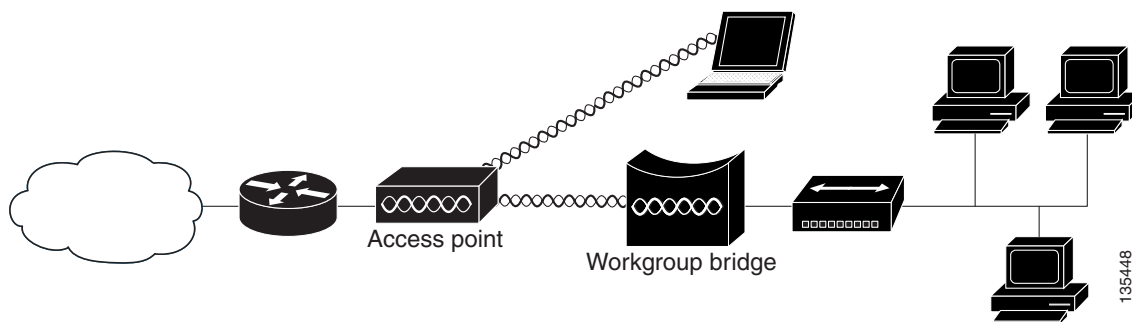


Workgroup Bridge Configuration

When configured in the workgroup bridge mode, the autonomous unit provides a wireless connection for remote wired devices to a Cisco Aironet access point or to a Cisco Aironet bridge.

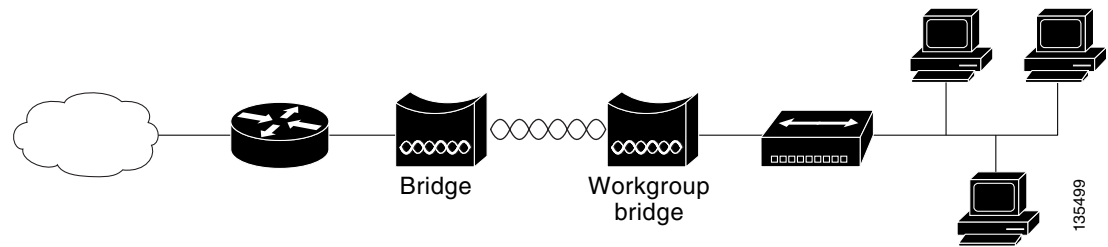
In [Figure 1-7](#), the unit is configured in workgroup bridge mode and is associated to a Cisco Aironet access point as a wireless client device. This configuration allows the Ethernet-enabled devices to pass Ethernet traffic to and from the main LAN using the workgroup bridge.

Figure 1-7 Workgroup Bridge Configuration 1



In [Figure 1-8](#), the autonomous unit is configured in workgroup bridge mode and is associated to a Cisco Aironet root bridge as a wireless bridge device. This configuration allows the Ethernet-enabled devices pass Ethernet traffic to and from the main LAN using the workgroup bridge. The main advantage of this configuration is that the wireless communication link can be over a longer distance than an access point supports. Typically, an access point can communicate over approximately a 1-mile range; however, the bridge-to-bridge wireless link can communicate over approximately a 21-mile range.

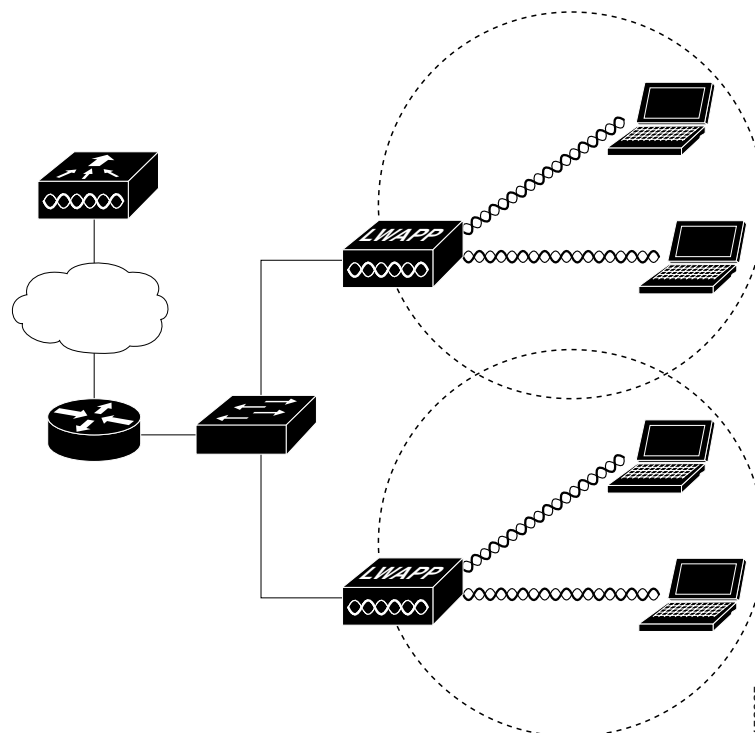
Figure 1-8 Workgroup Bridge Configuration 2



Network Example with Lightweight Access Points

The lightweight access points support Layer 3 network operation. Lightweight access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco. [Figure 1-9](#) illustrates a typical network configuration containing lightweight access points.

Figure 1-9 Typical Lightweight Access Point Network Configuration Example





CHAPTER 2

Installing the Access Point

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

- [Safety Information, page 2-2](#)
- [Warnings, page 2-2](#)
- [Unpacking the Access Point, page 2-3](#)
- [Basic Installation Guidelines, page 2-4](#)
- [Controller Discovery Process for Lightweight Access Points, page 2-4](#)
- [Deploying the Access Points on the Wireless Network, page 2-5](#)
- [Opening the Access Point Cover, page 2-11](#)
- [Opening the Access Point Cover, page 2-11](#)
- [Mounting the Access Point on a Horizontal Surface, page 2-12](#)
- [Mounting the Access Point Below a Suspended Ceiling, page 2-13](#)
- [Mounting the Access Point Above a Suspended Ceiling, page 2-14](#)
- [Mounting Access Point on a Network Cable Box, page 2-16](#)
- [Mounting Access Point on a Desktop or Shelf, page 2-16](#)
- [Attaching the Access Point to the Mounting Plate, page 2-16](#)
- [Securing the Access Point, page 2-18](#)
- [Connecting the Ethernet and Power Cables, page 2-21](#)

Safety Information

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

FCC Safety Compliance Statement

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

General Safety Guidelines

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

Warnings

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



Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

Statement 1071

SAVE THESE INSTRUCTIONS



Warning

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



Warning

This product 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

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 or Cisco Aironet 1130AG Series Lightweight 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
- Product quick start guide
- Translated safety warnings document
- Cisco product registration and Cisco documentation feedback cards

Basic Installation Guidelines

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

- Ensure a site survey has been performed to determine the optimum placement of access points.
- For lightweight access points, check the latest release notes to ensure that your controller software version supports the access points to be installed. You can find the controller release notes by selecting your controller under **Wireless LAN Controllers** at this URL:
http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html
- Ensure that access points are not mounted closer than 20 cm (7.9 in) from the body of all persons.
- Do not mount the access point within 3 feet of metal obstructions.
- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.
- Do not mount the access point outside of buildings.
- The integrated antenna design of the 1130AG series access point is designed for horizontal surfaces, (table top and ceiling installations). When mounted to such surfaces, the integrated antennas produce the best antenna radiation pattern. For advanced features such as voice, location, and rogue access point detection, ceiling mounting is strongly recommended. However, for smaller areas such as conference rooms, kiosks, transportation, and hot-spot usage where the customer is concerned primarily with data coverage and not advanced features, this unit may be wall mounted using the supplied plastic wall anchors and #8 screws.

Controller Discovery Process for Lightweight Access Points

The lightweight access point supports these controller discovery processes:

- DHCP server discovery—Uses DHCP Option 43 to provide controller IP addresses to the lightweight access points. Cisco switches support a DHCP server option. For additional information, refer to the “[Configuring DHCP Option 43 for Lightweight Access Points](#)” section on page G-1.
- DNS server discovery—The lightweight access point uses the name `CISCO-LWAPP-CONTROLLER.<local domain>` to discover the controller IP addresses from a DNS server. Where `<local domain>` is the access point domain name.
- Locally stored controller IP addresses—If the lightweight access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point non-volatile memory. The process of storing controller IP addresses in access points for later deployment is called priming the lightweight access point. For additional information, refer to the “[Priming Lightweight Access Points Prior to Deployment](#)” section on page F-1.

You can also manually configure controller information using CLI commands on new (out-of-the-box) access points that are not connected to a controller. For additional information refer to the “[Manually Configuring Controller Information Using the Access Point CLI](#)” section on page 4-8.

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

Deploying the Access Points on the Wireless Network

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

- Ensure that a site survey has been preformed.
- Ensure that your network infrastructure devices are operational and properly configured.
- For lightweight access points, perform these tasks:
 - Ensure that your controllers are connected to switch trunk ports.
 - Ensure that your switch is configured with untagged access ports for connecting your access points.
 - Ensure that a DHCP server with Option 43 configured is reachable by your access points.

To deploy your access points, follow these steps:

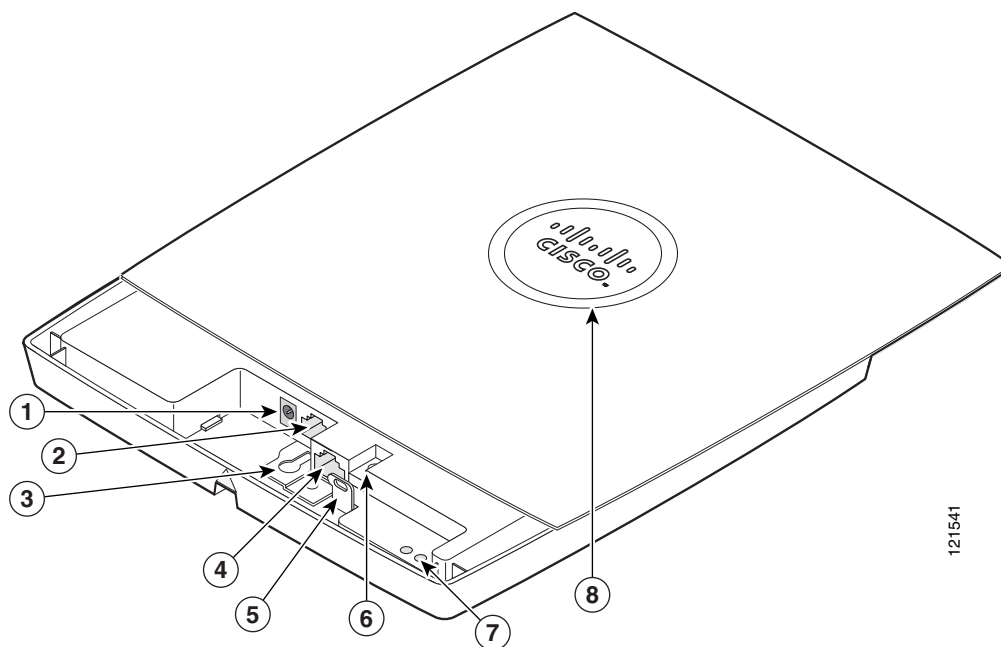
-
- Step 1** Obtain the access point location map created during your building site survey.
- Step 2** Review the access point locations and identify the specific mounting methods required for each access point location.
- Step 3** For each access point perform these steps:
- a. For lightweight access points, record the access point MAC address on the access point location map. When you have completed the access point deployment, return the access point MAC addresses and the access point locations on the access point location maps or floor plans to your network planner or manager. The network operators can use the MAC address and location information to create maps for precise wireless system management.
 - b. Attach your access point to the mounting plate (see the [“Attaching the Access Point to the Mounting Plate”](#) section on page 2-16).
 - c. Mount the access point at the indicated destination using the specified mounting method. For specific mounting instructions, see these sections:
 - Horizontal surface, such as a ceiling (see the [“Mounting the Access Point on a Horizontal Surface”](#) section on page 2-12).
 - Below a suspended ceiling (see the [“Mounting the Access Point Below a Suspended Ceiling”](#) section on page 2-13).
 - Above a suspended ceiling (see the [“Mounting the Access Point Above a Suspended Ceiling”](#) section on page 2-14).
 - On a desktop or shelf (see the [“Mounting Access Point on a Desktop or Shelf”](#) section on page 2-16).
 - d. Optionally secure the access point using a padlock or security cable (see the [“Securing the Access Point”](#) section on page 2-18).
 - e. Connect the access point cables (Ethernet, optional power, optional antennas). For instructions see the [“Connecting the Ethernet and Power Cables”](#) section on page 2-21.
 - f. On power up, verify that the access point is associated to a controller and operating normally. For additional information, refer to the [“Checking the Autonomous Access Point LEDs”](#) section on page 3-2 or the [“Checking the Lightweight Access Point LEDs”](#) section on page 4-2.

- Step 4** For lightweight access points, after your access points are deployed, ensure that your controller is not configured as a master controller. A master controller should only be used for configuring access points and not in a working network.

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



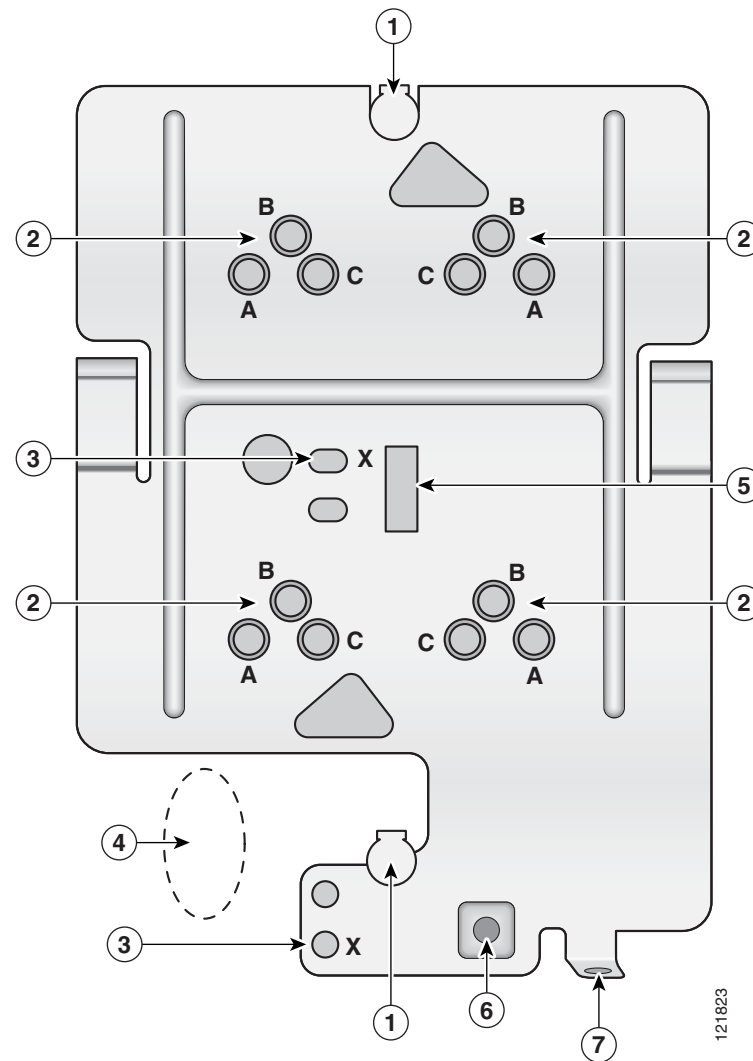
Note

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 installation. Refer to [Figure 2-2](#) to locate the various mounting holes for the method you intend to use.

Figure 2-2 **Mounting Plate**



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

The mounting plate features are described below:

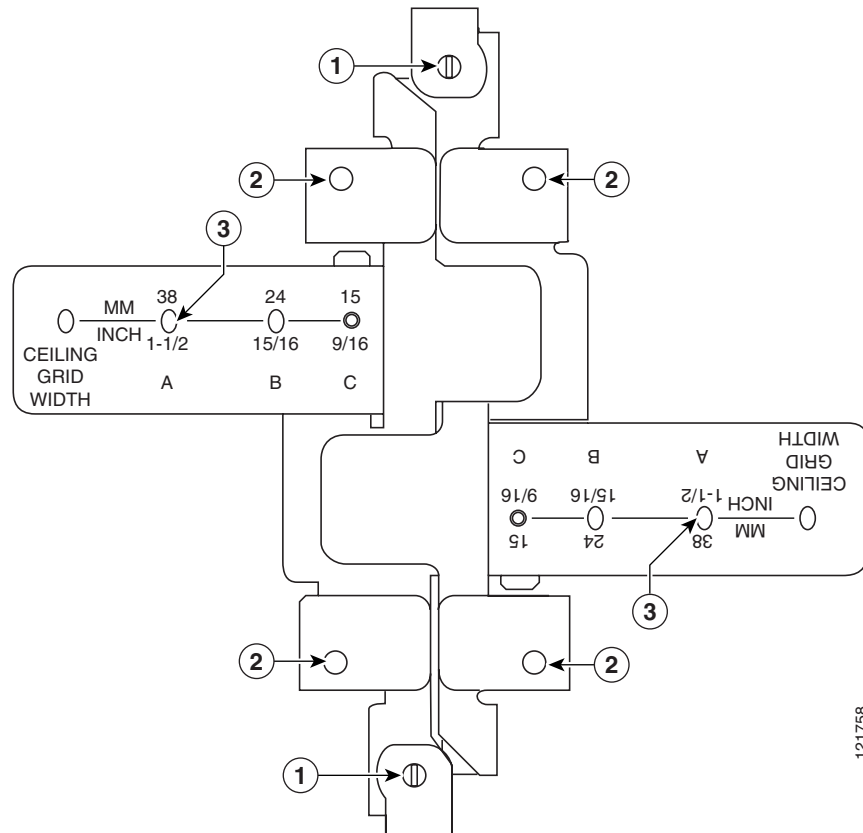
- Keyhole clips—used to attach the access point to the mounting plate. The keyhole clips slide into the keyhole slots on the bottom of the access point.
- Screw holes (A, B, C)—used to attach the suspended ceiling adjustable T-rail clips.
- Screw hole (X)—used to attach the mounting plate to a network 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 accomodate 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

121758

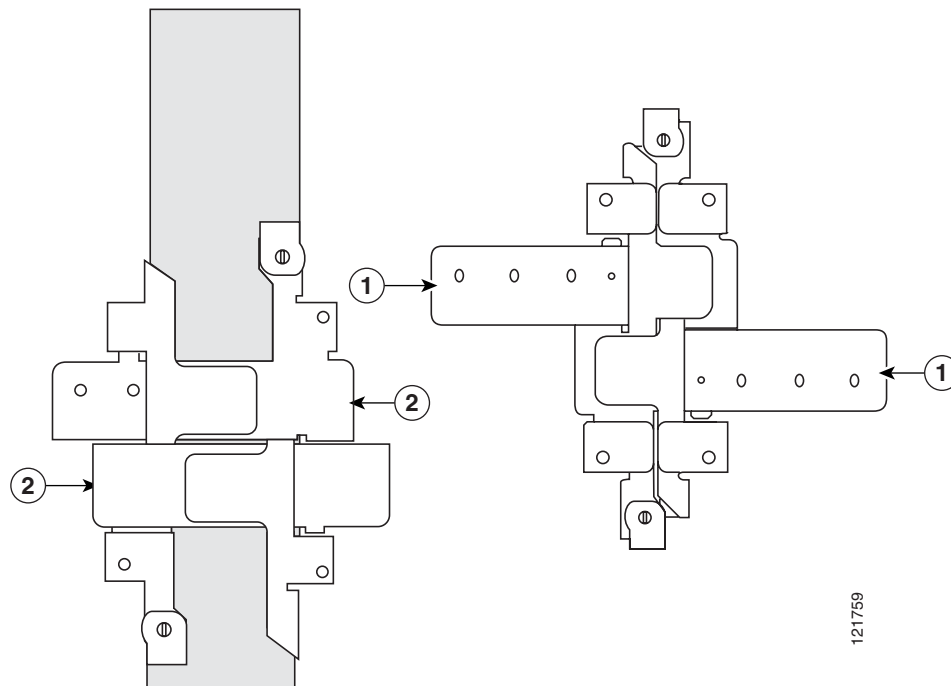
1	T-rail locking screws	3	T-rail width adjustment detents (A, B, C) correspond to the A, B, and C holes on the mounting plate
2	Mounting plate screw holes (8 x 32 flat head screw)		

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*



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

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.

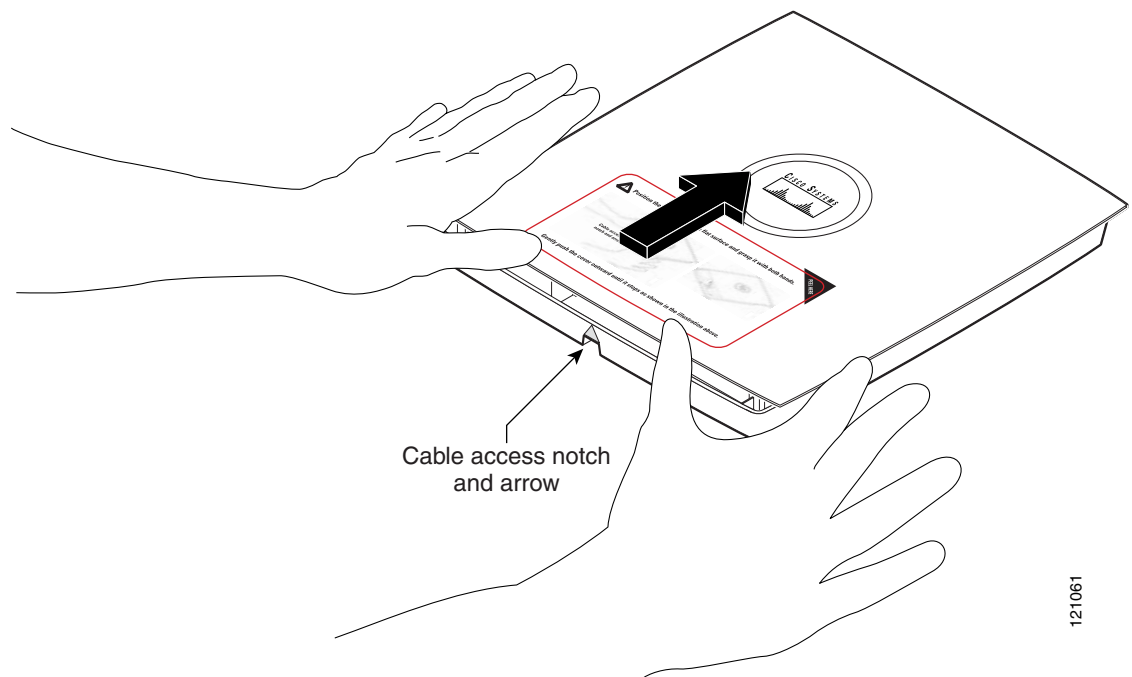
**Caution**

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 Surface



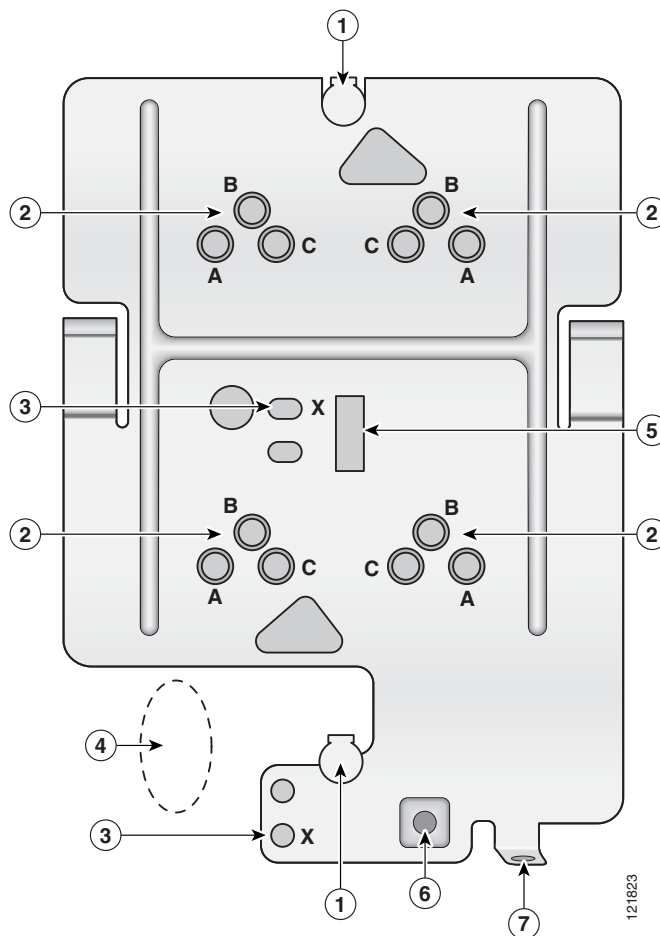
Caution

Avoid mounting the access point on a wall or vertical surface because the metal plate on the unit designed to dissipate heat acts as a reflector, causing the access point's integrated antenna to propagate directionally. The directional propagation can result in reduced performance, especially when using advanced features such as voice or location.

Follow these steps to mount the access point on a horizontal 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](#)).

Figure 2-6 Mounting Plate



1	Keyhole clip	5	T-bar hanger clip hole
2	Screw holes (A, B, C)	6	Security screw hole
3	Screw hole (X)	7	Padlock hole
4	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.



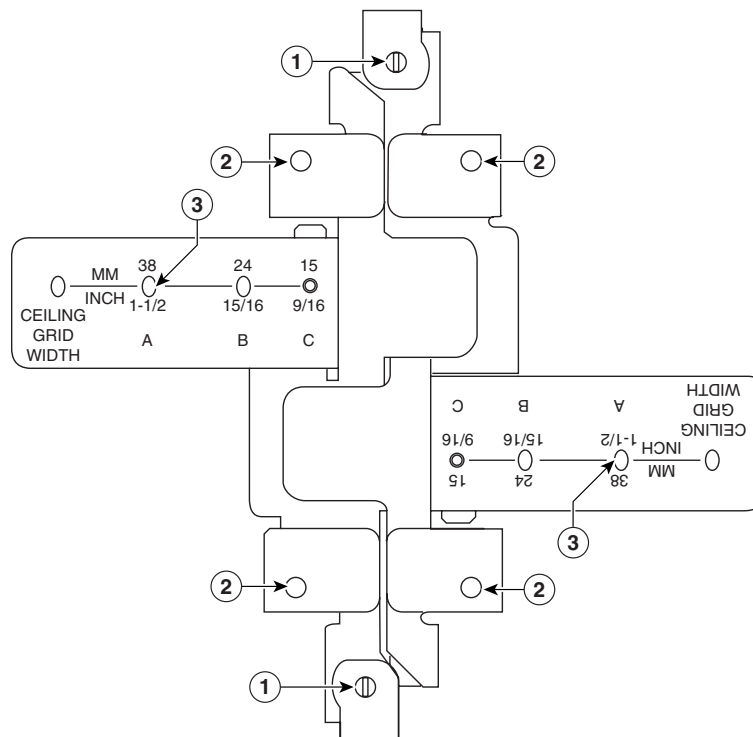
Note You can optionally insert the Ethernet cable and the power cable (if used) through the cable access notch in access point housing (see [Figure 2-5](#)).

- 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 2-16.

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



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

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

-
- Step 1** Decide where you want to mount the access point on your suspended ceiling.
 - Step 2** Select the appropriate adjustable T-rail clip for your suspended ceiling and open the clip to the maximum (see [Figure 2-4](#)).
 - Step 3** 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 2-16.

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.

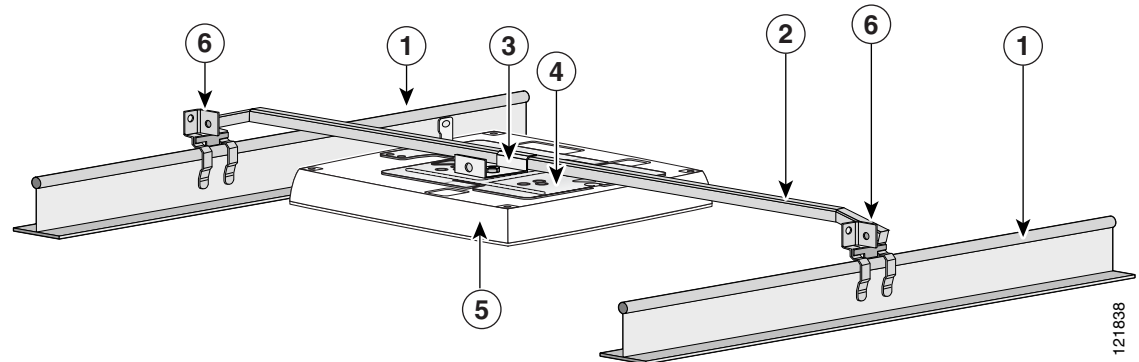


Caution

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.

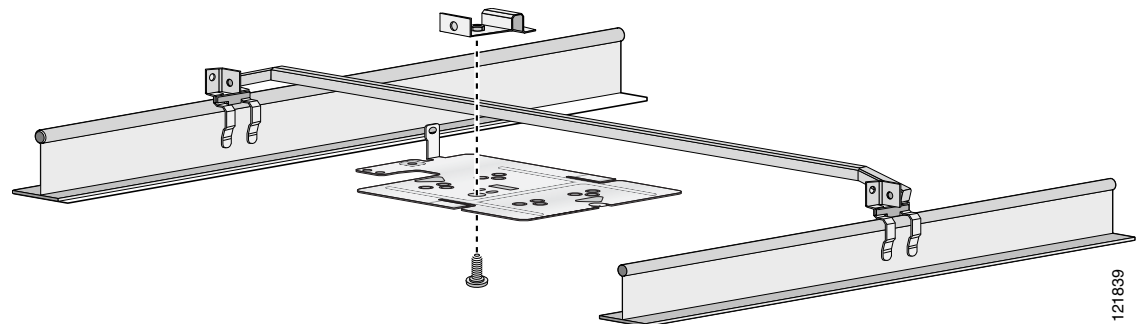
Figure 2-8 T-Bar Grid Mounting Bracket Parts



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 2-22).
- Step 6** Attach the access point to the access point mounting bracket (see the [“Attaching the Access Point to the Mounting Plate”](#) section on page 2-16).
- Step 7** Attach the T-rail clips on the each end of the T-bar box hanger to the ceiling grid T-rails. Make sure the clips are securely attached to the T-rails.

- Step 8** Connect a drop wire to a building structural element and the hole provided in the bracket mounting clip. This additional support is required in order to comply with the U.S. National Electrical Safety Code.
- Step 9** If you need additional security, you can secure the access point to a nearby immovable object using a Kensington lock and security cable (see the [“Securing the Access Point”](#) section on page 2-18).
- 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 2-16.

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 2-21.

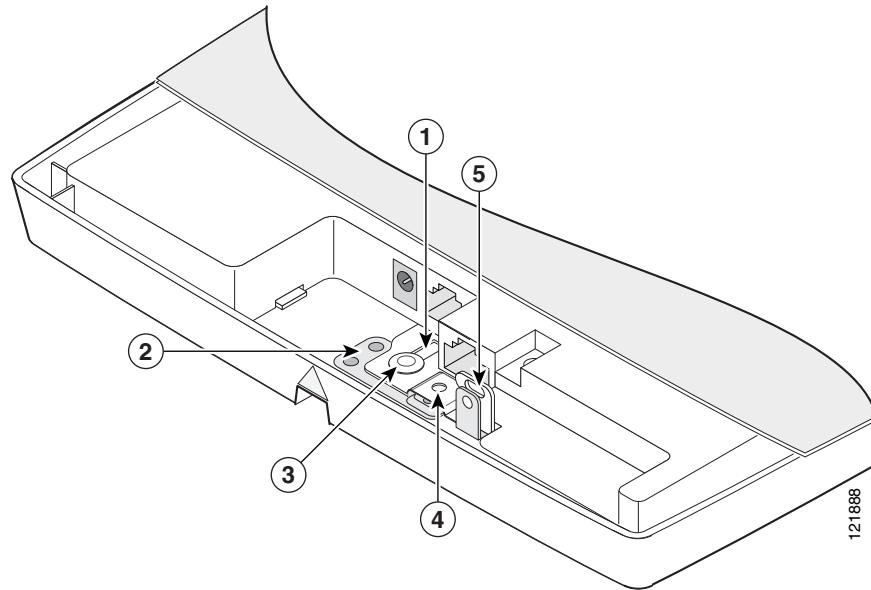
Attaching the Access Point to the Mounting Plate

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 2-11).
- 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*



1	Access point keyhole	4	Security screw hole
2	Mounting plate	5	Padlock hole
3	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 2-21.

For instructions on securing your access point, refer to the [“Securing the Access Point”](#) section on page 2-18.

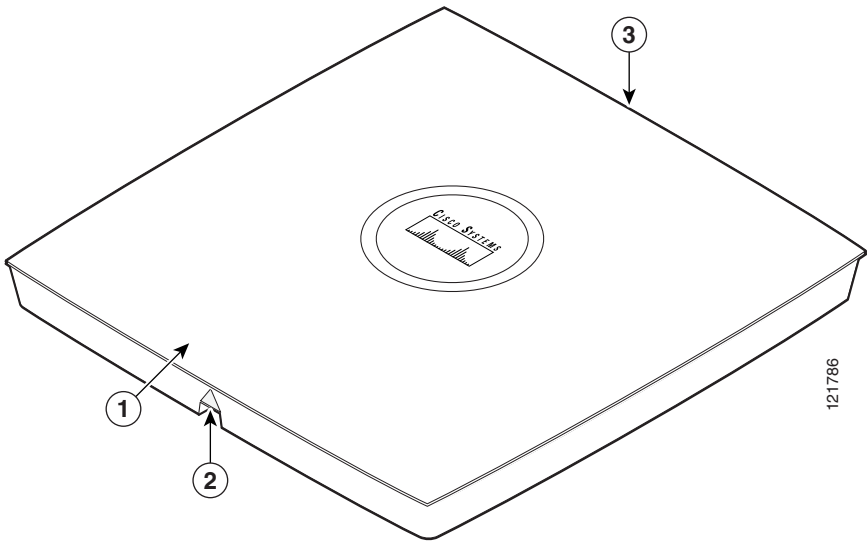
Securing the Access Point

- 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



1	Access point cover	3	Security cable slot
2	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 1-7](#)). 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](#)).

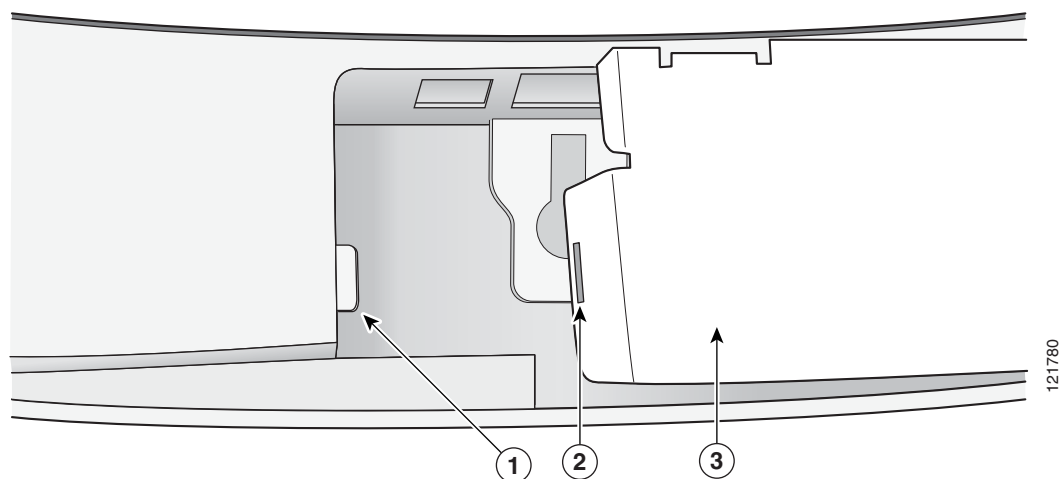


Note Using a tamper-resistant head screw to secure the access point to the mounting plate does not prevent someone from inserting or removing the access point cables or pressing the mode button.

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 2-11).
- 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

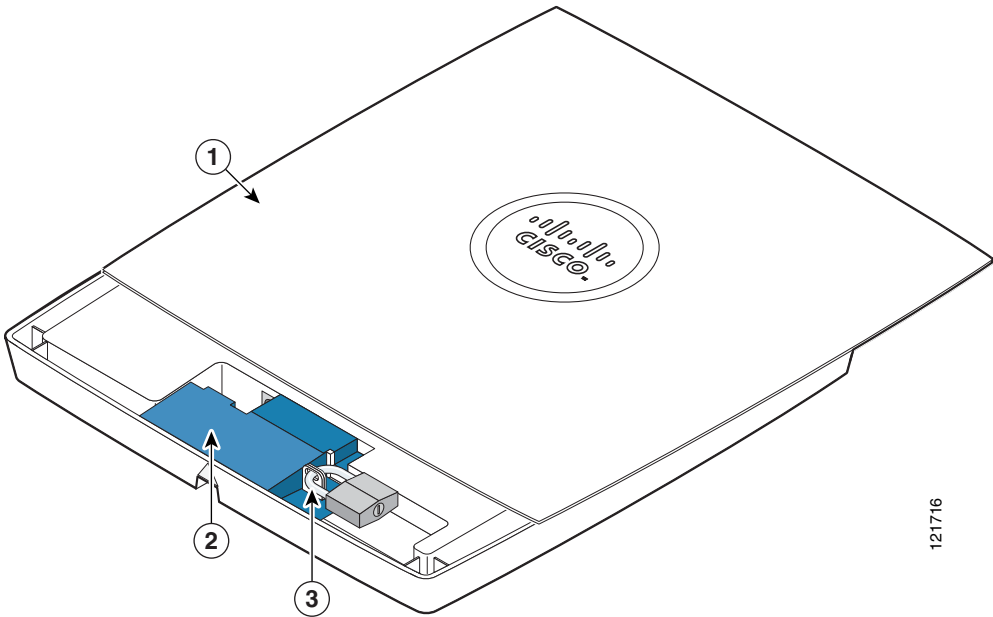


1	Access point security hasp tab	3	Security hasp adapter
2	Security hasp notch		

- 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



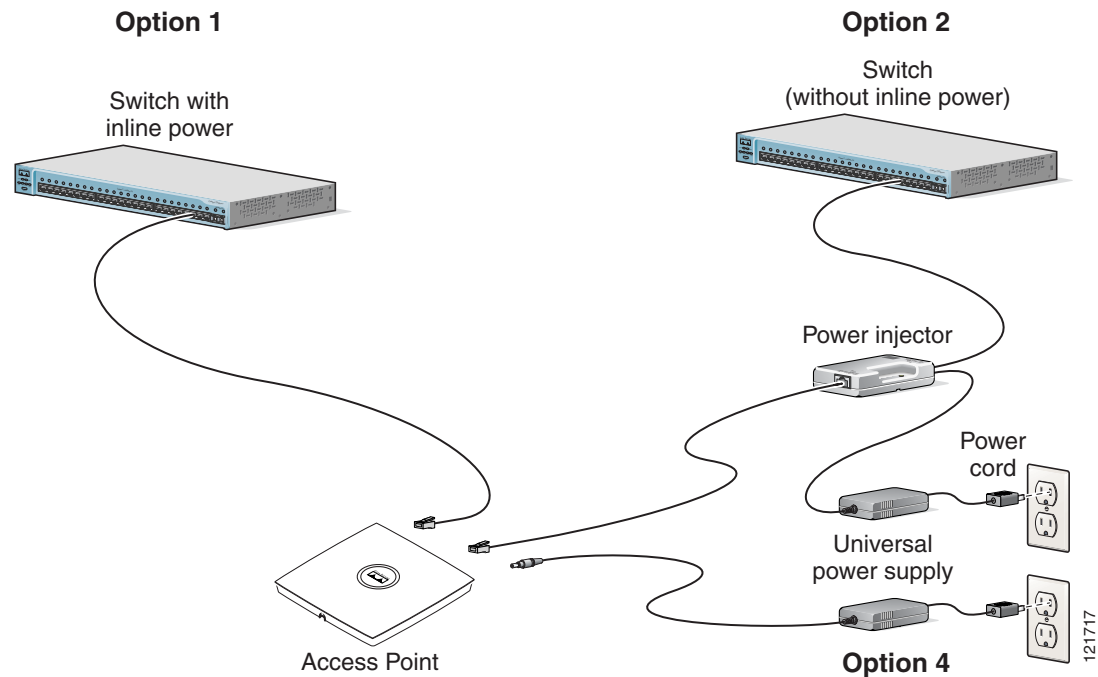
1	Access point cover in open position	3	Security padlock
2	Security hasp adapter		

- 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 [“Low Power Condition for Autonomous Access Points”](#) section on page 3-6 or the [“Low Power Condition for Lightweight Access Points”](#) section on page 4-6).

Connecting to an Ethernet Network with an Inline Power Source

**Caution**

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

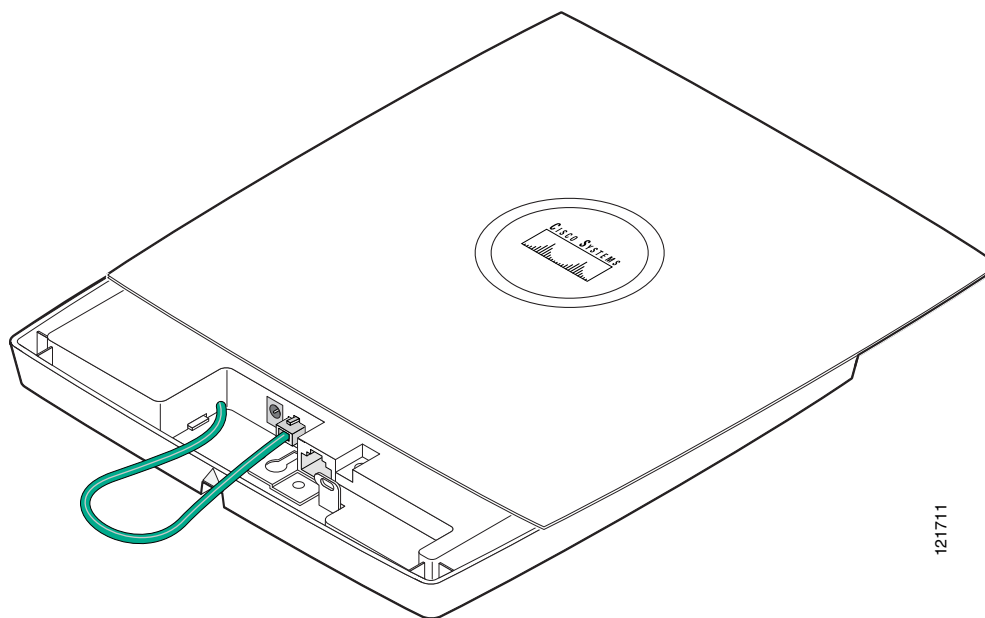
**Note**

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 2-11).
- 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 2-21).
 - 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 2-11).
- 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 2-18.
-

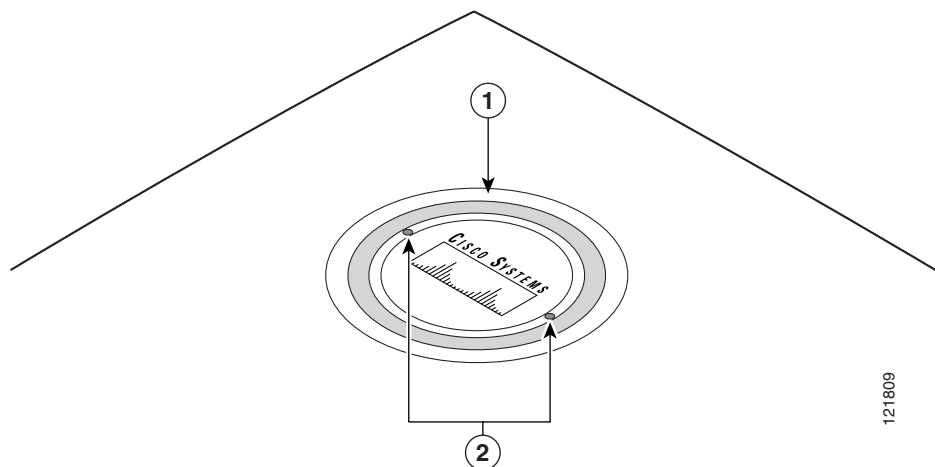
Rotating the Cisco Logo

The Cisco logo on the top of the unit can be rotated to correctly position the logo for any mounting arrangement making it always 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



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.



CHAPTER 3

Troubleshooting Autonomous Access Points

This chapter provides troubleshooting procedures for basic problems with the autonomous access point (model: AIR-AP1131AG or AIR-AP1131G). For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

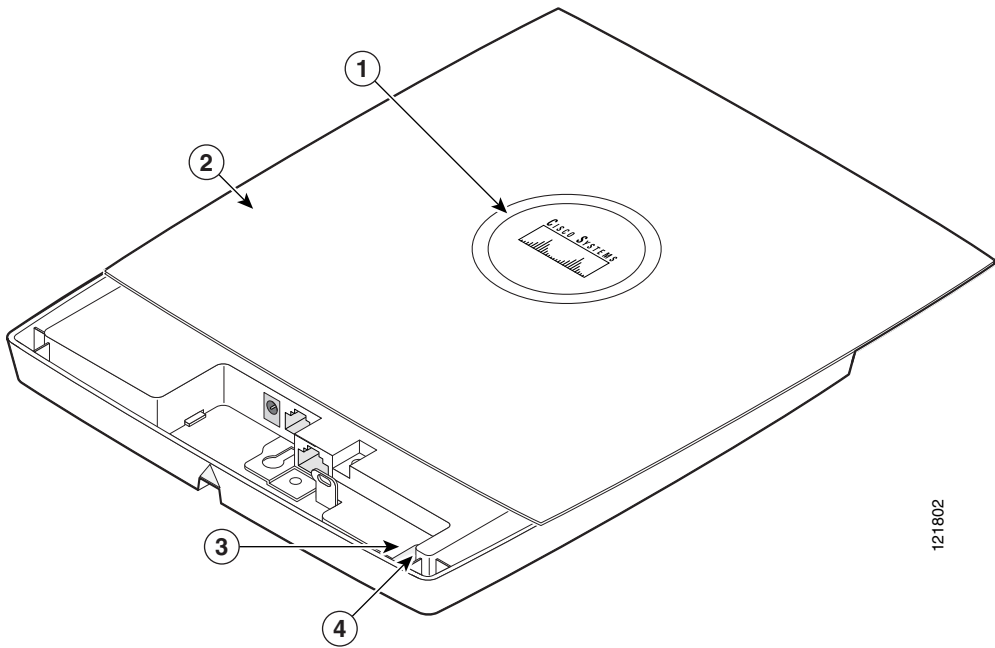
Sections in this chapter include:

- [Checking the Autonomous Access Point LEDs, page 3-2](#)
- [Checking Basic Settings, page 3-4](#)
- [Low Power Condition for Autonomous Access Points, page 3-6](#)
- [Running the Carrier Busy Test, page 3-14](#)
- [Running the Ping Test, page 3-15](#)
- [Resetting to the Default Configuration, page 3-16](#)
- [Reloading the Access Point Image, page 3-17](#)
- [Obtaining the Access Point Image File, page 3-19](#)
- [Obtaining the TFTP Server Software, page 3-21](#)


Checking the Autonomous Access Point LEDs


If your autonomous 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 3-1](#) shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).


Figure 3-1 Access Point LEDs



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 2-11).

 **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 3-1](#).

Table 3-1 **LED Signals**

Message type	Cable Bay Area	Top of Unit		Meaning
	Ethernet LED	Radio LED	Status LED	
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
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.
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 “Low Power Condition for Autonomous Access Points” section).
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.
Boot loader warnings	Off	Off	Yellow	Ethernet link not operational.
	Red	Off	Yellow	Ethernet failure.
	Amber	Off	Yellow	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Pink	Image recovery (Mode button pressed for 20 to 30 seconds).
	Blinking green	Blinking red	Blinking pink	Image recovery in progress and Mode button is released.

Table 3-1 LED Signals (continued)

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.

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 and later, 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 *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on configuring the SSID and the [“Enable Radio Interfaces” section on page 3-5](#) 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** At the prompt, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.
 - Step 3** When the Summary Status page displays, click **Network Interfaces > Radio0-802.11B** or **Radio0-802.11G** and the radio status page displays.
 - Step 4** Click **Settings** and the radio settings page displays.
 - Step 5** Click **Enable** in the Enable Radio field.
 - Step 6** Click **Apply**.
 - Step 7** Click **Network Interfaces > Radio0-802.11A** and the radio status page displays.
 - Step 8** Click **Settings** and the radio settings page displays.
 - Step 9** Click **Enable** in the Enable Radio field.
 - Step 10** Click **Apply**.
 - Step 11** 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 *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* 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 or later. 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 for Autonomous Access Points



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 Autonomous Access Point LEDs”](#) section on page 3-2 and [“Inline Power Status Messages”](#) section on page 3-7).

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 Autonomous Access Point LEDs”](#) section on page 3-2 and the [“Inline Power Status Messages”](#) section on page 3-7).

**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 3-2](#) and [Table 3-3](#)).

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 the *power inline never* command.
- %CDP_PD-4-POWER_OK: Full power - INJECTOR_CONFIGURED_ON_CURRENT_PORT inline power source—This message indicates the access point is operating at full power because it has been configured to expect a power injector on this port.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_PD inline power source—This message indicates the access point is operating at full power because it has detected a CDP packet from another Cisco powerable device (PD). The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not transmit this type of CDP packet.
- %CDP_PD-4-POWER_OK: Full Power - INJECTOR_DETECTED_MULTIPLE_MACS_ON_HUB inline power source—This message indicates the access point is operating at full power because it has detected multiple Cisco devices. The access point power is being supplied from a power injector or a non-Cisco power source because a Cisco power source does not forward CDP packets.
- %CDP_PD-4-POWER_OK: Full Power - NON_CISCO-NO_CDP_RECEIVED inline power source—This message indicates the access point is operating at full power because it has not received any CDP packets within the timeout period. This condition indicates your access point is connected to a non-Cisco power source.

**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_NO_INJECTOR_CONFIGURED <platform name> (<MAC address>)—This message indicates the access point is in low power mode with all radios disabled and has detected a CDP device that is unable to supply sufficient power to the access point.

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

**Note**

A Cisco power injector might be required.

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

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

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

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



Note A Cisco power injector might be required.

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

1. Verify the required power injector is installed on the new port: *<platform name> (<Ethernet port>)*.

(where *<platform name>* indicates the CDP device detected by the access point and *<Ethernet port>* indicates the Ethernet port of the CDP device.

2. If a power injector is installed, issue the command: `power inline negotiation injector installed`.

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

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



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

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



Caution

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

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 Cisco switch software using the following Cisco IOS CLI command:

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

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



Caution

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



Note

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

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

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

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



Caution

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



Note

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

Refer to [Table 3-2](#) for information on when to use this special Cisco IOS command and the corresponding Cisco switch power command.

Table 3-2 *Using Cisco IOS Commands*

Power Source	Cisco IOS Commands	
	Access Point	Cisco Switch
AC power module	None required	power inline never
Cisco switch that supports Intelligent Power Management ¹	no power inline negotiation prestandard source no power inline negotiation injector	power inline auto
Cisco switch that does not support Intelligent Power Management ¹	power inline negotiation prestandard source no power inline negotiation injector	power inline auto
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	None required ³	power inline never⁴
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	no power inline negotiation prestandard source power inline negotiation injector installed	power inline never
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. The Cisco switch uses Intelligent Power Management to inform the access point of the power injector being used.
4. Cisco switches that support Intelligent Power Management always configure the use of a power injector at the switch.

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 Console Port”](#) section on page 3-20).
- Step 2** From the global configuration mode, enter the command below that applies to your power configuration (see [Table 3-2](#)):
- **power inline negotiation injector installed**
 - **no power inline negotiation injector**
 - **power inline negotiation prestandard source**
 - **no power inline negotiation prestandard source**
- Step 3** Enter **exit** to exit the global configuration mode.
- Step 4** Enter **write memory** to save the setting to the access point memory.
- Step 5** Enter **quit** to exit the terminal session.
- Step 6** Close your terminal emulator.
-

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 3-2 shows the system power setting options and indicates the power status of the access point.

Figure 3-2 System Power Settings



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

Table 3-3 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	power inline never
Cisco switch that supports Intelligent Power Management ¹	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (unchecked)	power inline auto
Cisco switch that does not support Intelligent Power Management ¹	Power Settings: Pre-standard Compatibility (selected) Power Injector: Installed on Port with MAC Address (unchecked)	power inline auto

Table 3-3 Access Point System Power Settings and Cisco Switch Commands (continued)

Power Source	Access Point System Power Settings	Cisco Switch Power Command
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (unchecked)	power inline never³
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	Power Settings: Power Negotiation (selected) Power Injector: Installed on Port with MAC Address (checked)	power inline never
Power injector used with a non-Cisco switch	Configuration changes are not required	—
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.

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

-
- Step 1** Obtain the access point IP address and browse to your access point.
- Step 2** At the prompt, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.
- Step 3** Choose one of these operations:
- a. 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.
 - b. When you browse to your access point operating in full-power mode, choose **System Software > System Configuration**.
- Step 4** Choose one of these Power Settings options (see [Figure 3-2](#)):
- a. If your Cisco switch supports Intelligent Power Management negotiations, choose **Power Negotiation**.
 - b. If your Cisco switch does not support Intelligent Power Management negotiations, choose **Pre-standard Compatibility**.
 - c. If you are using a non-Cisco switch, changes to the power settings are not required.

- Step 5** If you are using a power injector with a Cisco switch, choose one of these Power setting options:
- 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 6** Click **Apply** and a message appears indicating that you should disable pop-up blockers before proceeding.

- Step 7** Click **OK** to continue. Your access point reboots and your access point power settings are configured.



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 are deassociated during the 6 to 8 seconds needed for the carrier busy test.

Follow these steps to activate the carrier busy test:

- Step 1** Use your web browser to access the access point browser interface.
- Step 2** At the prompts, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.
- Step 3** Click **Network Interfaces** and the Network Interface Summary screen appears.
- Step 4** Choose the radio interface experiencing problems by clicking **Radio0-802.11G** or **Radio1-802.11A**. The respective radio status page appears.
- Step 5** Click the **Carrier Busy Test** tab and the Carrier Busy Test screen appears.

Step 6 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** At the prompt, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.
- Step 3** Click **Association** and the main association page appears.
- Step 4** Click the MAC address of an associated wireless device and the Statistics page for that device appears.
- Step 5** Click the **Ping/Link Test** tab and the Ping/Link Test page appears.
- Step 6** 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 and click **Start**.
- Step 7** 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 3-4](#) and the [“Default SSID and Radio Behavior” section on page 3-4](#).

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 2-11](#)).
- 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**.
- Step 3** At the prompt, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.
- Step 4** Click **System Software** and the System Software screen appears.
- Step 5** Click **System Configuration** and the System Configuration screen appears.
- Step 6** Click **Reset to Defaults**.



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

- Step 7** 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.123-8.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 2-11).
 - 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. You should disable your browser pop-up blocker.

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.

- Step 2** Enter the access point's IP address in the browser address line and press **Enter**.
- Step 3** At the prompt, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.
- Step 4** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
- Step 5** Click the **Browse** button to locate the access point image file (such as c1130-k9w7-tar.123-8.JA.tar) on your PC.
- Step 6** Click **Upload**.

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**.

Step 3 At the prompt, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 4 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 5 Click the **TFTP Upgrade** tab.

Step 6 Enter the IP address for the TFTP server in the TFTP Server field.

Step 7 Enter the file name for the access point image file (such as c1130-k9w7-tar.123-8.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 8 Click **Upload**.

Step 9 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/cisco/software/navigator.html>

Step 2 Click **Access Points > Cisco Aironet 1130 AG Series**.

Step 3 Click **Cisco Aironet 1130AG Access Point**.

Step 4 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 5 Click **IOS**.

Step 6 Choose the Cisco IOS release desired, such as 12.3.8.JA.

Step 7 Click **WIRELESS LAN** for an access point image file, such as c1130-k9w7-tar.123-8.JA.tar.

- Step 8** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
 - Step 9** On the Security Information window, click **Yes** to display non-secure items.
 - Step 10** On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.
 - Step 11** If you checked No, enter the requested information and click **Submit**.
 - Step 12** Click **Yes** to continue.
 - Step 13** Click **DOWNLOAD**.
 - Step 14** Read and accept the terms and conditions of the Software Download Rules.
 - Step 15** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
 - Step 16** Click **Save** to download your image file to your hard disk.
 - Step 17** Select the desired download location on your hard disk and click **Save**.
-

Connecting to the Access Point Console Port

The console port is enabled during power up for diagnostic and monitoring purposes, which might be helpful if the access point is unable to associate to a controller. You can connect a PC to the 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.

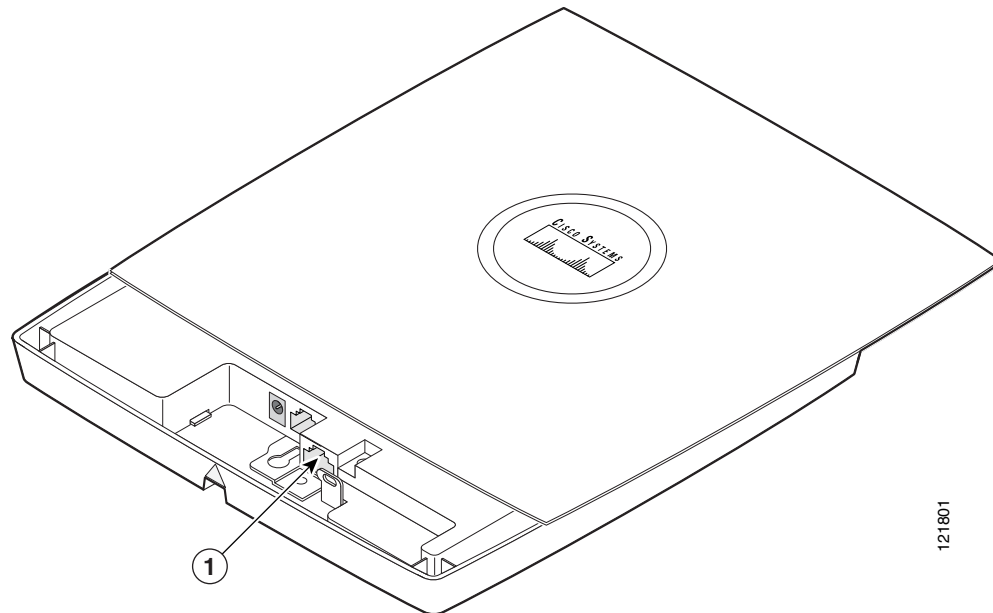


Note

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

Follow these steps to view the power up sequences by connecting to the access point console port:

- Step 1** Open the access point cover (refer to the “[Opening the Access Point Cover](#)” section on page 2-11).
- 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. The location of the access point console port is shown in [Figure 3-3](#).

Figure 3-3 Console Port Location

1	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.
- Step 4** At the prompts, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

When you have finished using the console port, you must remove the serial cable from the access point.

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.



CHAPTER 4

Troubleshooting Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the 1130AG series lightweight access point (model: AIR-LAP1131AG or AIR-LAP1131G). For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Sections in this chapter include:

- [Guidelines for Using 1130AG Series Lightweight Access Points, page 4-2](#)
- [Checking the Lightweight Access Point LEDs, page 4-2](#)
- [Low Power Condition for Lightweight Access Points, page 4-6](#)
- [Manually Configuring Controller Information Using the Access Point CLI, page 4-8](#)
- [Returning the Access Point to Autonomous Mode, page 4-9](#)
- [Obtaining the Autonomous Access Point Image File, page 4-11](#)
- [Connecting to the Access Point Console Port, page 4-12](#)
- [Obtaining the TFTP Server Software, page 4-13](#)

Guidelines for Using 1130AG Series Lightweight Access Points

Keep these guidelines in mind when you use a 1130AG series lightweight access point:

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

**Note**

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

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

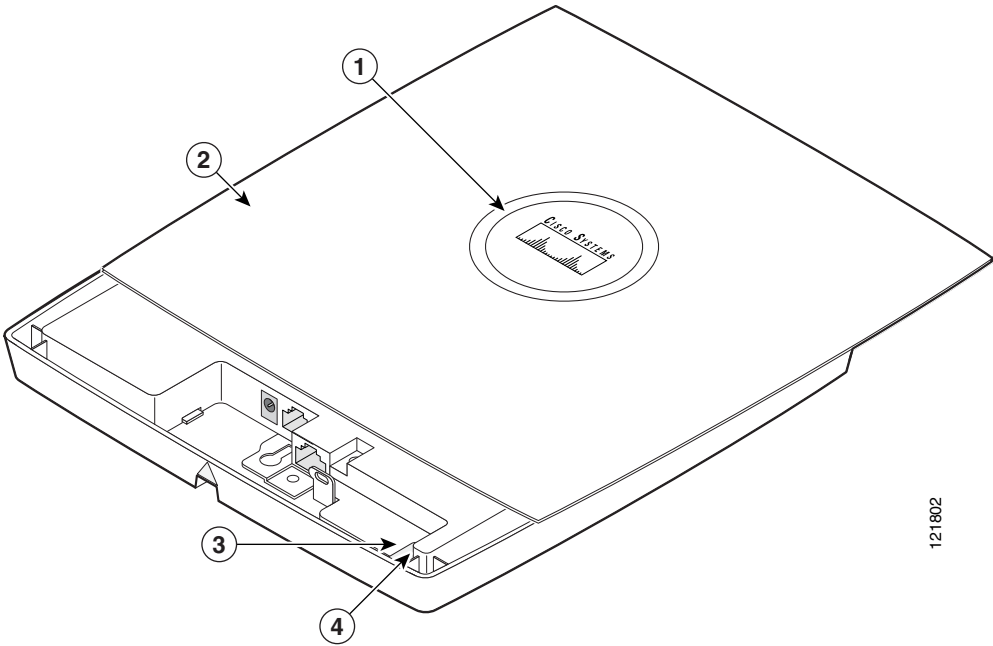
Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. For additional information, refer to the [“Configuring DHCP Option 43 for Lightweight Access Points”](#) section on page G-1.


Checking the Lightweight 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 4-1](#) shows the access point LEDs.


Figure 4-1 Access Point LEDs



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

 **Note** To view the Ethernet and Radio LEDs you must open the access point cover (refer to the [“Opening the Access Point Cover”](#) section on page 2-11).

 **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 4-1](#).

Table 4-1 **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
	Slow blinking green	—	—	Hybrid-REAP standalone mode
Boot loader warnings	Off	Off	Yellow	Ethernet link not operational.
	Red	Off	Yellow	Ethernet failure.
	Amber	Off	Yellow	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Pink	Image recovery (Mode button pressed for 20 to 30 seconds)
	Blinking green	Blinking red	Blinking pink	Image recovery in progress and Mode button is released.

Table 4-1 LED Signals (continued)

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 “Low Power Condition for Lightweight Access Points” section).
Controller status	—	—	Alternating green, red , and amber ¹	Connecting to the controller. Note If the access point remains in this mode for more than five minutes, the access point is unable to find the controller. Ensure a DHCP server is available or that controller information is configured on the access point.
	—	—	Blinking dark blue	Loading the access point image file.

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

Low Power Condition for Lightweight Access Points



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 lightweight 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 both radios are turned on; otherwise, the access point remains in low power mode with one or both radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication (see the [“Checking the Lightweight Access Point LEDs”](#) section on page 4-2).

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 one or both 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, one or both radios are deactivated and the Status LED turns amber to indicate low power mode (see [Table 4-1](#)).

If your Cisco switch is capable of supplying sufficient power for full operation but the access point remains in low-power mode, your access point or your switch (or both) might be misconfigured (see [Table 4-2](#)).

If your inline power source is not able to supply sufficient power for full operation, you should consider these options (see [Table 4-2](#)):

- 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

Configuring Power Using Controller CLI Commands

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

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



Note

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

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

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



Caution

If the access point receives power through PoE, the output current of the power sourcing equipment (PSE) cannot exceed 400 mA per port. The power source must comply with IEEE 802.3af or IEC60950 for limited power sources.

Refer to [Table 4-2](#) for information on when to use these special CLI controller commands and the corresponding Cisco switch power command.

Table 4-2 *Using CLI Power Commands*

Power Source	CLI Commands	
	Cisco Wireless LAN Controller	Cisco Switch
AC power module	None required	power inline never
Cisco switch that supports Intelligent Power Management ¹	None required	power inline auto
Cisco switch that does not support Intelligent Power Management ¹	config ap power pre-standard enable	power inline auto
Power injector ² used with a Cisco switch that supports Intelligent Power Management ¹	None required	power inline never³
Power injector ² used with a Cisco switch that does not support Intelligent Power Management ¹	config ap power injector enable	power inline never
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.

Manually Configuring Controller Information Using the Access Point CLI

In a new installation, when your access point is unable to reach a DHCP server, you can manually configure needed controller information using the access point CLI. For information on how to connect to the console port, see the [“Connecting to the Access Point Console Port”](#) section on page 4-12.



Note

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

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

Configuring Controller Information

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

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

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

**Note**

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

Clearing Manually Entered Controller Information

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

**Note**

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

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

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

Manually Resetting the Access Point to Defaults

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

**Note**

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

```
clear lwapp private-config
```

Returning the Access Point to Autonomous Mode

You can return a lightweight access point to autonomous mode by loading a Cisco IOS release that supports autonomous mode (such as Cisco IOS Release 12.3(7)JA or earlier). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP.

Using a WLAN Controller to Return the Access Point to Autonomous Mode

Follow these steps to revert from lightweight mode to autonomous mode using a controller:

-
- Step 1** Log into the CLI on the controller to which the access point is associated and enter this command:
- ```
config ap tftp-downgrade tftp-server-ip-address filename access-point-name
```
- (where:
- a) *tftp-server-ip-address* is the IP address of the TFTP server
  - b) *filename* is the full path and filename of the access point image file, such as `D:/Images/c1130-k9w7-tar.123-7.JA.tar`
  - c) *access-point-name* is the name that identifies the access point on the controller.)
- Step 2** Wait until the access point reboots, as indicated by all LEDs turning green followed by the Status LED blinking green.
- Step 3** After the access point reboots, reconfigure it using the access point GUI or the CLI.
- 

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

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



### Note

The access point MODE button is enabled by default, but you need to verify that the MODE button is enabled (see the [“MODE Button Setting” section on page 4-11](#)).

---

- 
- Step 1** Set the static IP address of the PC on which your TFTP server software runs to an address between 10.0.0.2 and 10.0.0.30.
- Step 2** Make sure that the PC contains the access point image file (such as `c1130-k9w7-tar.123-7.JA.tar` for an 1130 series access point) in the TFTP server folder and that the TFTP server is activated.
- Step 3** Rename the access point image file in the TFTP server folder to **c1130-k9w7-tar.default**.
- Step 4** Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.
- Step 5** Disconnect power from the access point.
- Step 6** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 7** Hold the **MODE** button until the Radio LED turns red (approximately 20 to 30 seconds) and then release.
- Step 8** Wait until the access point reboots, as indicated by all LEDs turning green followed by the Status LED blinking green.
- Step 9** After the access point reboots, reconfigure it using the access point GUI or the CLI.
-

## MODE Button Setting

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

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

## Obtaining the Autonomous Access Point Image File

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


**Note**

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

- 
- Step 1** Use your Internet browser to access the Cisco Software Center at the following URL:  
<http://www.cisco.com/cisco/software/navigator.html>
  - Step 2** Click **Access Points > Cisco Aironet 1130 AG Series**.
  - Step 3** Click **Cisco Aironet 1130AG Access Point**.
  - Step 4** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
  - Step 5** Click **IOS**.
  - Step 6** Choose the Cisco IOS release desired, such as 12.3.8.JA.
  - Step 7** Click **WIRELESS LAN** for an access point image file, such as c1130-k9w7-tar.123-8.JA.tar.
  - Step 8** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
  - Step 9** On the Security Information window, click **Yes** to display non-secure items.
  - Step 10** On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.
  - Step 11** If you checked No, enter the requested information and click **Submit**.
  - Step 12** Click **Yes** to continue.
  - Step 13** Click **DOWNLOAD**.
  - Step 14** Read and accept the terms and conditions of the Software Download Rules.
  - Step 15** On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.
  - Step 16** Click **Save** to download your image file to your hard disk.
  - Step 17** Select the desired download location on your hard disk and click **Save**.
-


# Connecting to the Access Point Console Port

The console port is enabled during power up for diagnostic and monitoring purposes, which might be helpful if the access point is unable to associate to a controller. You can connect a PC to the 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.

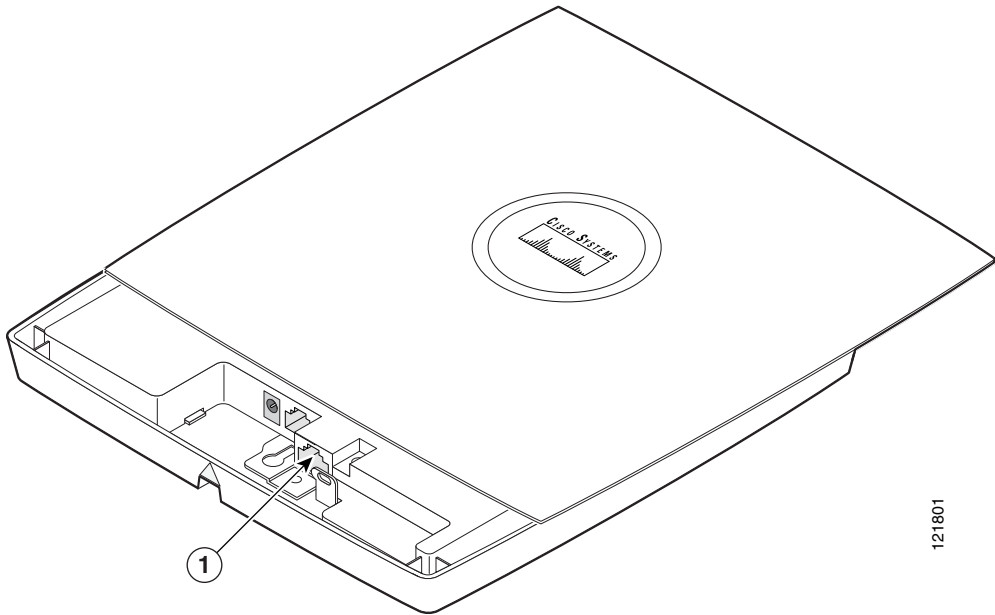
Follow these steps to view the power up sequences by connecting to the access point console port:

- Step 1

Open the access point cover (refer to the “Opening the Access Point Cover” section on page 2-11).
- 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. The location of the access point console port is shown in Figure 4-2.

Figure 4-2 Console Port Location



|   |              |  |
|---|--------------|--|
| 1 | 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.

- Step 4** At the prompts, enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.
- When you have finished using the console port, you must remove the serial cable from the access point.
- 

## 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.

---





## APPENDIX **A**

# Translated Safety Warnings

---

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

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

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







## APPENDIX **B**

# Declarations of Conformity and Regulatory Information

---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1130AG Series Access Points and the Cisco Aironet 1130AG Series Lightweight Access Points.

This appendix contains the following sections:

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

# Manufacturers Federal Communication Commission Declaration of Conformity Statement

**Autonomous Access Point Models:**

AIR-AP1131AG-A-K9  
AIR-AP1131G-A-K9

**Lightweight Access Point Models:**

AIR-AP1131AG-A-K9  
AIR-AP1131G-A-K9  
AIR-LAP1131G-A-K9

**FCC Certification numbers:**

LDK102054  
LDK102054E  
LDK102065

**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.

**Note**

Dynamic Frequency Selection (DFS) operation and operation from 5500 to 5700 MHz has not been authorized as required by the rules of the Federal Communications Commission and is not supported until authorization is obtained.

## VCCI Statement for Japan

**Warning**

**This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

**警告**

VCCI 準拠クラスB機器（日本）

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としています。この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

# Industry Canada

**Models:**

AIR-AP1131AG-A-K9 / AIR-AP1131G-A-K9  
AIR-LAP1131AG-A-K9 / AIR-LAP1131G-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

**Autonomous Access Point Models:**

AIR-AP1131AG-E-K9  
AIR-AP1131G-E-K9

**Lightweight Access Point Models:**

AIR-LAP1131AG-E-K9  
AIR-LAP1131G-E-K9

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

This declaration is only valid for configurations (combinations of software, firmware, and hardware) provided and supported by Cisco Systems. The use of software or firmware not provided and supported by Cisco Systems may result in the equipment no longer being compliant with the regulatory requirements.

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

121403

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

121404

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

For 2.4 GHz radios, the following standards were applied:

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

**Note**

This equipment is intended to be used in all EU and EFTA countries. 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.

**Autonomous Access Point Models:**

AIR-AP1131AG-J-K9 / AIR-AP1131G-P-K9

**Lightweight Access Point Models:**

AIR-LAP1131AG-J-K9 / AIR-LAP1131G-P-K9

## Japanese Translation

## English Translation

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

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

Contact Number: 03-5549-6500



# Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operating Cisco Aironet access points in Taiwan. The rules are provided in both Chinese and English.

## Access Points with IEEE 802.11a Radios

### Chinese Translation

本設備限於室內使用

95814

### English Translation

This equipment is limited for indoor use.

## All Access Points

### Chinese Translation

#### 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

### English Translation

#### Administrative Rules for Low-power Radio-Frequency Devices

##### Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

##### Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

# Declaration of Conformity Statements

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

<http://www.ciscofax.com>

## Declaration of Conformity Statements for European Union Countries

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

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

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

Declare under our sole responsibility that the product,

**Product:** *AIR-AP1131AG-E-K9*  
**Variant:** *AIR-LAP1131AG-E-K9*

*Cisco Aironet 1130AG Series IEEE802.11 a/b/g Access Point*

Fulfills 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**

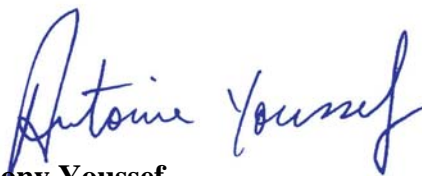
The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark:



Date & Place of Issue: *25 July 2005, San Jose*

**Signature:**

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

*DofC 441919rev1*



## Annex to DofC# 441919

### 1. Information on Antennas and Power Levels

The AIR-(L)AP1131AG-E-K9 has integral antennas. The antenna gain is 4 dBi (for both 2.4 GHz & 5 GHz).

The maximum (conducted) power level for operation in the 2.4 GHz band and the 5 GHz band mentioned are given below and are based on a 100 mW eirp limit applicable in the 2.4 GHz band and a 200 mW eirp limit (5150-5350 MHz) or a 1 W eirp limit (5470-5725 MHz) applicable in the 5 GHz bands.

A separate compliance document shipped with each product will correctly inform the user on the applicable maximum power level (eirp) in his area/country, the corresponding maximum setting for the conducted power and other restrictions that might be applicable.

Any configuration resulting in an eirp level above the regulatory limit applicable in a given country is illegal and is outside the scope of this Declaration.

| Antenna P/N              | Integral Ant. Gain | Max Power Level |
|--------------------------|--------------------|-----------------|
| Integral antenna 2.4 GHz | 4 dBi              | 15 dBm          |
| Integral antenna 5 GHz   | 4 dBi              | 17 dBm          |

July 25, 2005

Tony Youssef  
Director Corporate Compliance

**Declaration of Conformity Statements**



# APPENDIX C

## Access Point Specifications

Table C-1 lists the technical specifications for the 1130AG series access point.

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


| Category              | 802.11g Radio Specifications                                                                                                                                                                        |                   | 802.11a Radio Specifications |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|------------------------------|
|                       | 802.11b Operation                                                                                                                                                                                   | 802.11g Operation |                              |
| Size                  | 7.53 in. W x 7.53 in. D x 1.31 in. H<br>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)<br><br>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:<br>32 to 104°F (0 to 40°C)<br>1130AG series power module:<br>32 to 104°F (0 to 40°C)                                                                                                     |                   |                              |
| Weight                | Without mounting hardware:<br>1.48 lbs (0.67 kg)                                                                                                                                                    |                   |                              |

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

| Category              | 802.11g Radio Specifications                                                                                                                                                                                          |                                                                                                                                                                                                    | 802.11a Radio Specifications                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | 802.11b Operation                                                                                                                                                                                                     | 802.11g Operation                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                      |
| Power Output          | 100 mW (20 dBm)<br>50 mW (17 dBm)<br>25 mW (14 dBm)<br>10 mW (11 dBm)<br>5 mW (8 dBm)<br>3 mW (5 dBm)<br>2 mW (2 dBm)<br>1 mW (-1 dBm)<br>(Depending on the regulatory domain in which the access point is installed) | 50 mW (17 dBm)<br>25 mW (14 dBm)<br>10 mW (11 dBm)<br>5 mW (8 dBm)<br>3 mW (5 dBm)<br>2 mW (2 dBm)<br>1 mW (-1 dBm)<br>(Depending on the regulatory domain in which the access point is installed) | Autonomous access points<br>50 mW (17 dBm)<br>30 mW (15 dBm)<br>25 mW (14 dBm)<br>10 mW (11 dBm)<br>5 mW (8 dBm)<br>3 mW (5 dBm)<br>2 mW (2 dBm)<br>1 mW (-1 dBm)<br>Lightweight access points<br>50 mW (17 dBm)<br>25 mW (14 dBm)<br>10 mW (11 dBm)<br>5 mW (8 dBm)<br>3 mW (5 dBm)<br>2 mW (2 dBm)<br>1 mW (-1 dBm)<br>(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.                                                                                                                                                                                                                                                                                                                                             |
| Frequency             | 2.400 to 2.497 GHz<br>(Depending on the regulatory domain in which the access point is installed)                                                                                                                     |                                                                                                                                                                                                    | 5.15 to 5.25 GHz<br>5.25 to 5.35 GHz<br>5.725 to 5.85 GHz<br>(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)<br>QPSK (2 Mbps)<br>CCK (5.5 and 11 Mbps)                                                                                                                                                               | BPSK (6 and 9 Mbps)<br>QPSK (12 and 18 Mbps)<br>16-QAM (24 and 36 Mbps)<br>64-QAM (48 and 54 Mbps)                                                                                                 | BPSK (6 Mbps and 9 Mbps)<br>QPSK (12 Mbps and 18 Mbps)<br>16-QAM (24 and 36 Mbps)<br>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<br>360 ft at 11 Mbps                                                                                                                                                                                 | 400 ft at 6 Mbps<br>100 ft at 54 Mbps                                                                                                                                                              | 325 ft at 6 Mbps<br>80 ft at 54 Mbps                                                                                                                                                                                                                                                                                                                                                                 |



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

|                        | 802.11g Radio Specifications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                   |                                                                       |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------|
| Category               | 802.11b Operation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 802.11g Operation | 802.11a Radio Specifications                                          |
| Compliance             | <div>The 1130AG series access point complies with UL 2043 for products installed in a building’s environmental air handling spaces, such as above suspended ceilings.</div> <div><div></div><div><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.</div></div> |                   |                                                                       |
| Safety                 | Designed to meet:<br><br>UL 60950-1<br>CAN/CSA C22.2 No. 60950-1<br>UL 2043<br>EN 60950-1<br>IEC 60950-1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                   |                                                                       |
| Radio Approvals        | FCC Parts 15.247<br>Canada RSS-210<br>Japan ARIB-STD-33B<br>Japan ARIB-STD-66<br>Europe EN-300.328                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                   | FCC Part 15.407<br>Canada RSS-210<br>Japan ARIB STD-T71<br>EN 301.893 |
| EMI and Susceptibility | FCC Part 15.107 and 15.109 Class B<br>ICES-003 Class B (Canada)<br>EN 55022 B<br>EN 60601-1-2:2001<br>AS/NZS 3548 Class B<br>VCCI Class B<br>EN 301.489-1<br>EN 301.489-17                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                   |                                                                       |
| RF Exposure            | OET-65C<br>RSS-102<br>ANSI C95.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                   |                                                                       |





## APPENDIX **D**

# Channels and Maximum Power Levels

---

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

To browse to the document, follow these steps:

- 
- Step 1** Click this link to the Cisco Wireless documentation home page:  
[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)
  - Step 2** Click **Cisco Aironet 1130AG Series** listed under Access Points.
  - Step 3** Click **Install and Upgrade Guides**.
  - Step 4** Click **Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges**. or **Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges**.
-





## APPENDIX **E**

# Console Cable Pinouts

---

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

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

# Overview

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

## Console Port Signals and Pinouts

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

**Note**

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

**Note**

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

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

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

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

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



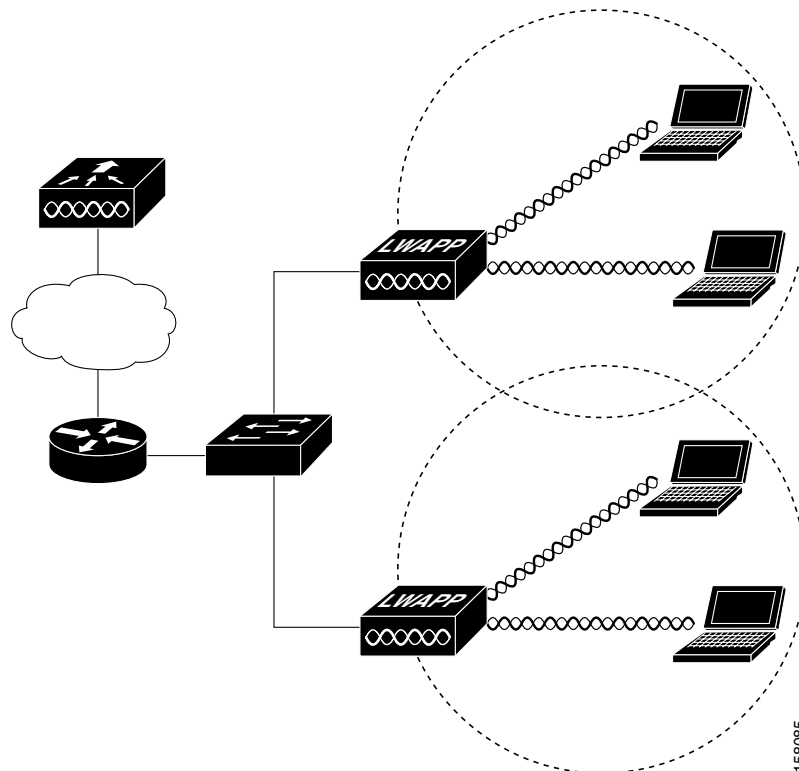
# APPENDIX **F**

## Priming Lightweight Access Points Prior to Deployment

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

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

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



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

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

The lightweight access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, OTAP, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For more information, refer to the [“Configuring DHCP Option 43 for Lightweight Access Points” section on page G-1](#).



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

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

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

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

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

- Step 5** Apply power to the lightweight access points:

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



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

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



- Step 6** If the operating system download is successful, the lightweight access point reboots. Normal operation is indicated when the radio LED is blinking to indicate radio activity.
- Step 7** Use controller CLI, controller GUI, or Cisco WCS to configure the lightweight access point with primary, secondary, and tertiary controller names.
- Step 8** If the lightweight access point is in a Controller Mobility Group, use the controller CLI, controller GUI, or Cisco WCS to configure the Controller Mobility Group name.
- Step 9** Use controller CLI, controller GUI, or Cisco WCS to configure the access point-specific 802.11a, 802.11b, and 802.11g network settings.
- Step 10** If the configuration priming was successful, the radio LED is blinking to indicate normal operation.
- Step 11** Repeat Steps 4 to 9 for each access point.

When you successfully complete the configuration priming of all your lightweight access points, ensure Master setting is disabled on your controller. You can begin deploying the access points to their final destinations.

---





## APPENDIX G

# Configuring DHCP Option 43 for Lightweight Access Points

---

This appendix describes the steps needed to configure DHCP Option 43 for use with Cisco Aironet lightweight access points. This appendix contains these sections:

- [Overview, page G-2](#)
- [Configuring Option 43 for 1000 and 1500 Series Access Points, page G-3](#)
- [Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Lightweight Access Points, page G-4](#)

# Overview

This section contains a DHCP Option 43 configuration example on the embedded Cisco IOS DHCP server for use with Cisco Aironet lightweight access points. For instructions on configuring DHCP Option 43 on Microsoft, Sun Solaris, Linux, and Lucent QIP DHCP servers, consult the document at this URL:

[http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_configuration\\_example09186a00808714fe.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00808714fe.shtml)

For other DHCP server implementations, consult the DHCP server documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.



## Note

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

Cisco Aironet 1000 and 1500 series access points use a comma separated string format for DHCP Option 43. Other Cisco Aironet access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI strings for Cisco access points capable of operating in lightweight mode are listed in [Table G-1](#):

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

| Access Point              | Vendor Class Identifier (VCI) |
|---------------------------|-------------------------------|
| Cisco Aironet 1000 series | Airespace.AP1200              |
| Cisco Aironet 1100 series | Cisco AP c1100                |
| Cisco Aironet 1130 series | Cisco AP c1130                |
| Cisco Aironet 1200 series | Cisco AP c1200                |
| Cisco Aironet 1240 series | Cisco AP c1240                |
| Cisco Aironet 1300 series | Cisco AP c1300                |
| Cisco Aironet 1500 series | Cisco AP.LAP1510              |

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

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

# Configuring Option 43 for 1000 and 1500 Series Access Points

To configure DHCP Option 43 for Cisco 1000 and 1500 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

---

**Step 1** Enter configuration mode at the Cisco IOS command line interface (CLI).

**Step 2** Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

Where:

- <pool name> is the name of the DHCP pool, such as AP1000
- <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
- <Netmask> is the subnet mask, such as 255.255.255.0
- <Default router> is the IP address of the default router, such as 10.0.0.1
- <DNS Server> is the IP address of the DNS server, such as 10.0.10.2

**Step 3** Add the option 60 line using the following syntax:

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

The quotation marks must be included.

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

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

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

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

The quotation marks must be included.

---

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

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, and 1300 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

**Step 1** Enter configuration mode at the Cisco IOS CLI.

**Step 2** Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

Where:

<pool name> is the name of the DHCP pool, such as AP1240  
 <IP Network> is the network IP address where the controller resides, such as 10.0.15.1  
 <Netmask> is the subnet mask, such as 255.255.255.0  
 <Default router> is the IP address of the default router, such as 10.0.0.1  
 <DNS Server> is the IP address of the DNS server, such as 10.0.10.2

**Step 3** Add the option 60 line using the following syntax:

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

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

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

```
option 43 hex <hex string>
```

The *hex string* is assembled by concatenating the TLV values shown below:

*Type + Length + Value*

*Type* is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is  $2 * 4 = 8 = 08$  (*hex*). The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```



## GLOSSARY

|                |                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>802.3af</b> | The IEEE standard that describes a mechanism for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling.                        |
| <b>802.11</b>  | 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.              |
| <b>802.11a</b> | The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.                                         |
| <b>802.11b</b> | 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.                      |
| <b>802.11g</b> | 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

|                                |                                                                                                                                                                                                        |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access point</b>            | A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.                                                                                               |
| <b>ad hoc network</b>          | A wireless network composed of stations without Access Points.                                                                                                                                         |
| <b>antenna gain</b>            | 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. |
| <b>associated</b>              | A station is configured properly to allow it to wirelessly communicate with an Access Point.                                                                                                           |
| <b>Autonomous access point</b> | A fully featured standalone access point that does not require a Cisco Wireless LAN Controller to operate.                                                                                             |

---

**B**

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

---

**C**

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

---

**D**

|                   |                                                                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>data rates</b> | The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).                                                                   |
| <b>dBi</b>        | A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage. |



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

---

## E

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

---

## F

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

---

## G

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

---

**I**

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

---

**J****L**

|                                 |                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Lightweight access point</b> | An access point operating in the Cisco Centralized Wireless LAN Architecture with a Cisco Wireless LAN Controller.                                   |
| <b>LWAPP</b>                    | Lightweight Access Point Protocol. An Internet Engineering Task Force (IETF) draft protocol used in the Cisco Centralized Wireless LAN Architecture. |

---

**M**

|                         |                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MAC</b>              | Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter. |
| <b>modulation</b>       | Any of several techniques for combining user information with a transmitter's carrier signal.                                                                      |
| <b>multipath</b>        | The echoes created as a radio signal bounces off of physical objects.                                                                                              |
| <b>multicast packet</b> | A single data message (packet) sent to multiple addresses.                                                                                                         |

---

**O**

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

---

**P**

**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.

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

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

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

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

---

**S**

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

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

---

**T**

**transmit power** The power level of radio transmission.

---

**U**

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

---

**W**

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



## INDEX

---

### A

access point image [3-17](#)  
antenna connectors [C-2](#)

---

### B

basic settings, checking [3-4](#)  
bridge configuration [1-1](#)

---

### C

configuring DHCP Option 43 [G-2](#)  
connectors [C-1](#), [C-2](#)  
console port [E-2](#)  
    terminal emulator settings [3-21](#), [4-12](#)  
controller discovery process [2-4](#)

---

### D

data rates [C-2](#)  
declarations of conformity [B-1](#)  
default, configuration, resetting [3-15](#)  
deployment  
    access points [2-5](#)  
    process [2-5](#)  
DHCP Option 43 [4-2](#), [G-1](#)  
DHCP pool [G-2](#)  
discovery process  
    DHCP server [2-4](#)  
    DNS server [2-4](#)  
    locally stored [2-4](#)

---

### E

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

---

### F

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

---

### G

guidelines, installation [2-4](#)

---

### I

indicators [3-2](#), [4-2](#)  
input power [C-1](#)  
installation guidelines [2-4](#)

---

### K

key features [1-3](#)

---

### M

MAC information [2-5](#)  
Mode button [3-17](#)  
modulation [C-2](#)

---

### O

operating temperature [C-1](#)

---

**P**

package contents [2-3](#)  
password reset [3-15](#)  
pinouts, serial cable [E-2](#)  
power  
    connecting [2-21](#)  
    input [C-1](#)  
    output [C-2](#)  
priming access points [F-1](#)  
process, controller discovery [2-4](#)

---

**R**

range, radio [C-2](#)  
regulatory information [B-1](#)  
reloading access point image [3-17](#)  
RF exposure [B-7](#)

---

**S**

safety warnings, translated [A-1](#)  
serial  
    cable [E-2](#)  
    Cisco cable [E-2](#)  
size [C-1](#)  
status indicators [C-1](#)

---

**T**

temperature, operating [C-1](#)  
terminal emulator [3-21, 4-12](#)  
TFTP server [3-17](#)  
troubleshooting [3-1, 4-1](#)  
type-length-value (TLV) [G-2](#)

---

**U**

unpacking [2-3](#)

---

**V**

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

---

**W**

warnings [2-2, A-1](#)  
web site, Cisco Software Center [3-19, 4-11](#)  
weight [C-1](#)  
WEP key [3-5](#)