



CISCO CONFIDENTIAL - First Draft



Cisco Aironet 1300 Series Bridge Hardware Installation Guide

April 2004

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5048-01



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

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

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

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

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

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

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

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

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

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

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

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, 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 U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

Preface ix

Objectives ix

Audience ix

Organization ix

Conventions x

Related Publications xi

Obtaining Documentation xii

Cisco.com xii

Documentation CD-ROM xii

Ordering Documentation xiii

Documentation Feedback xiii

Obtaining Technical Assistance xiii

Cisco TAC Website xiii

Opening a TAC Case xiv

TAC Case Priority Definitions xiv

Obtaining Additional Publications and Information xiv

CHAPTER 1

Overview 1-1

Key Features 1-2

Power 1-3

Integrated Antenna 1-3

External Antenna 1-3

Ethernet Ports 1-4

Enclosure 1-4

Bridge Connectors 1-4

Bridge LEDs 1-5

Network Configuration Examples 1-6

Point-to-Point Configuration 1-6

Port Aggregation or Redundancy Configuration 1-6

Point-to-Multipoint Configuration 1-7

Workgroup Bridge Configuration 1-7

Access Point Configuration 1-8

CISCO CONFIDENTIAL - First Draft

CHAPTER 2**Installation Overview 2-1**

- Warnings 2-2
- Safety Information 2-3
 - FCC Safety Compliance Statement 2-3
 - Safety Precautions 2-3
 - Typical Bridge Installation Components 2-4
- Installation Guidelines 2-5
- Site Surveys 2-5
- Unpacking the Bridge 2-5
 - Package Contents 2-6
- Before Beginning the Installation 2-6
- Installation Summary 2-8

CHAPTER 3**Mounting and Alignment Overview 3-1**

- Mounting the Bridge 3-2
- Mounting Hardware 3-2
 - Multi-function Mount 3-2
 - Bridge Bracket 3-3
 - Mast Bracket 3-3
- Bridge LEDs 3-3
- Aligning the Antenna Using RSSI LED Indications 3-5

CHAPTER 4**Stacking Bridges 4-1**

- Overview 4-2
- Choosing a Second Mounting Location 4-2
- Installing the Stacked Bridges 4-2
- Verifying Isolation - TBD 4-3

CHAPTER 5**Configuring the Bridge for the First Time 5-1**

- Before You Start 5-2
 - Resetting the Bridge to Default Settings 5-2
- Obtaining and Assigning an IP Address 5-3
- Connecting to the Bridge Locally 5-3
- Assigning Basic Settings 5-4
 - Default Settings on the Express Setup Page 5-8

CISCO CONFIDENTIAL - First Draft

What To Do Next	5-9
Output Power Level	5-9
Protecting Your Wireless LAN	5-9
Using the IP Setup Utility	5-9
Obtaining and Installing IPSU	5-10
Using IPSU to Find the Bridge's IP Address	5-10
Using IPSU to Set the Bridge's IP Address and SSID	5-12
Assigning an IP Address Using the CLI	5-13
Using a Telnet Session to Access the CLI	5-13

CHAPTER 6

Using the Web-Browser Interface 6-1

Using the Web-Browser Interface for the First Time	6-2
Using the Management Pages in the Web-Browser Interface	6-2
Using Action Buttons	6-3
Character Restrictions in Entry Fields	6-5
Using Online Help	6-5

CHAPTER 7

Using the Command-Line Interface 7-1

IOS Command Modes	7-2
Getting Help	7-3
Abbreviating Commands	7-3
Using no and default Forms of Commands	7-3
Understanding CLI Messages	7-4
Using Command History	7-4
Changing the Command History Buffer Size	7-5
Recalling Commands	7-5
Disabling the Command History Feature	7-5
Using Editing Features	7-6
Enabling and Disabling Editing Features	7-6
Editing Commands through Keystrokes	7-6
Editing Command Lines that Wrap	7-7
Searching and Filtering Output of show and more Commands	7-8
Accessing the CLI	7-9
Opening the CLI with Telnet	7-9
Opening the CLI with Secure Shell	7-9

CISCO CONFIDENTIAL - First Draft**CHAPTER 8****Troubleshooting 8-1**

- Checking the Bridge LEDs 8-2
 - Bridge Normal Mode LED Indications 8-2
- Power Injector 8-4
- Checking Power 8-5
- Checking Basic Configuration Settings 8-5
 - SSID 8-5
 - Security Settings 8-5
- Antenna Alignment 8-5
- Resetting to the Default Configuration - TBD 8-6
 - Using the Serial Console Port -TBD 8-6
 - Using the Web Browser Interface - TBD 8-6
- Reloading the Bridge Image - TBD 8-7
 - Using the Serial Console Port - TBD 8-7
 - Web Browser Interface - TBD 8-8
 - Browser HTTP Interface 8-8
 - Browser TFTP Interface 8-8
- Obtaining the Bridge Image File 8-9
- Obtaining the TFTP Server Software 8-9

APPENDIX A**Translated Safety Warnings A-1**

- Installation Warning A-2
- Installation and Grounding Warning A-2
- Ground Conductor Warning A-4
- Lightning Activity Warning A-6
- Antenna Installation Warning A-7
- Explosive Device Proximity Warning A-8
- Circuit Breaker (15A) Warning A-9

APPENDIX B**Declarations of Conformity and Regulatory Information B-1**

- Manufacturers Federal Communication Commission Declaration of Conformity Statement B-2
- Department of Communications—Canada B-3
 - Canadian Compliance Statement B-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein B-3
 - Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC B-3
- Declaration of Conformity for RF Exposure B-5

CISCO CONFIDENTIAL - First Draft

Guidelines for Operating Cisco Aironet Access Points and Bridges in Japan	B-5
Japanese Translation	B-5
English Translation	B-5
Administrative Rules for Cisco Aironet Bridges in Taiwan	B-6
All Bridges	B-6
Chinese Translation	B-6
English Translation	B-6

APPENDIX C

Specifications C-1

Operating Range	C-5
-----------------	------------

APPENDIX D

Channels and Antenna Settings D-1

Channels	D-2
IEEE 802.11g (2.4-GHz Band)	D-2
Maximum Power Levels and Antenna Gains	D-3
IEEE 802.11g (2.4-GHz Band)	D-3
Changing the Bridge's Output Power	D-4

GLOSSARY

INDEX

CISCO CONFIDENTIAL - First Draft

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Aironet 1300 Series Bridge Hardware Installation Guide*.

Objectives

This publication explains the steps for initial setup and basic configuration of the Cisco Aironet 1300 Series Wireless Bridge (hereafter called the *bridge*) supporting 2.4-GHz operation. This publication also provides troubleshooting information and detailed specifications.

Audience

This publication is for the person installing and configuring a bridge for the first time. The installer should be familiar with network structures, terms, and concepts.

Organization

This guide contains the following sections:

[Chapter 1, “Overview,”](#) describes the major components, features, and specifications of the bridge.

[Chapter 2, “Installation Overview,”](#) provides warnings, safety information, and information needed before you begin the installation of your bridge system.

[Chapter 3, “Mounting and Alignment Overview,”](#) provides an overview of components and features used during bridge mounting and antenna alignment operations.

[Chapter 4, “Stacking Bridges,”](#) describes the how to install and verify stacked bridges for increased bandwidth.

[Chapter 5, “Configuring the Bridge for the First Time,”](#) describes how to enter basic bridge configuration settings.

[Chapter 6, “Using the Web-Browser Interface,”](#) describes how to use the web-browser interface to configure the bridge.

[Chapter 7, “Using the Command-Line Interface,”](#) describes how to use the command-line interface (CLI) to configure the bridge.

[Chapter 8, “Troubleshooting,”](#) provides solutions to potential problems encountered during setup.

CISCO CONFIDENTIAL - First Draft

Appendix A, “Translated Safety Warnings,” lists translations of the safety warnings in this publication.

Appendix B, “Declarations of Conformity and Regulatory Information,” describes the regulatory conventions to which the bridge conforms and provides guidelines for operating bridges in Japan.

Appendix C, “Bridge Specifications,” describes the channels and antenna settings supported by the regulatory organizations.

Appendix D, “Channels and Antenna Settings,” lists the access point radio channels and the maximum power levels supported by the world’s regulatory domains

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.



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 in 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).

CISCO CONFIDENTIAL - First Draft

Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körpverletzung 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

For more information about bridges and related products, refer to the following publications:

- *Quick Start Guide: Cisco Aironet 1300 Series Bridge* describes the bridge, system components, and how to obtain bridge documentation. This document is included in the shipping box with your bridge.
- *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* describes the bridge's management system and explains how to configure the bridge. This document is available on the Cisco CCO web site at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
- *Cisco Aironet 1400 Series Wireless Bridge Mounting Instructions* that was shipped with your bridge provides detailed instructions for mounting the bridge and aligning the antenna.

CISCO CONFIDENTIAL - First Draft

- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* describes the IOS commands supported by Cisco Aironet access points and bridges. This document is available on the Cisco CCO web site at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
- *Release Notes for Cisco Aironet 1300 Series Bridge* describes features and caveats for the bridge running IOS release 12.2(11)JA. This document is available on the Cisco CCO web site at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
- Cisco Secure Access Control Server for Windows 2000/NT Servers Version 3.0 User Guide provides complete instructions for using Cisco Secure ACS, including steps for configuring Cisco Secure ACS to support access points and bridges. This document is available on the Cisco CCO web site at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt30/user/index.htm

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

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

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

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

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

CISCO CONFIDENTIAL - First Draft

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

CISCO CONFIDENTIAL - First Draft

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

CISCO CONFIDENTIAL - First Draft

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

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

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

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

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

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

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

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

CISCO CONFIDENTIAL - First Draft

Overview

The Cisco Aironet 1300 Series Bridget (hereafter called the *bridge*) is a wireless device designed for building-to-building wireless connectivity. Operating in the 2.4-GHz band (2.400 to 2.497 GHz), using the IEEE 802.11g standard, the bridge delivers 1 to 54 Mbps data rates without the need for a license. The bridge is a self-contained unit designed for outdoor installations, providing differing antenna gains as well as coverage patterns. It supports point-to-point and multipoint bridging configurations. When placed in access point mode, the bridge supports wireless IEEE 802.11b and IEEE 802.11g client devices.

The bridge uses a browser-based management system, but you can also configure the bridge using Cisco IOS commands or Simple Network Management Protocol (SNMP).

This chapter provides information on the following topics:

- [Key Features, page 1-2](#)
- [Network Configuration Examples, page 1-6](#)

Key Features

Key features of the bridge:

- Unlicensed IEEE 802.11g 2.4-GHz radio operation
- Enclosure supports indoor or outdoor installations
- Integrated antenna or external antenna configurations (see Figure 1-1)
- Dual-coax 100-Mbps Ethernet ports
- Four LEDs on bridge
- Inline power over dual-coax cables
- Receive Signal Strength Indicator (RSSI) LED patterns for easy antenna alignment
- Bridge control using Cisco IOS commands, Internet browser, or SNMP

Figure 1-1 Bridge Configurations



1	Integrated antenna bridge configuration	2	External antenna bridge configuration
---	---	---	---------------------------------------


Note

Antenna connectors are available only on the external antenna bridge configuration.

CISCO CONFIDENTIAL - First Draft

Power

The bridge receives inline power from the Cisco Aironet Power Injector (hereafter called the *power injector*). Dual-coax cables are used to provide Ethernet data and power from the power injector to the bridge. The power injector is an external unit designed for operation in a sheltered environment, such as inside a building or vehicle. The power injector also functions as an Ethernet repeater by connecting to a Category 5 LAN backbone and using the dual-coax cable interface to the bridge.

The power injector uses an external 48-VDC power module and injects the DC voltage into the dual-coax cables to power the bridge. The power injector can be also directly connected to a +12 VDC to +48 VDC power source, such as a vehicle battery.

**Note**

The power injector and the power module should not be placed in an outdoor unprotected environment or in an environmental air space, such as above a suspended ceiling.

Integrated Antenna

The bridge is available with an integrated 13-dBi patch array antenna. The antenna is covered with a radome to protect it from environmental elements. When configured with the integrated antenna, the antenna polarization is controlled by the mounting orientation of the bridge.

**Note**

Some international regulatory regions may restrict the integrated antenna bridge configuration.

External Antenna

The bridge is available in an external antenna configuration (see [Figure 1-1](#)) for use with existing Cisco Aironet 2.4-GHz antennas. Two reverse-TNC type RF connectors are provided on the end of the unit to support single or diversity antenna configurations.

The antennas connect to the bridge antenna connectors using a coax cable. The list below contains some of the external antennas supported by the bridge.

- 2.2 dBi omnidirectional
- 5.2-dBi omnidirectional antenna with vertical polarization
- 12-dBi omnidirectional antenna with vertical polarization
- 9-dBi patch wall mount antenna
- 10 dBi yagi antenna
- 13.5 dBi yagi antenna
- 15-dBi sector antenna with vertical polarization
- 21-dBi dish antenna

**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

CISCO CONFIDENTIAL - First Draft

**Note**

Some international regulatory regions may restrict the use of some external antennas.

Ethernet Ports

The bridge's power injector dual-coax ports accept a pair of 75-ohm F-type connectors, linking the bridge to your 100BASE-T Ethernet LAN through the power injector. The dual-coax cables are used to send and receive Ethernet data and to supply inline 48-VDC power from the power injector. For the location of the ports, refer to [Figure 1-3](#).

**Tip**

You can connect the dual-coax cable connectors to either of the bridge's power injector dual-coax ports. The bridge senses the Ethernet signals and automatically switches internal circuitry to match the cable connections.

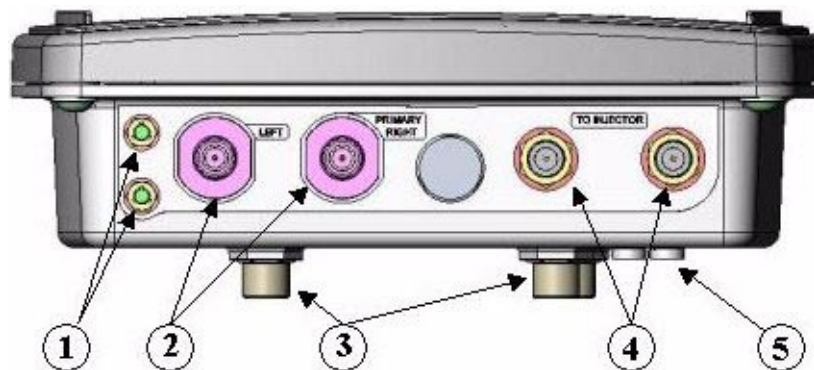
Enclosure

The bridge uses an enclosure that supports indoor or outdoor operating environments. (refer to [“Bridge Specifications”](#) section on page C-1).

Bridge Connectors

The connectors (see [Figure 1-2](#)) provided depends upon the bridge configuration:

- Integrated antenna bridge configuration
 - Dual-coax Ethernet connectors—used to provide Ethernet signals and in-line power
- External antenna bridge configuration
 - Dual-coax Ethernet connectors—used to provide Ethernet signals and in-line power
 - Dual antenna connectors—used to support a single antenna or dual-diversity antennas

CISCO CONFIDENTIAL - First Draft**Figure 1-2 Bridge Connector Locations**

1	Ground lug mounting screws	3	Bridge mounting posts
2	Left antenna connector (external antenna bridge configuration only)	4	Dual-coax Ethernet ports
	Primary right antenna connector (external antenna bridge configuration only)	5	Bridge LEDs

Bridge LEDs

Four LEDs are located on back of the housing to report installation and alignment conditions, bridge status, radio activity, and Ethernet activity (see [Figure 1-3](#)).

Figure 1-3 Bridge LEDs

1	Radio LED (R)	3	Ethernet LED (E)
2	Status LED (S)	4	Install LED (I)

CISCO CONFIDENTIAL - First Draft

The bridge LEDs are shown in [Figure 1-3](#).

- The install LED indicates that installation mode is activated. During installation mode, the other LEDs provide signal strength readings used for antenna alignment.
- The radio LED blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the bridge radio link. This LED also provides signal strength readings during installation mode.
- The status LED signals bridge association status. Blinking green indicates that the bridge is not associated with another bridge. Steady green indicates that the bridge is associated with at least one other bridge. This LED also provides signal strength readings during installation mode.
- The Ethernet LED signals Ethernet traffic. This LED blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet link not working or the port is shutdown. This LED also provides signal strength readings during installation mode.

For additional information on the LEDs, refer to “[Checking the Bridge LEDs](#)” section on page 8-2.

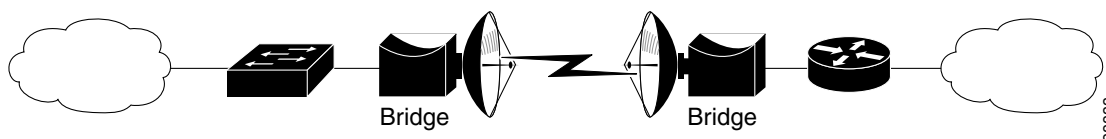
Network Configuration Examples

This section describes the bridge’s role in five common wireless network configurations.

Point-to-Point Configuration

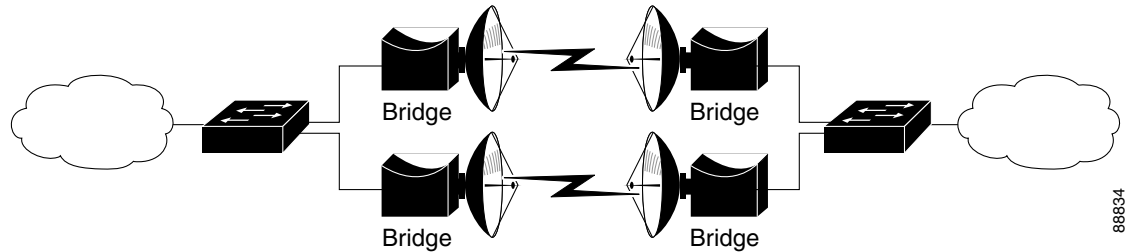
In a point-to-point configuration, two bridges connect two remote LAN networks using a wireless communication link (see [Figure 1-4](#)). The bridge connected to the main LAN network is classified as a root bridge and the other bridge is classified as a repeater bridge.

Figure 1-4 Point-to-Point Bridge Configuration



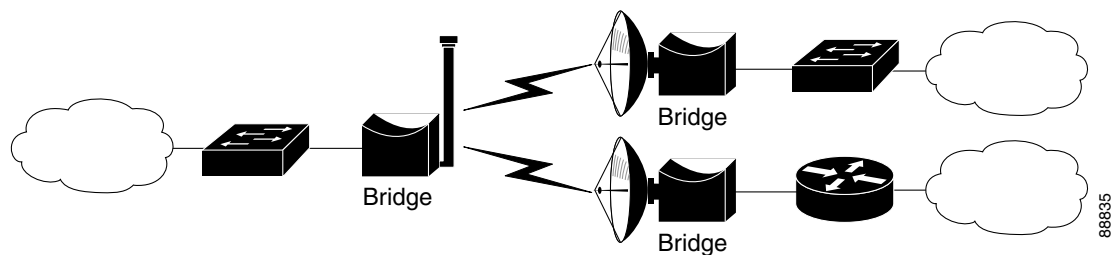
Port Aggregation or Redundancy Configuration

The port aggregation or redundancy configuration ([Figure 1-5](#)) is used to provide increased bandwidth or backup redundancy communications between two LANs. Port aggregation or increased bandwidth occurs when both wireless links are used to simultaneously pass Ethernet traffic. Backup communication redundancy can be achieved with this configuration when one wireless bridge link is used only if the other wireless bridge link fails.

CISCO CONFIDENTIAL - First Draft**Figure 1-5 Port Aggregation or Redundancy Bridge Configuration**

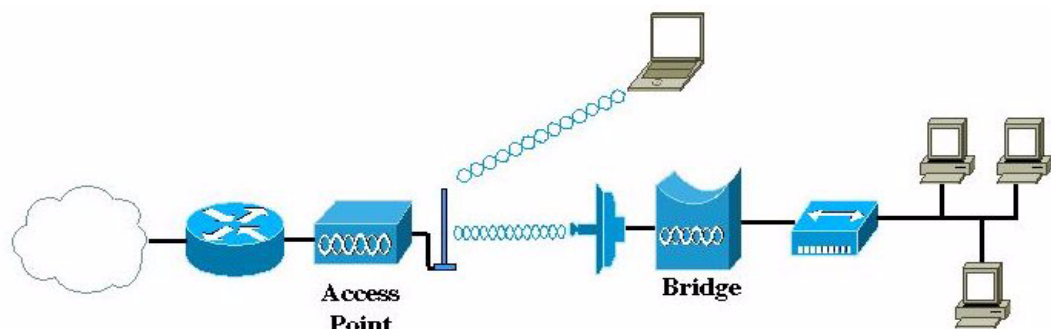
Point-to-Multipoint Configuration

The point-to-multipoint configuration (Figure 1-6) connects the main LAN network to multiple remote LAN networks.

Figure 1-6 Point-to-Multipoint Bridge Configuration

Workgroup Bridge Configuration

The workgroup bridge configuration (Figure 1-7) connects remote workstations to an access point.

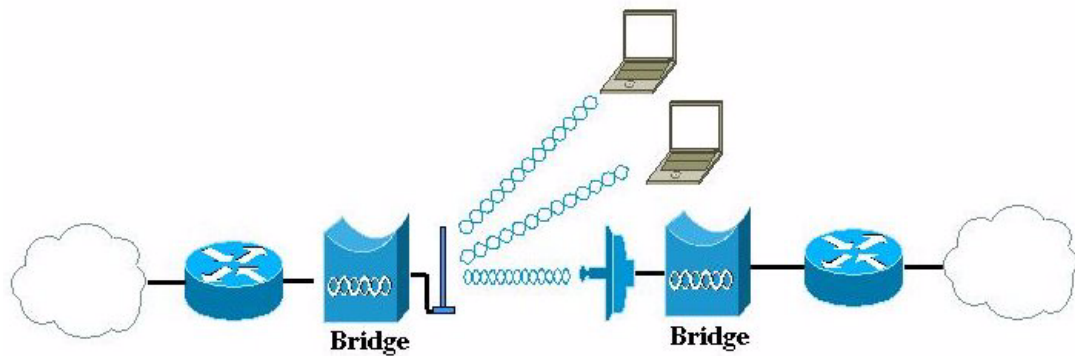
Figure 1-7 Workgroup Bridge Configuration

CISCO CONFIDENTIAL - First Draft

Access Point Configuration

The bridge's access point configuration mode (Figure 1-8) supports remote bridge networks and wireless client devices.

Figure 1-8 Access Point Configuration



Installation Overview

This chapter provides warnings, safety information, and information needed before you begin the installation of your bridge system. This chapter includes the following sections:

- [Safety Warnings, page 2-2](#)
- [Safety Information, page 2-3](#)
- [Unpacking the Bridge, page 2-5](#)
- [Before Beginning the Installation, page 2-6](#)
- [Installation Summary, page 2-8](#)

CISCO CONFIDENTIAL - First Draft

Safety 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. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”) Statement 84



Warning

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).

Statement 1052



Warning

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

120 VAC, 15A U.S. (240 VAC, 10A International) Statement 1005



Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024



Warning

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



Warning

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

Statement 1001



Warning

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

Statement 245B



Warning

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



Warning

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

Statement 1040

CISCO CONFIDENTIAL - First Draft

Safety Information

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

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to 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 operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

**Warning**

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution, but did not take adequate steps to avoid the hazard.

For your safety, and to help you achieve a good installation, please read and follow these safety precautions. They may save your life!

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance.
2. Select your installation site with safety, as well as performance in mind. Remember: electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successful raising of a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task, and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing your antenna, remember:
 - a. Do not use a metal ladder.
 - b. Do not work on a wet or windy day.
 - c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember, the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line complete an electrical path through the antenna and the installer: you!

CISCO CONFIDENTIAL - First Draft

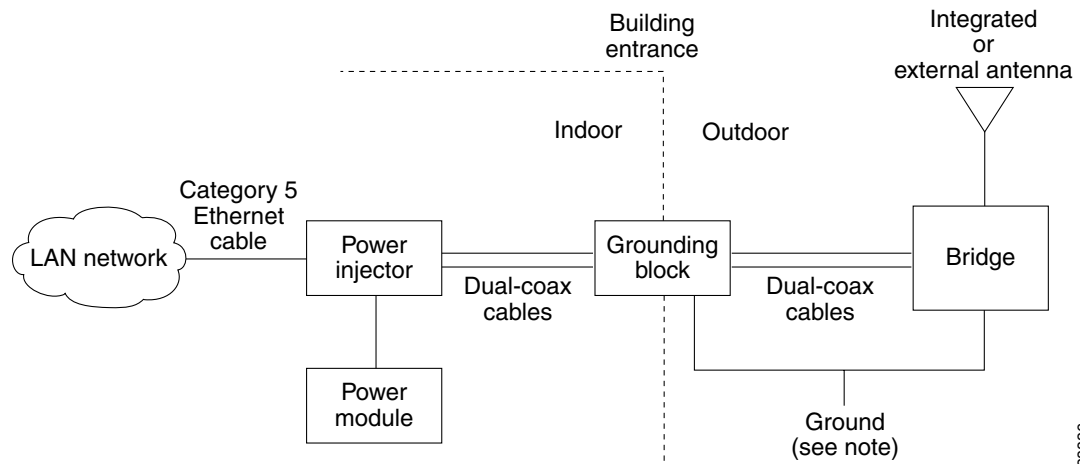
7. If any part of the antenna system should come in contact with a power line, don't touch it or try to remove it yourself. Call your local power company. They will remove it safely.

If an accident should occur with the power lines call for qualified emergency help immediately.

Typical Bridge Installation Components

The bridge is designed to be installed in an outdoor environment, typically, on a tower or a tall building. A typical bridge installation diagram is shown in [Figure 2-1](#).

Figure 2-1 Typical Bridge Installation Diagram



Note

Ground wires must comply with Sections 810 and 820 of the National Electrical Code and Section 54 of the Canadian Electrical Code.



Caution

To ensure correct installation and grounding, install the bridge in compliance with your local and national electrical codes: National Fire Protection Association (NFPA) 70, National Electrical Code (U.S.); Canadian Electrical Code, Part I, CSA 22.1 (Canada); and if local or national electrical codes are not available, refer to IEC 364, Part 1 through 7 (other countries).

CISCO CONFIDENTIAL - First Draft

Installation Guidelines

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

- Install the bridge in an area where structures, trees, or hills do not obstruct radio signals to and from the bridge.
- Install the bridge at a height sufficient to provide clear line-of-sight signal path.

Site Surveys

Every network application is a unique installation. Before installing multiple bridges, you should perform a site survey to determine the optimum use of networking components and to maximize range, coverage, and network performance.

Consider the following operating and environmental conditions when performing a site survey:

- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
- Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary, because the extra height also increases potential interference from other unlicensed radio systems.
- Physical environment—Clear or open areas provide better radio range than closed or filled areas.
- Obstructions—Physical obstructions such as buildings, trees, or hills can hinder performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.

Unpacking the Bridge

Follow these steps to unpack the bridge:

-
- | | |
|---------------|--|
| 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. If any item is damaged or missing, notify your authorized Cisco sales representative. |
-

CISCO CONFIDENTIAL - First Draft

Package Contents

Each bridge package contains the following items:

- Bridge unit
- Power injector unit (with mounting screws and wall anchors)
- Power module and AC power cord (with mounting screws and wall anchors)
- Two dual-coax cables [20 ft (6.1 m) and 50 ft (15.2 m)]
- Mounting kit and hardware
 - Multi-function mount (consisting of two bridge brackets and one tower or mast bracket)
 - Two tower clamps (U-bolts) with four nuts and washers
 - Four bolts, lock washers, and washers for securing the bridge brackets to the tower or mast bracket
 - Four bolts and lock washers for securing the bridge brackets to the bridge
- Grounding block and mounting screws
- Ground lug for the bridge with screws
- Weatherproofing kit (consisting of Coax Seal and electrical joint compound)
- *Quick Start Guide: Cisco Aironet 1300 Series Wireless Bridge*
- *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions*
- Cisco product registration and Cisco documentation feedback cards

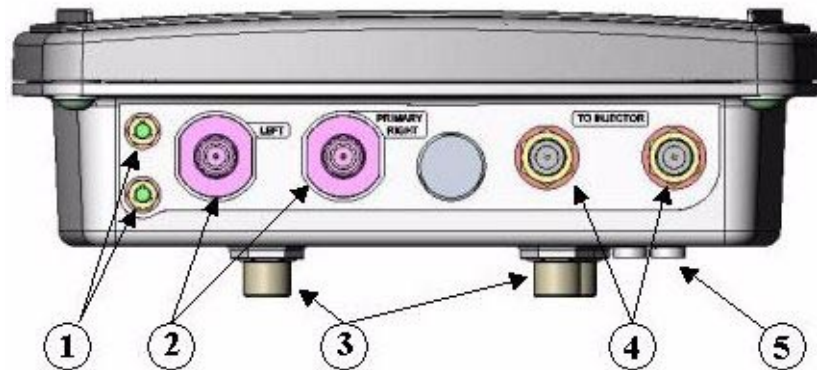
Before Beginning the Installation

Before you begin the installation process, please carefully review the following list of figures to become familiar with the system components, connectors, indicators, cables, system interconnection, and grounding:

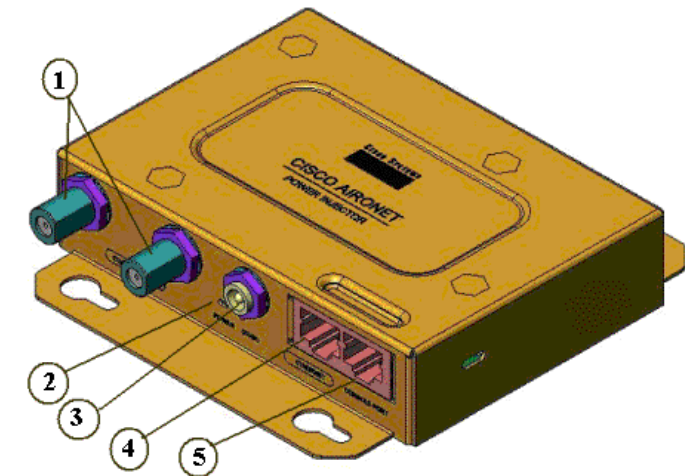
- Bridge Installation diagram ([Figure 2-1](#))
- Bridge layout ([Figure 2-2](#))
- Power injector layout ([Figure 2-3](#))
- Power module ([Figure 2-4](#))
- Grounding block ([Figure 2-5](#))

**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

CISCO CONFIDENTIAL - First Draft**Figure 2-2 Bridge Layout**

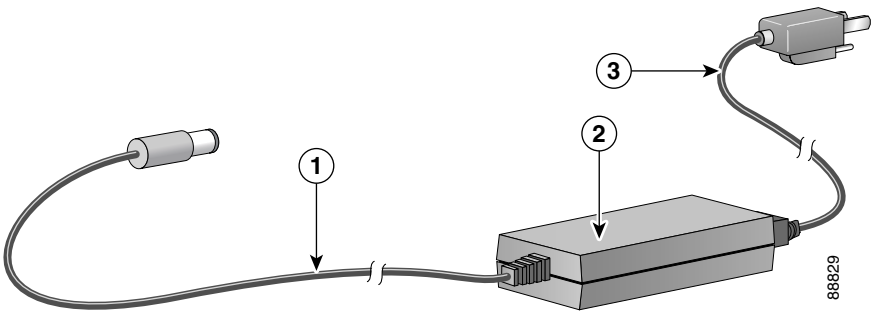
1	Grounding studs	4	Power injector dual-coax ports (F-Type connectors)
2	Antenna connectors	5	Bridge LEDs
3	Mounting studs		

Figure 2-3 Power Injector Indicators and Connectors

1	Power injector dual-coax ports (F-Type connectors)	4	Ethernet port (RJ-45 connector)
2	Power LED	5	Serial Console Port (RJ-45 connector)
3	Power jack (12 to 48 VDC)		

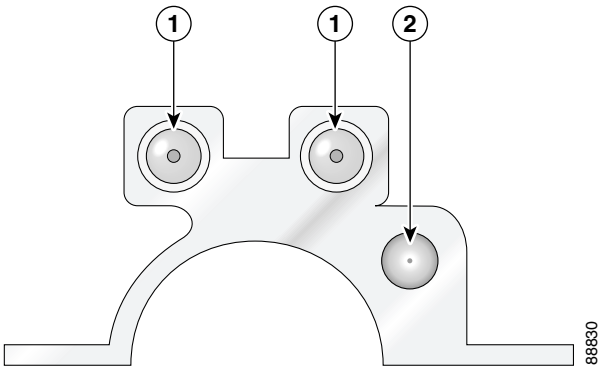
CISCO CONFIDENTIAL - First Draft

Figure 2-4 Power Module



1	48-VDC power output cable	3	AC power cord
2	Power module		

Figure 2-5 Grounding Block



1	F-type coaxial connectors	2	Ground wire lug
---	---------------------------	---	-----------------

Installation Summary

Warning

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

During the installation of the bridge, you will perform the following operations:

- Connect a user-supplied Category 5 Ethernet cable from your wired LAN network to the power injector.
- Connect the dual-coax Ethernet cables between the power injector and the grounding block.

Tip

You can connect the dual-coax cable connectors to either of the grounding block connectors or the power injector’s dual-coax ports. The bridge senses the Ethernet signals and automatically switches internal circuitry to match the cable connections.

CISCO CONFIDENTIAL - First Draft**Note**

You should securely tighten the cable connectors (15 to 20 inch-pounds) using a small wrench.

- Connect a ground wire to the grounding block.
- Mount the bridge to the external tower or mast. For additional information, refer to the *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions* that shipped with your bridge.

**Warning**

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

- Connect a ground wire to the bridge (use the bridge ground lug).
- Connect the dual-coax Ethernet cables to the grounding block and to the bridge.

**Tip**

You can connect the dual-coax cable connectors to either of the grounding block connectors or the bridge's dual-coax ports. The bridge senses the Ethernet signals and automatically switches internal circuitry to match the cable connections.

**Note**

You should securely tighten the cable connectors (15 to 20 inch-pounds) using a small wrench.

**Warning**

**This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:
120 VAC, 15A U.S. (240 VAC, 10A International)**

- Connect the AC power cord to the 48-VDC power module.
- Connect the power module to the power injector and plug the AC cord into an AC power receptacle.
- Align the bridge antenna. For additional information, refer to the *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions* that shipped with your bridge.
- Configure basic settings (refer to [Chapter 5, "Configuring the Bridge for the First Time"](#)).
- Seal all external connectors with special weather sealing material.

Configure security and other bridge options. For additional information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges*.

CISCO CONFIDENTIAL - First Draft

Mounting and Alignment Overview

This chapter provides an overview of bridge mounting and antenna alignment. The following sections are included in this chapter:

- [Mounting the Bridge, page 3-2](#)
- [Mounting Hardware, page 3-2](#)
- [Bridge LEDs, page 3-3](#)
- [Aligning the Antenna Using RSSI LED Indications, page 3-5](#)

CISCO CONFIDENTIAL - First Draft

Mounting the Bridge

Typically, the bridge is installed on a rooftop, mast, tower, wall, or a suitable flat surface. Each of these installations requires a different approach. This document provides a mounting overview. For detailed mounting instructions, refer to the *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions* that shipped with your bridge.

The bridge is available in two configurations:

- Integrated antenna bridge (with 13-dBi)
- External antenna bridge (with two antenna connectors for use with a single antenna or dual diversity antennas)

Personnel installing the bridge must understand wireless bridging techniques, antenna alignment and adjustment, and grounding methods. The integrated antenna bridge can be installed by an experienced IT professional.

**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Mounting Hardware

The bridge is shipped with the following mounting hardware:

- Multi-function mount (consisting of one bridge bracket and one mast bracket)
- Fastener hardware (consisting of nuts, bolts, washers, and U-bolts)

Multi-function Mount

The multi-function mount provides a method for mounting the bridge on a mast, tower, or an optional roof-mast mount. The multi-function mount permits easy azimuth and elevation adjustments for antenna alignment purposes. The basic mounting procedure is shown below:

1. Mount the bridge bracket to the bridge.
2. Mount the mast bracket to the tower or mast using the supplied U-bolts.
3. Suspend the bridge on the mast bracket using the support pins.
4. Secure the bridge bracket to the mast bracket using the supplied nuts, bolts, and washers (hand tighten).
5. Connect the dual-coax cable to the power injector dual-coax ports (F-type connectors) on the bridge.

**Note**

You should securely tighten the cable connectors (15 to 20 inch-pounds) using a small wrench.

6. Connect the ground wire to the bridge.
7. Align the bridge and tighten the nuts and bolts.

CISCO CONFIDENTIAL - First Draft

Bridge Bracket

The bridge bracket mounts on the back side of the bridge housing. The bracket mounts on four screw posts on the unit. The support pins on the bridge bracket must be facing the sides of the unit. These support pins are used to suspend the bridge in the notches on the mast mounting bracket until you secure the mounting bolts.

The bridge brackets must be positioned to obtain the correct antenna polarization that matches the remote antenna. The bridge housing contains an antenna polarization mark consisting of an arrow on the side of the housing. When the bridge is positioned so that the arrow is pointing up, the bridge antenna is vertically polarized. For horizontal polarization, the arrow should be pointing from left to right. All bridges must use the same antenna polarization for best operation.

Mast Bracket

The mast bracket attaches to a mast or tower support and is used to secure the bridge. The procedure for attaching the mounting bracket to the support depends on the pipe diameter, as shown in [Table 3-1](#).

Table 3-1 Mast Bracket Attachment Methods

Mast Type	Mast Diameter	Mast Attachment Method
Roof mount, small mast, or tower	1.5 to 2.5 in. (30.5 to 63.5 mm)	Attach the pipe inside the mounting bracket, between the bracket and bridge.
Large mast	2.5 to 4.5 in. (63.5 to 115 mm)	Attach the pipe outside the mounting bracket, away from the bridge.

**Note**

The U-bolts supplied with the bridge support mast diameters up to 1.75 in. (44.5 mm). For larger masts, you must supply the U-bolts to attach the bridge.

Bridge LEDs

When you power up the bridge for the first time, it starts in a special installation mode. The LEDs indicate the startup status, operating mode, association status, and received signal strength. This information simplifies the process of activating the link and positioning the antenna from the bridge mounting location.

CISCO CONFIDENTIAL - First Draft

The LEDs are mounted on the back of the housing (see [Figure 3-1](#)).

Figure 3-1 Bridge LEDs



1	Radio LED (R)	3	Ethernet LED (E)
2	Status LED (S)	4	Install LED (I)

When the bridge is initially powered-up, installation mode is activated and the bridge attempts to associate to a root bridge for 60 seconds. If it is unable to associate with a root bridge, it automatically assumes the root bridge role. The Install LED provides bridge association status during installation mode as shown in [Table 3-2](#).

Table 3-2 Install LED Association Status

Install LED	State	Bridge State
Off	Self test	Startup.
Amber blinking	Non-root, searching	Not associated (non-root mode). The bridge attempts to associate with a root bridge for 60 seconds ¹ .
Amber	Non-root, associated	Associated (non-root mode).
Green blinking	Root, searching	Not associated (root mode). The bridge attempts to associate with a non-root bridge indefinitely.
Green	Root, associated	Associated (root mode).

1. Preconfigured bridges search indefinitely.

CISCO CONFIDENTIAL - First Draft

Use the Install LED to determine when the bridge successfully associates with a remote bridge and to verify its mode of operation. After association, the other three LEDs indicate signal strength.

The startup and association sequence depends on the bridge configuration, which can be one of the following types:

- **Default**—The bridge attempts to associate with a root bridge for 60 seconds. If it does not associate with a root bridge, it then attempts to associate with a non-root bridge.
- **Preconfigured**—The bridge attempts to associate with a remote bridge in the configured mode, either root or non-root. Because there are no timeouts, it is easier to align the antenna.

Aligning the Antenna Using RSSI LED Indications

You can align the integrated antenna using LEDs after the bridge successfully associates with a remote bridge. In the installation mode before association to another bridge, the Install LED blinks amber. If the bridge associates to a root bridge, the Install LED turns amber. If the bridge does not associate to a root bridge in the first 60 seconds, the Install LED blinks green to indicate beacons are being transmitted and the bridge is waiting for another non-root bridge to associate.

During the first 20 seconds after association, the bridge reads the receive signal strength indicator (RSSI) levels and records the maximum level received. Once 20 seconds have elapsed, the Install LED turns amber and the Ethernet, status, and radio LEDs then display the relative RSSI levels compared to the maximum received. The RSSI LED indications are shown in [Table 3-3](#).


Note

For the signal level (dBm), a smaller number represents a stronger signal because the signal level is given as a negative value.

Table 3-3 LED Installation Mode RSSI Display

RSSI Level (dBm)	Ethernet LED	Status LED	Radio LED
> -44	On	On	On
-47 to -44	Fast blink ¹	On	On
-50 to -47	Medium blink ²	On	On
-53 to -50	Slow blink ³	On	On
-54 to -53	Off	On	On
-57 to -54	Off	Fast blink ¹	On
-60 to -57	Off	Medium blink ²	On
-63 to -60	Off	Slow blink ³	On
-66 to -63	Off	Off	On
-69 to -66	Off	Off	Fast blink ¹
-72 to -69	Off	Off	Medium blink ²
-75 to -72	Off	Off	Slow blink ³
< -75	Off	Off	Off

1. Slow blinking rate of 1 blink/sec.

2. Medium blinking rate of 2 blinks/sec.

3. Fast blinking rate of 4 blinks/sec.

CISCO CONFIDENTIAL - First Draft

When using LEDs to maximize the signal, adjust the antenna until as many LEDs as possible are turned on and the rest are blinking as fast as possible.

Stacking Bridges

This chapter describes how to install stacked bridges for increased bandwidth and how to verify their isolation. This chapter contains the following topics:

- [Overview, page 4-2](#)
- [Choosing a Second Mounting Location, page 4-2](#)
- [Installing the Stacked Bridges, page 4-2](#)
- [Verifying Isolation - TBD, page 4-3](#)

CISCO CONFIDENTIAL - First Draft

Overview

You can double the throughput, or create a standby link, by stacking two bridges. A stacked installation consists of two bridge systems installed at the same physical location. For detailed mounting instructions refer to the *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions* that shipped with your bridge.

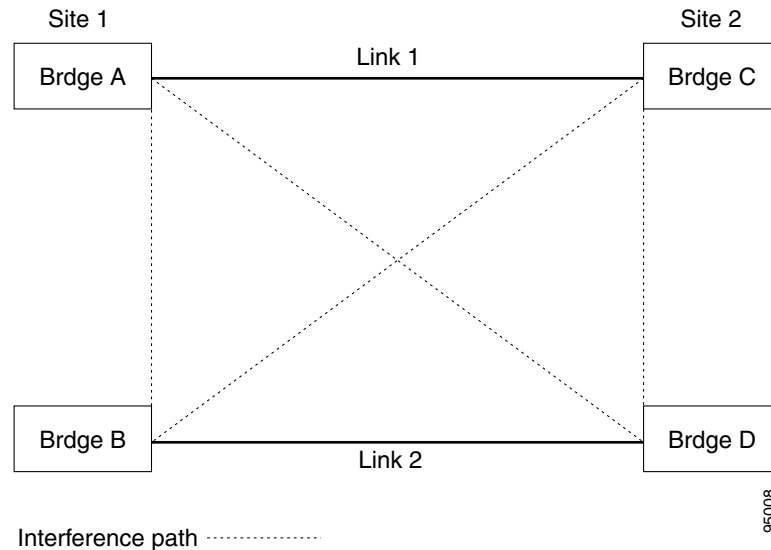
**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Choosing a Second Mounting Location

You can mount the second bridge system in the same general location as the first as long as you separate the antennas by at least **TBD** ft (**TBD** m). For example, in a flat-roof installation you can separate the bridges horizontally, roughly perpendicular to the line of signal propagation. In a tower installation, you can separate the antennas vertically. During the activation process, you verify that the interference between systems is acceptably low. Do not attempt to stack more than two bridges. [Figure 4-1](#) identifies the interference paths with stacked bridges.

Figure 4-1 Interference Paths with Stacked Bridges



Installing the Stacked Bridges

To install stacked bridges, refer to [Figure 4-1](#) as you follow these steps:

CISCO CONFIDENTIAL - First Draft

-
- Step 1** Install the link 1 bridges (bridges A and C) normally, but leave room at each site to install the link 2 bridges (bridges B and C).
- Step 2** Activate the link 1 bridges, align the antennas, and verify proper operation of the link.
- Step 3** At each site location, choose a candidate location for the second bridge that is at least **TBD** ft (**TBD** m) away from the first bridge. Separate the bridges as far as is practical from each other, keeping in mind that the second antenna must have a clear path to the remote system.
- Step 4** At each site location, temporarily install the second link 2 bridge, positioning the antenna toward the intended location of the corresponding link 2 remote antenna.



Note You can improve system isolation by using different polarizations for the two local antennas. For example, if the link 1 system has vertical polarization, assemble the link 2 system for horizontal polarization.

Verifying Isolation - **TBD**

Isolation measurements are valid only if the link 1 bridges are operating at maximum power. By default, the bridge operates at maximum power.

To verify signal isolation, refer to [Figure 4-1](#) as you follow these steps:

-
- Step 1** Ensure that the link 1 bridges are operating at full power and bridge A is configured as the root bridge.
- Step 2** At Site 1, measure the isolation between bridges A and B:
- Activate the link 2 bridge (bridge B) as a non-root bridge and let it associate to bridge A (the root bridge).
 - Observe the bridge LEDs and verify that the RSSI signal level is (**-54 dBm to -53 dBm**) or less. If the RSSI signal exceeds **-54 dBm**, move the bridge farther away and repeat this procedure.
 - Slowly rotate the bridge B antenna a few degrees to the left and to the right and verify that the RSSI signal level does not spike above **-54 dBm**. If the signal peaks above **-54 dBm**, move the bridge farther away and repeat this step.
- Step 3** Go to the remote Site 2 location to measure the isolation between bridges A and D:
- Activate the link 2 bridge (bridge D) as a non-root bridge and let bridge D associate to bridge A (the root bridge).
 - Observe bridge D's LEDs and align the bridge D antenna with bridge A so that the RSSI signal level is maximized.
 - When the antennas are fully aligned, if the RSSI signal level is greater than **-54 dBm**, the bridge sites are very close. Reduce the output power on all bridges at both sites (bridges A, B, C, and D) to 12 dBm.
 - If you are still unable to reduce the RSSI signal level to **-54 dBm**, change the polarization of the link 2 bridges (bridges B and D). For example; change the antenna polarization from vertical to horizontal.
- Step 4** At Site 2, measure the isolation between bridge C and D by following these steps:
- Turn off bridge A for this measurement.

CISCO CONFIDENTIAL - First Draft

- b. Activate the link 2 bridge (bridge D) as a non-root bridge and the link1 bridge (bridge C) as a root bridge and let bridge D associate to bridge C.
- c. Observe bridge D's LEDs and verify that the RSSI signal level is **-54 dBm** or less. If the signal level exceeds **-54 dBm**, move the bridge farther away and repeat this step.
- d. Slowly rotate the antenna of bridge D a few degrees to the left and to the right and verify that the RSSI signal level does not spike above **-54 dBm**. If the signal peaks above **-54 dBm**, move the bridge farther away and repeat this step.

Step 5 After you verify the isolation of the second bridge link, you must properly set the root and non-root bridge settings for both links, align the link 2 bridge antennas, and verify proper link 2 operation.

Configuring the Bridge for the First Time

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

This chapter contains these sections:

- [Before You Start, page 5-2](#)
- [Obtaining and Assigning an IP Address, page 5-3](#)
- [Connecting to the Bridge Locally, page 5-3](#)
- [Assigning Basic Settings, page 5-4](#)
- [What To Do Next, page 5-9](#)
- [Using the IP Setup Utility, page 5-9](#)
- [Assigning an IP Address Using the CLI, page 5-13](#)
- [Using a Telnet Session to Access the CLI, page 5-13](#)

CISCO CONFIDENTIAL - First Draft

Before You Start

Before you install the bridge, make sure you are using a computer connected to the same network as the bridge, and obtain the following information:

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

Resetting the Bridge to Default Settings

If you need to start over during the initial setup process, follow these steps to reset the bridge to factory default settings using the power injector's Mode button:

-
- Step 1** Disconnect the power jack from the power injector.
 - Step 2** Press and hold the power injector's **MODE** button while you reconnect the power jack.
 - Step 3** Hold the **MODE** button until the Status LED turns amber (approximately 1 to 3 seconds) and wait until the bridge boots up (Status LED turns green). All bridge settings return to factory defaults.
-

You can also use the web-browser interface to reset the bridge to defaults. Follow these steps to return to default settings using the web-browser interface:

-
- Step 1** Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).
 - Step 2** Enter the bridge's IP address in the browser address line and press **Enter**. An Enter Network Password window appears.
 - Step 3** Enter your username in the User Name field. The default username is **Cisco**.
 - Step 4** Enter the bridge password in the Password field and press **Enter**. The default password is **Cisco**. The Summary Status page appears.
 - Step 5** Click **System Software** and the System Software screen appears.
 - Step 6** Click **System Configuration** and the System Configuration screen appears.
 - Step 7** Click **Default**.

CISCO CONFIDENTIAL - First Draft**Note**

If the bridge is configured with a static IP address, the IP address is not changed.

Obtaining and Assigning an IP Address

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

- Use default address 10.0.0.1 when you connect to the bridge locally. For detailed instructions, see the [“Connecting to the Bridge Locally” section on page 5-3](#).
- Use a DHCP server (if available) to automatically assign an IP address. You can find the DHCP-assigned IP address using one of the following methods:
 - Provide your organization's network administrator with your bridge's Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The bridge's MAC address is on label attached to the bottom of the bridge.
 - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. You can also use IPSU to assign an IP address to the bridge if it did not receive an IP address from the DHCP server. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, Me, NT, and XP.

You can download IPSU from the Software Center on Cisco.com. For additional information refer to the [“Obtaining and Installing IPSU” section on page 5-10](#).

Connecting to the Bridge Locally

If you need to configure the bridge locally (without connecting the bridge's power injector to a wired LAN), you can connect a PC to the power injector's Ethernet port using a Category 5 Ethernet cable. You can use a local connection to the Ethernet port much as you would use a serial port connection.

**Note**

You do not need a special crossover cable to connect your PC to the bridge's power injector; you can use either a straight-through cable or a crossover cable.

If the bridge is configured with default values and not connected to a DHCP server or cannot obtain an IP address, it defaults to IP address 10.0.0.1 and becomes a mini-DHCP server. In that capacity, the bridge provides up to twenty IP addresses between 10.0.0.11 and 10.0.0.30 to an Ethernet-capable PC connected to the power injector's Ethernet port.

The mini-DHCP server feature is disabled automatically when you assign a static IP address to the bridge.

**Caution**

When a bridge with default settings is connected on a wired LAN and does not receive an IP address from a DHCP server, the bridge provides an IP address to any DHCP requests it receives.

CISCO CONFIDENTIAL - First Draft

Follow these steps to connect to the bridge locally:

- Step 1** Make sure that the PC you intend to use is configured to obtain an IP address automatically, or manually assign it an IP address from 10.0.0.31 to 10.0.0.40. Connect your PC to the power injector using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.



Note When you connect your PC to the bridge's power injector or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering **ipconfig /release** and **ipconfig /renew** commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

- Step 2** Power up the power injector.
- Step 3** Follow the steps in the [“Assigning Basic Settings” section on page 5-4](#). If you make a mistake and need to start over, follow the steps in the [“Resetting the Bridge to Default Settings” section on page 5-2](#).
- Step 4** After configuring the bridge, remove the Ethernet cable from your PC and connect the power injector to your wired LAN.

Assigning Basic Settings

After you determine or assign the bridge's IP address, you can browse to the bridge's Express Setup page and perform an initial configuration. Follow these steps:

- Step 1** Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).
- Step 2** Enter the bridge's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Press **Tab** to bypass the Username field and advance to the Password field.

CISCO CONFIDENTIAL - First Draft

- Step 4** Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears. [Figure 5-1](#) shows the Summary Status page.

Figure 5-1 *Summary Status Page*

CISCO CONFIDENTIAL - First Draft

Step 5 Click **Express Setup**. The Express Setup screen appears. [Figure 5-2](#) shows the Express Setup page.

Figure 5-2 *Express Setup Page*

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

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



Note When DHCP is enabled, the IP Address, Subnet Mask, and Default Gateway fields indicate *Negotiated by DHCP*

- **Static IP**—The bridge uses a static IP address that you enter in the IP address field.

CISCO CONFIDENTIAL - First Draft

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

**Note**

If the bridge's IP address changes while you are configuring the bridge using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the bridge. If you lose your connection, reconnect to the bridge using its new IP address. Follow the steps in the [“Resetting the Bridge to Default Settings”](#) section on page 5-2 if you need to start over.

- **IP Subnet Mask**—Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. If DHCP is enabled, leave this field blank.
- **Default Gateway**—Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
- **SNMP Community**—If your network is using SNMP, enter the SNMP Community name provided by your network administrator and select the attributes of the SNMP data (also provided by your network administrator).
 - **Read-Only**—indicates the bridge allows only SNMP read accesses. Using this option, an SNMP user cannot change bridge configuration settings.
 - **Read-Write**—indicates the bridge allows SNMP read and write accesses. This setting allows an SNMP user to change the bridge configuration.
- **Radio Service Set ID (SSID)**—Enter the case-sensitive SSID (32 alphanumeric characters maximum) provided by your network administrator. The SSID is a unique identifier that remote bridges use to associate with your bridge.
- **Broadcast SSID in Beacon**—Use this setting to allow devices that do not specify an SSID to associate with the bridge.
 - **Yes**—This is the default setting; it allows a remote bridge that does not specify an SSID to associate with the bridge.
 - **No**—Remote bridges must specify an SSID to associate with the bridge. With No selected, the SSID used by the remote bridge must match exactly the bridge's SSID.
- **Role in Radio Network**—Click on the check box and button that describes the role of the bridge on your network.
 - **Install Mode**—Activates the bridge install and alignment mode. Specifies that the bridge automatically determines the network role. If the bridge is able to associate to another root bridge within 60 seconds, the bridge assumes a non-root bridge role. If the bridge is unable to associate with another root bridge within 60 seconds, the bridge assumes a root bridge role.
You can also pre-configure the bridge into root or non-root modes and avoid the 60 seconds automatic detection phase.
 - **Root**—Specifies that the bridge connects directly to the main Ethernet LAN network and accepts associations from other bridges.
 - **Non-root**—Specifies that the bridge connects to a remote LAN network and must associate with the root bridge using the wireless interface.

**Note**

When initially powered up, the bridge is configured in Install mode with automatic detection activated.

CISCO CONFIDENTIAL - First Draft

- **Optimize Radio Network for**—Use this setting to select either preconfigured settings for the bridge radio or customized settings for the bridge radio.
 - **Throughput**—Maximizes the data volume handled by the bridge but might reduce its range.
 - **Range**—Maximizes the bridge's range but might reduce throughput.
 - **Default**—The bridge retains default radio settings that are designed to provide good range and throughput for most bridges.
 - **Custom**—The bridge uses settings you enter on the Network Interfaces: Radio-802.11b Settings page. Clicking **Custom** takes you to the Network Interfaces: Radio-802.11b Settings page.

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

**Note**

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

Default Settings on the Express Setup Page

Table 5-1 lists the default settings for the settings on the Express Setup page.

Table 5-1 Default Settings on the Express Setup Page

Setting	Default
System Name	Bridge
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP (default setting); if DHCP is disabled, the default setting is 10.0.0.1
IP Subnet Mask	Assigned by DHCP (default setting); if DHCP is disabled, the default setting is 255.255.255.224
Default Gateway	Assigned by DHCP (default setting); if DHCP is disabled, the default setting is 0.0.0.0
SNMP	defaultCommunity Read Only
SSID	autoinstall ¹ or tsunami ²
Broadcast SSID in Beacon	Yes
Role in Radio Network	Install
Optimize Radio Network for	Throughput

1. During Install Mode, the SSID is *autoinstall*.

2. After a static IP address is assigned or the role is changed from Install, the SSID is *tsunami*.

CISCO CONFIDENTIAL - First Draft

What To Do Next

After your bridge has basic settings, you need to complete your bridge's configuration. You might need to adjust the output power level and other network and security settings.

Output Power Level

Your bridge's output power level might require adjustment under the following conditions:

- The bridge's output power level must be reduced when using the 15-dBi sector or the 21-dBi dish antenna (refer to [“Maximum Power Levels and Antenna Gains” section on page D-3](#)).
- When bridges are installed less than 328 ft (100 m) apart, you should reduce their output power to avoid overloading the bridge's receivers.
- Your regulatory domain may limit the equivalent isotropic radiated power (EIRP) from the bridge's antenna (refer to [“Maximum Power Levels and Antenna Gains” section on page D-3](#)).

To configure your bridge's output power level, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges*.

Protecting Your Wireless LAN

To prevent unauthorized access to your network, you must configure security settings. Because the bridge is a radio device, the bridge communicates beyond the physical boundaries of your building. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges* to configure security features to protect your network from intruders:

- Unique SSIDs that are not broadcast in the bridge beacon
- WEP and additional WEP features, such as TKIP and broadcast key rotation
- Dynamic WEP and EAP authentication

Using the IP Setup Utility

IPSU enables you to find the bridge's IP address when it has been assigned by a DHCP server. You can also use IPSU to set the bridge's IP address and SSID if they have not been changed from the default settings.

**Note**

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

The sections below explain how to install the utility, how to use it to find the bridge's IP address, and how to use it to set the IP address and the SSID.

CISCO CONFIDENTIAL - First Draft

Obtaining and Installing IPSU

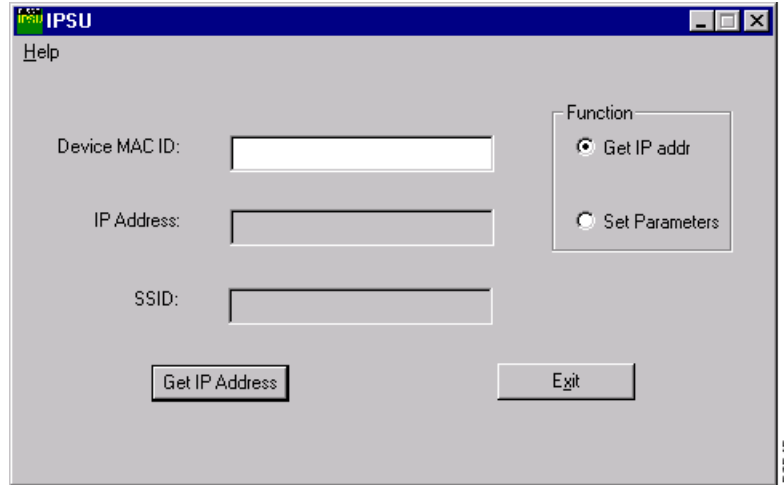
IPSU is available on the Cisco web site. Follow these steps to obtain and install IPSU:

-
- Step 1** Use your web browser to go to the Cisco Software Center at the following URL:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
 - Step 2** Select **Option #1: Aironet Wireless Software Selector**.
 - Step 3** For the Product Type, select **Wireless Bridge** and click **Submit**.
 - Step 4** Select **1400 Series** for the model number and click **Submit**.
 - Step 5** Select **Current Release (Recommended)** and click **Submit**.
 - Step 6** Under Utilities, select **IPSUvxxxxxx.exe**.
 - Step 7** On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply. Click **Submit**.
 - Step 8** Read and accept the terms and conditions of the Software License Agreement.
 - Step 9** Select the IPSU file again to download it.
 - Step 10** Save the file to a temporary directory on your hard drive and then exit the Internet browser.
 - Step 11** Double-click **IPSUvxxxxxx.exe** in the temporary directory to expand the file.
 - Step 12** Double-click **Setup.exe** and follow the steps provided by the installation wizard to install IPSU.
The IPSU icon appears on your computer desktop.
-

Using IPSU to Find the Bridge's IP Address

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

-
- Step 1** Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see [Figure 5-3](#)).

CISCO CONFIDENTIAL - First Draft**Figure 5-3 IPSU Get IP Address Screen**

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

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

000164xxxxxx



Note The MAC address field is not case sensitive.

Step 4 Click **Get IP Address**.

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

If IPSU reports that the IP address is 10.0.0.1, the default IP address, the bridge did not receive a DHCP-assigned IP address. To change the bridge IP address from the default value using IPSU, refer to the [“Using IPSU to Set the Bridge's IP Address and SSID”](#) section on page 5-12.

CISCO CONFIDENTIAL - First Draft

Using IPSU to Set the Bridge's IP Address and SSID

You can use IPSU to change the default IP address (10.0.0.1) of the bridge. You can also set the bridge's SSID at the same time.

**Note**

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

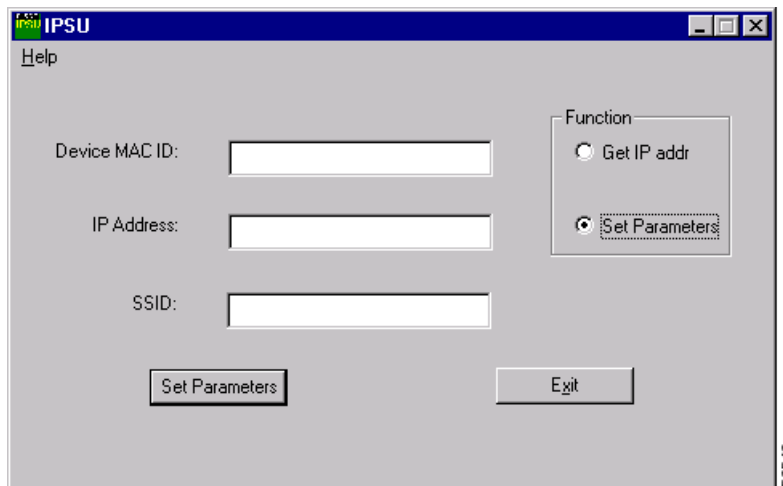
**Note**

IPSU can change the bridge's IP address and SSID only from their default settings. After the IP address and SSID are changed, IPSU cannot change them again.

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

- Step 1** Double-click the **IPSU** icon on your computer desktop to start the utility.
- Step 2** Click the **Set Parameters** radio button in the Function box (see [Figure 5-4](#)).

Figure 5-4 IPSU Set Parameters Screen



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

004096xxxxxx

**Note**

The MAC address field is not case sensitive.

- Step 4** Enter the IP address you want to assign to the bridge in the IP Address field.
- Step 5** Enter the SSID you want to assign to the bridge in the SSID field.

**Note**

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

CISCO CONFIDENTIAL - First Draft

- Step 6** Click **Set Parameters** to change the bridge's IP address and SSID settings.
- Step 7** Click **Exit** to exit IPSU.

Assigning an IP Address Using the CLI

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

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface bvi1	Enter interface configuration mode for the BVI.
Step 3	ip address <i>address</i> <i>mask</i>	Assign an IP address and address mask to the BVI. This step automatically saves the running configuration to the startup configuration. Note You lose your connection to the bridge when you assign a new IP address to the BVI. If you need to continue configuring the bridge, use the new IP address to open another Telnet session to the bridge.

Using a Telnet Session to Access the CLI

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

- Step 1** Select **Start > Programs > Accessories > Telnet**.
If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.
- Step 2** When the Telnet window appears, click **Connect** and select **Remote System**.
-  **Note** In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the bridge's IP address.
- Step 3** In the Host Name field, type the bridge's IP address and click **Connect**.

CISCO CONFIDENTIAL - First Draft

Using the Web-Browser Interface

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

- [Using the Web-Browser Interface for the First Time, page 6-2](#)
- [Using the Management Pages in the Web-Browser Interface, page 6-2](#)
- [Using Online Help, page 6-5](#)

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

CISCO CONFIDENTIAL - First Draft

Using the Web-Browser Interface for the First Time

Use the access point's IP address to browse to the management system. See the [“Obtaining and Assigning an IP Address”](#) section on page 5-3 for instructions on assigning an IP address to the access point.

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

-
- | | |
|---------------|--|
| Step 1 | Start the browser. |
| Step 2 | Enter the access point's IP address in the browser Location field (Netscape Communicator) or Address field (Internet Explorer) and press Enter . The Summary Status page appears. |
-

Using the Management Pages in the Web-Browser Interface

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

**Note**

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

CISCO CONFIDENTIAL - First Draft

Figure 6-1 shows the web-browser interface home page.

Figure 6-1 Web-Browser Interface Home Page

Using Action Buttons

Table 6-1 lists the page links and buttons that appear on most management pages.

Table 6-1 Common Buttons on Management Pages

Button/Link	Description
Navigation Links	
Home	Displays access point status page with information on the number of radio devices associated to the access point, the status of the Ethernet and radio interfaces, and a list of recent access point activity.
Express Setup	Displays the Express Setup page that includes basic settings such as system name, IP address, and SSID.
Network Map	Displays a list of infrastructure devices on your wireless LAN.

CISCO CONFIDENTIAL - First Draft**Table 6-1 Common Buttons on Management Pages (continued)**

Button/Link	Description
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.
Network Interfaces	Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.
Security	Displays a summary of security settings and provides links to security configuration pages.
Services	Displays status for several access point features and links to configuration pages for Telnet/SSH, CDP, Domain Name Server, Filters, Proxy Mobile IP, QoS, SNMP, SNTTP, and VLANs.
System Software	Displays the version number of the firmware that the access point is running and provides links to configuration pages for upgrading and managing firmware.
Event Log	Displays the access point event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.
Configuration Action Buttons	
Apply	Saves changes made on the page and remains on the page.
Refresh	Updates status information or statistics displayed on a page.
Cancel	Discards changes to the page and remains on the page.
Back	Discards any changes made to the page and returns to the previous page.

CISCO CONFIDENTIAL - First Draft

Character Restrictions in Entry Fields

Because the 1100 series access point uses Cisco IOS software, there are certain characters that you cannot use in the entry fields on the web-browser interface. [Table 6-2](#) lists the prohibited characters and the fields in which you cannot use them.

Table 6-2 *Prohibited Characters for Web-Browser Interface Entry Fields*

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

Using Online Help

Click the help icon at the top of any page in the web-browser interface to display online help. [Figure 6-2](#) shows the print and help icons.

Figure 6-2 *Print and Help Icons*



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

CISCO CONFIDENTIAL - First Draft

Using the Command-Line Interface

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

- [IOS Command Modes, page 7-2](#)
- [Getting Help, page 7-3](#)
- [Abbreviating Commands, page 7-3](#)
- [Using no and default Forms of Commands, page 7-3](#)
- [Understanding CLI Messages, page 7-4](#)
- [Using Command History, page 7-4](#)
- [Using Editing Features, page 7-6](#)
- [Searching and Filtering Output of show and more Commands, page 7-8](#)
- [Accessing the CLI, page 7-9](#)

CISCO CONFIDENTIAL - First Draft

IOS Command Modes

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

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

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

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

[Table 7-1](#) describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *ap*.

Table 7-1 Command Mode Summary

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

CISCO CONFIDENTIAL - First Draft

Getting Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in [Table 7-2](#).

Table 7-2 Help Summary

Command	Purpose
help	Obtain a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Obtain a list of commands that begin with a particular character string. For example: ap# di? dir disable disconnect
<i>abbreviated-command-entry<Tab></i>	Complete a partial command name. For example: ap# sh conf<tab> ap# show configuration
?	List all commands available for a particular command mode. For example: ap> ?
<i>command ?</i>	List the associated keywords for a command. For example: ap> show ?
<i>command keyword ?</i>	List the associated arguments for a keyword. For example: ap(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet

Abbreviating Commands

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

```
ap# show conf
```

Using no and default Forms of Commands

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

CISCO CONFIDENTIAL - First Draft

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

Understanding CLI Messages

Table 7-3 lists some error messages that you might encounter while using the CLI to configure your access point.

Table 7-3 Common CLI Error Messages

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

Using Command History

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

- [Changing the Command History Buffer Size, page 7-5](#)
- [Recalling Commands, page 7-5](#)
- [Disabling the Command History Feature, page 7-5](#)

CISCO CONFIDENTIAL - First Draft

Changing the Command History Buffer Size

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

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

The range is from 0 to 256.

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

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

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in [Table 7-4](#):

Table 7-4 Recalling Commands

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

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

Disabling the Command History Feature

The command history feature is automatically enabled.

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

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

Using Editing Features

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

- [Enabling and Disabling Editing Features, page 7-6](#)
- [Editing Commands through Keystrokes, page 7-6](#)
- [Editing Command Lines that Wrap, page 7-7](#)

Enabling and Disabling Editing Features

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

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

```
ap# terminal editing
```

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

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

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

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

Editing Commands through Keystrokes

[Table 7-5](#) shows the keystrokes that you need to edit command lines.

Table 7-5 *Editing Commands through Keystrokes*

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

CISCO CONFIDENTIAL - First Draft**Table 7-5** *Editing Commands through Keystrokes (continued)*

Capability	Keystroke ¹	Purpose
Delete entries if you make a mistake or change your mind.	Delete or Backspace	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or Ctrl-X	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	Esc C	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Ctrl-V or Esc Q	
Scroll down a line or screen on displays that are longer than the terminal screen can display. Note The <code>More</code> prompt appears for output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the <code>More</code> prompt.	Return	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the access point suddenly sends a message to your screen.	Ctrl-L or Ctrl-R	Redisplay the current command line.

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

Editing Command Lines that Wrap

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

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


Note

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

CISCO CONFIDENTIAL - First Draft

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

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

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

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

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

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the [“Editing Commands through Keystrokes”](#) section on page 7-6.

Searching and Filtering Output of show and more Commands

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

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

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

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

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

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

CISCO CONFIDENTIAL - First Draft

Accessing the CLI

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

Opening the CLI with Telnet

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

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

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

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



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

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

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

Opening the CLI with Secure Shell

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

<http://www.ssh.com/>

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

CISCO CONFIDENTIAL - First Draft

Troubleshooting

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

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

Sections in this chapter include:

- [Checking the Bridge LEDs, page 8-2](#)
- [Power Injector, page 8-4](#)
- [Checking Basic Configuration Settings, page 8-5](#)
- [Antenna Alignment, page 8-5](#)
- [Resetting to the Default Configuration - TBD, page 8-6](#)
- [Reloading the Bridge Image - TBD, page 8-7](#)

Checking the Bridge LEDs

If your bridge is not associating with the remote bridge, check the four LEDs on the back panel. You can use them to quickly assess the unit’s status. For information on using the LEDs during the installation and alignment of the bridge antenna, refer to the “Bridge LEDs” section on page 3-3.

Figure 8-1 shows the bridge LEDs.

Figure 8-1 Bridge LEDs



1	Radio LED	3	Ethernet LED
2	Status LED	4	Install LED

Bridge Normal Mode LED Indications

During bridge operation the LEDs provide status information as shown in Table 8-1.

Table 8-1 Bridge Normal Mode LED Indications

Ethernet LED	Status LED	Radio LED	Meaning
Off	—	—	Ethernet link is down or disabled.
Blinking green	—	—	Transmitting and receiving Ethernet packets.
Blinking amber	—	—	Transmitting and receiving Ethernet errors.
amber	—	—	Firmware error—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.

CISCO CONFIDENTIAL - First Draft**Table 8-1 Bridge Normal Mode LED Indications (continued)**

Ethernet LED	Status LED	Radio LED	Meaning
—	Blinking green	—	Root mode—no remote bridges are associated. Non-root mode—not associated to the root bridge. If all bridges are powered up, this could be caused by incorrect SSID and security settings or improper antenna alignment. You should check the SSID and security settings of all bridges and verify antenna alignment. If the problem continues, contact technical support for assistance.
—	Green	—	Root mode—associated to at least one remote bridge. Non-root mode—associated to the root bridge. This is normal operation.
—	Blinking amber	—	General warning—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	Amber	—	Loading firmware.
Red	Amber	Red	Loading Firmware error—disconnect and reconnect the power injector power. If the problem continues, contact technical support for assistance.
—	—	Off	Normal operation.
—	—	Blinking green	Transmitting and receiving radio packets—normal operation.
—	—	Blinking amber	Maximum retries or buffer full occurred on the radio interface—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	—	Amber	Radio firmware error—disconnect and reconnect power injector power. If the problem continues, contact technical support for assistance.

The bridge uses a blinking code to identify various error conditions. The code sequence uses a two-digit diagnostic code that starts with a long pause to delimit the code, followed by the LED flashing red to count out the first digit, then a short pause, followed by the LED flashing red to count out the second digit.

CISCO CONFIDENTIAL - First Draft

The bridge LED blinking error codes are described in [Table 8-2](#).

Table 8-2 Bridge LED Blinking Error Codes

LED	Blinking Codes		Description
	First Digit	Second Digit	
Ethernet	2	1	Ethernet cable problem—verify that the cable is properly connected and not defective. This error might also indicate a problem with the Ethernet link. If the cable is connected properly and not defective, contact technical support for assistance.
Radio	1	2	Radio not detected—contact technical support for assistance.
	1	3	Radio not ready—contact technical support for assistance.
	1	4	Radio did not start—contact technical support for assistance.
	1	5	Radio failure—contact technical support for assistance.
	1	6	Radio did not flash its firmware—contact technical support for assistance.

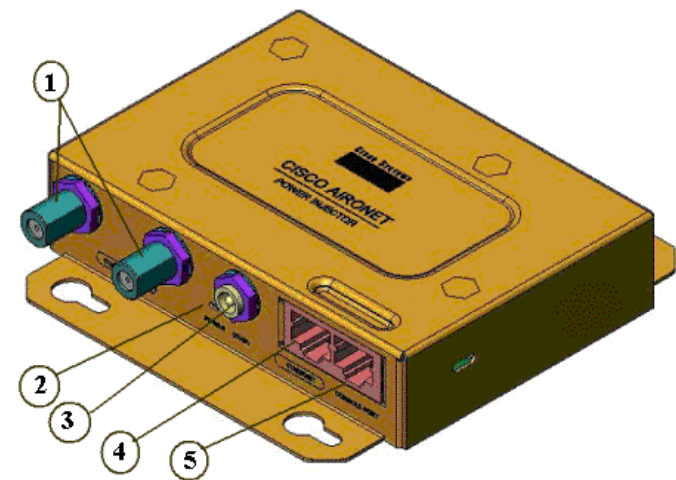
Power Injector

When the power injector is powered up, it sends a constant discovery tone on the dual-coax cables to the bridge. When the bridge is connected to the dual-coax cables, it returns the discovery tone to the power injector. When the power injector detects the returned discovery tone, it applies +48 VDC to the dual-coax cables to the bridge.

When power is applied to the bridge, the bridge activates the bootloader and begins the POST operations. The bridge begins to load the IOS image when the Post operations are successfully completed. Upon successfully loading the IOS image, the bridge initializes and tests the radio.

The power injector LED is shown in [Figure 8-2](#).

Figure 8-2 Power Injector



CISCO CONFIDENTIAL - First Draft

1	Dual-Coax Ethernet Ports	4	RJ-45 Ethernet Connector
2	Power LED	5	RJ-45 Serial Console Port
3	Power Jack (12 to 48 VDC)		

Checking Power

You can verify the availability of power to the bridge by checking the power injector LED (see [Figure 8-2](#)):

- Power LED
 - Green color indicates 48 VDC is available (see [Figure 8-2](#)).
 - Off indicates 48 VDC is not available—verify that the power module is connected to the power injector and to an AC receptacle and that AC power is available.

Checking Basic Configuration Settings

Mismatched basic settings are the most common causes of lost wireless connectivity. If the bridge does not associate with a remote bridge, check the following areas.

SSID

To associate, all bridges must use the same SSID. The bridge installation mode SSID is *autoinstall* and the normal mode default SSID is *tsunami*. You should verify that the SSID value shown on the Express Setup page is the same for all bridges. You should also verify that the bridges are configured for the proper network role; only one bridge can be configured as the root bridge.

Security Settings

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

If a non-root bridge is unable to authenticate to your root bridge, verify that the security settings are the same as your bridge settings. For additional information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges*.

Antenna Alignment

If your non-root bridges are unable to associate to your root bridge, you should verify the basic configuration settings on all bridges before attempting to verify bridge antenna alignment (refer to [“Configuring the Bridge for the First Time”](#) section on page 5-1). If your basic configuration settings are correct, you can verify antenna alignment by using the Install mode RSSI LED indications. For additional information, refer to the [“Aligning the Antenna Using RSSI LED Indications”](#) section on page 3-5.

CISCO CONFIDENTIAL - First Draft

For detailed alignment instructions, refer to the *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions* that shipped with your bridge.

**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Resetting to the Default Configuration - TBD

If you forget the password that allows you to configure the bridge, you may need to completely reset the configuration. You can use the serial console port on the power injector or the web-browser interface.

**Note**

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

Using the Serial Console Port - TBD

Follow these steps to delete the current configuration and return all bridge settings to factory defaults using the serial console port:

Step 1**Step 2**

Step 3 After the bridge reboots, you must reconfigure the bridge by using the Web browser interface, the Telnet interface, or IOS commands.

**Note**

The bridge is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the bridge's new IP address, refer to the [“Using the IP Setup Utility”](#) section on page 5-9.

Using the Web Browser Interface - TBD

Follow the steps below to delete the current configuration and return all bridge settings to the factory defaults using the web browser interface.

Step 1 Open your Internet browser.

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

Step 3 Enter your username (default Cisco) in the User Name field.

CISCO CONFIDENTIAL - First Draft

- Step 4** Enter the bridge password (default Cisco) in the Password field and press **Enter**. The Summary Status page appears.
- Step 5** Click **System Software** and the System Software screen appears.
- Step 6** Click **System Configuration** and the System Configuration screen appears.
- Step 7** Click **Default**.



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

- Step 8** After the bridge reboots, you must reconfigure the bridge by using the Web browser interface, the Telnet interface, or IOS commands (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges*).

Reloading the Bridge Image - TBD

If your bridge has a firmware failure, you must reload the complete bridge image file using the Web browser interface or by using the serial console port. You can use the browser interface if the bridge firmware is still fully operational and you want to upgrade the firmware image. However, you can use the serial console port when the bridge has a corrupt firmware image.

Using the Serial Console Port - TBD

You can use the serial console port on the bridge to reload the bridge image file from an active Trivial File Transfer Protocol (TFTP) server on a PC connected directly to the power injector Ethernet port.



Note If your bridge experiences a firmware failure or a corrupt firmware image, indicated by three red LEDs, you must reload the image from a directly connected PC with a TFTP server.



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

Follow the steps below to reload the bridge image file:

- Step 1** The PC you intend to use must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.
- Step 2** Make sure the PC contains the bridge image file (*c1310-k9w7-tar.122-15.JA.tar*) in the TFTP server folder and the TFTP server is activated. For additional information, refer to the [“Obtaining the Bridge Image File”](#) and [“Obtaining the TFTP Server Software”](#) sections.
- Step 3** Connect the PC to the bridge using a Category 5 Ethernet cable.
- Step 4** TBD
- Step 5** Wait until the bridge reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

CISCO CONFIDENTIAL - First Draft

- Step 6** After the bridge reboots, you must reconfigure the bridge by using the Web interface, the Telnet interface, or IOS commands (refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges*).

**Note**

The bridge is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the bridge's new IP address, refer to the [“Using the IP Setup Utility” section on page 5-9](#).

Web Browser Interface - TBD

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

**Note**

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

Browser HTTP Interface

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

-
- Step 1** Open your Internet browser.
- Step 2** Enter the bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Enter your username in the User Name field.
- Step 4** Enter the bridge password in the Password field and press **Enter**. The Summary Status page appears.
- Step 5** Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.
- Step 6** Click **Browse** to locate the image file on your PC.
- Step 7** Click **Upload**.

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

Browser TFTP Interface

The TFTP interface enables you to use a TFTP server on a network device to load the bridge image file. Follow the instructions below to use a TFTP server:

-
- Step 1** Open your Internet browser.
- Step 2** Enter the bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Enter your username in the User Name field.

CISCO CONFIDENTIAL - First Draft

- Step 4** Enter the bridge password in the Password field and press **Enter**. The Summary Status page appears.
 - Step 5** Click **System Software** and then click **Software Upgrade**. The HTTP Upgrade screen appears.
 - Step 6** Click **TFTP Upgrade**.
 - Step 7** Enter the IP address for the TFTP server in the TFTP Server field.
 - Step 8** Enter the filename for the bridge image file (*c1310-k9w7-tar.122-15.JA.tar*) in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is in the TFTP root directory, enter only the filename.
 - Step 9** Click **Upload**.
- For additional information click the **Help** icon on the Software Upgrade screen.
-

Obtaining the Bridge Image File

You can obtain the bridge image file from the Cisco.com software center by following these steps:

-
- Step 1** Use your web browser to go to the Cisco Software Center at the following URL:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
 - Step 2** Select **Option #1: Aironet Wireless Software Selector**.
 - Step 3** For the Product Type, select **Wireless Bridge** and click **Submit**.
 - Step 4** Select **1300 Series** for the model number and click **Submit**.
 - Step 5** Select **Current Release (Recommended)** and click **Submit**.
 - Step 6** Select **c1310-k9w7-tar.122-15.JA.tar**, which is the bridge image file.
 - Step 7** On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply. Click **Submit**.
 - Step 8** Read and accept the terms and conditions of the Software License Agreement.
 - Step 9** Select the bridge image file again to download it.
 - Step 10** Save the file to a directory on your hard drive and then exit the Internet browser.
-

Obtaining the TFTP Server Software

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

<http://tftpd32.jounin.net>

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

CISCO CONFIDENTIAL - First Draft

Translated Safety Warnings

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

- [Statement 84—Warning Definition, page A-2](#)
- [Statement 332—Antenna Installation Warning, page A-4](#)
- [Statement 1001—Work During Lightning Activity, page A-5](#)
- [Statement 1004—Installation Instructions, page A-6](#)
- [Statement 1005—Circuit Breaker, page A-7](#)
- [Statement 1024—Ground Conductor, page A-8](#)
- [Statement 1040—Product Disposal, page A-9](#)
- [Statement 1052—Installing and Grounding the Antenna, page A-11](#)

CISCO CONFIDENTIAL - First Draft**Statement 84—Warning Definition****Warning**

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

Waarschuwing

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

Varoitus

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

Attention

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

Warnung

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

Avvertenza

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

Advarsel

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

CISCO CONFIDENTIAL - First Draft

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].)

Statement 245B—Explosive Device Proximity Warning**Warning**

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

Statement 245B

Waarschuwing	Gebruik dit draadloos netwerkkapparaat alleen in de buurt van onbeschermd ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.
Varoitus	Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.
Attention	Ne jamais utiliser un équipement de réseau sans fil à proximité d'un détonateur non blindé ou dans un lieu présentant des risques d'explosion, sauf si l'équipement a été modifié à cet effet.
Warnung	Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.
Avvertenza	Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.
Advarsel	Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.

CISCO CONFIDENTIAL - First Draft

Aviso	Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.
¡Advertencia!	No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.
Varning!	Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.

Statement 332—Antenna Installation Warning

**Warning**

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

Waarschuwing

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

Varoitus

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

Attention

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

Warnung

Um die in den FCC-Richtlinien festgelegten Expositionshöchstgrenzen für Radiofrequenzen (RF) nicht zu überschreiten, sollten antennen mindestens 20 cm (7,9 Zoll) vom Körper aller Person entfernt aufgestellt werden.

Avvertenza

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

Advarsel

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

Aviso

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

¡Advertencia!

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

Varning!

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

CISCO CONFIDENTIAL - First Draft**Statement 1001—Work During Lightning Activity****Warning**

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

Waarschuwing

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

Varoitus

Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.

Attention

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

Warnung

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

Avvertenza

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

Advarsel

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

Aviso

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

¡Advertencia!

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

Varning!

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

Figyelem

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

Предупреждение

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

警告

请勿在发生雷电时操作系统，也不要在此期间连接或断开电缆。

警告

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

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

CISCO CONFIDENTIAL - First Draft**Statement 1005—Circuit Breaker****Warning**

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:
(120 VAC, 15A U.S. (240 VAC, 10A international) Statement 1005

Waarschuwing

Dit product is afhankelijk van de installatie van het gebouw voor beveiliging tegen kortsluiting (overstroom). Controleer of de beschermingsinrichting niet meer dan:
(120 VAC, 15A U.S. (240 VAC, 10A international) is.

Varoitus

Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että suojalaitteen mitoitus ei ole yli:
(120 VAC, 15A U.S. (240 VAC, 10A international)

Attention

Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifiez que le courant nominal du dispositif de protection n'est pas supérieur à :
(120 VAC, 15A U.S. (240 VAC, 10A international)

Warnung

Dieses Produkt ist darauf angewiesen, dass im Gebäude ein Kurzschluss- bzw. Überstromschutz installiert ist. Stellen Sie sicher, dass der Nennwert der Schutzvorrichtung nicht mehr als:
(120 VAC, 15A U.S. (240 VAC, 10A international) beträgt.

Avvertenza

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia un rating superiore a:
(120 VAC, 15A U.S. (240 VAC, 10A international)

Advarsel

Dette produktet er avhengig av bygningens installasjoner av kortslutnings (overstrøm)-beskyttelse. Påse at verneenheter ikke er merket høyere enn:
(120 VAC, 15A U.S. (240 VAC, 10A international)

Aviso

Este produto depende das instalações existentes para proteção contra curto-circuito (sobrecarga). Assegure-se de que o fusível ou disjuntor não seja superior a:
(120 VAC, 15A U.S. (240 VAC, 10A international)

¡Advertencia!

Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) del edificio. Asegúrese de que el dispositivo de protección no sea superior a:
(120 VAC, 15A U.S. (240 VAC, 10A international)

Varning!

Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att skyddsanordningen inte har högre märkvärde än:
(120 VAC, 15A U.S. (240 VAC, 10A international)

Figyelem

A termék védelmi rendszerének része az épület kábelezésébe épített rövidzárlat (túláram) elleni védelem is. Gondoskodjon róla, hogy a készüléket védő eszköz legfeljebb a következő áramerősségre legyen méretezve:
(120 VAC, 15A U.S. (240 VAC, 10A international)

CISCO CONFIDENTIAL - First Draft

Предупреждение	Защита устройства от короткого замыкания (перегрузки) осуществляется с помощью оборудования, являющегося частью электропроводки здания. Убедитесь, что номинал защитного устройства не превышает: (120 VAC, 15A U.S. (240 VAC, 10A international))
警告	此产品的短路（过载电流）保护由建筑物的供电系统提供。确保短路保护设备的额定电流不大于： (120 VAC, 15A U.S. (240 VAC, 10A international))
警告	この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。保護装置の定格が以下の値を超えないことを確認してください。 (120 VAC, 15A U.S. (240 VAC, 10A international))

Statement 1024—Ground Conductor**Warning**

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

Waarschuwing

Deze apparatuur dient geaard te zijn. De aardingsleiding mag nooit buiten werking worden gesteld en de apparatuur mag nooit bediend worden zonder dat er een op de juiste wijze geïnstalleerde aardingsleiding aanwezig is. Neem contact op met de bevoegde instantie voor elektrische inspecties of met een elektricien als u er niet zeker van bent dat er voor passende aarding gezorgd is.

Varoitus

Laitteiden on oltava maadoitettuja. Älä koskaan ohita maajohdinta tai käytä laitteita ilman oikein asennettua maajohdinta. Ota yhteys sähkötarkastusviranomaiseen tai sähköasentajaan, jos olet epävarma maadoituksen sopivuudesta.

Attention

Cet équipement doit être mis à la masse. Ne jamais rendre inopérant le conducteur de masse ni utiliser l'équipement sans un conducteur de masse adéquatement installé. En cas de doute sur la mise à la masse appropriée disponible, s'adresser à l'organisme responsable de la sécurité électrique ou à un électricien.

Warnung

Dieses Gerät muss geerdet sein. Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an die zuständige Inspektionsbehörde oder einen Elektriker.

Avvertenza

Questa apparecchiatura deve essere dotata di messa a terra. Non escludere mai il conduttore di protezione né usare l'apparecchiatura in assenza di un conduttore di protezione installato in modo corretto. Se non si è certi della disponibilità di un adeguato collegamento di messa a terra, richiedere un controllo elettrico presso le autorità competenti o rivolgersi a un elettricista.

CISCO CONFIDENTIAL - First Draft

Advarsel	Dette utstyret må jordes. Omgå aldri jordingslederen og bruk aldri utstyret uten riktig montert jordingsleder. Ta kontakt med fagfolk innen elektrisk inspeksjon eller med en elektriker hvis du er usikker på om det finnes velegnet jordning.
Aviso	Este equipamento deve ser aterrado. Nunca anule o fio terra nem opere o equipamento sem um aterramento adequadamente instalado. Em caso de dúvida com relação ao sistema de aterramento disponível, entre em contato com os serviços locais de inspeção elétrica ou um eletricista qualificado.
¡Advertencia!	Este equipo debe estar conectado a tierra. No inhabilite el conductor de tierra ni haga funcionar el equipo si no hay un conductor de tierra instalado correctamente. Póngase en contacto con la autoridad correspondiente de inspección eléctrica o con un electricista si no está seguro de que haya una conexión a tierra adecuada.
Varning!	Denna utrustning måste jordas. Koppla aldrig från jordledningen och använd aldrig utrustningen utan en på lämpligt sätt installerad jordledning. Om det föreligger osäkerhet huruvida lämplig jordning finns skall elektrisk besiktningsauktoritet eller elektriker kontaktas.
Figyelem	A berendezés csak megfelelő védőföldeléssel működtethető. Ne iktassa ki a földelés csatlakozóját, és ne üzemeltesse a berendezést szabályosan felszerelt földelő vezeték nélkül! Ha nem biztos benne, hogy megfelelő földelés áll rendelkezésre, forduljon a helyi elektromos hatóságokhoz vagy egy villanyszerelőhöz.
Предупреждение	Данное устройство должно быть заземлено. Никогда не отключайте провод заземления и не пользуйтесь оборудованием при отсутствии правильно подключенного провода заземления. За сведениями об имеющихся возможностях заземления обратитесь к соответствующим контролирующим организациям по энергоснабжению или к инженеру-электрику.
警告	此设备必须接地。切勿使接地导体失效，或者在没有正确安装接地导体的情况下操作该设备。如果您不能肯定接地导体是否正常发挥作用，请咨询有关电路检测方面的权威人士或电工。
警告	この装置はアース接続する必要があります。アース導体を破損しないよう注意し、アース導体を正しく取り付けないまま装置を稼働させないでください。アース接続が適正であるかどうか分からない場合には、電気検査機関または電気技術者に相談してください。

Statement 1040—Product Disposal

**Warning**

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

Waarschuwing

Het uiteindelijke wegruimen van dit product dient te geschieden in overeenstemming met alle nationale wetten en reglementen.

CISCO CONFIDENTIAL - First Draft

Varoitus	Tämä tuote on hävitettävä kansallisten lakien ja määräysten mukaisesti.
Attention	La mise au rebut ou le recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environnement. Renseignez-vous auprès de l'organisme compétent.
Warnung	Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.
Avvertenza	Lo smaltimento di questo prodotto deve essere eseguito secondo le leggi e regolazioni locali.
Advarsel	Endelig kassering av dette produktet skal være i henhold til alle relevante nasjonale lover og bestemmelser.
Aviso	Deitar fora este produto em conformidade com todas as leis e regulamentos nacionais.
¡Advertencia!	Al deshacerse por completo de este producto debe seguir todas las leyes y reglamentos nacionales.
Varning!	Vid deponering hanteras produkten enligt gällande lagar och bestämmelser.
Figyelem	A készülék végső elhelyezéséről az adott országban érvényes törvények és előírások szerint kell intézkedni.
Предупреждение	Окончательная установка данного изделия должна выполняться в соответствии со всеми региональными и местными правилами и нормами.
警告	本产品的废弃处理应根据所有国家的法律和规章进行。
警告	この製品を廃棄処分する際は、各国の法律および規制に従って取り扱ってください。
주의	해당 국가의 관련 법규 및 규정에 따라 이 장치를 폐기해야 합니다.
Aviso	O descarte definitivo deste produto deve estar de acordo com todas as leis e regulamentações nacionais.
Advarsel	Endelig bortskaffelse af dette produkt skal ske i henhold til gældende love og regler.
تحذير	عند التخلص من المنتج يجب اتباع القوانين والتشريعات المحلية.
Upozorenje	Zbrinjavanje ovoga proizvoda u otpad treba provesti u skladu s važećim zakonima i odredbama.
Upozornění	Upozornění: Likvidace tohoto výrobku musí být provedena podle platných zákonů a předpisů.
Προειδοποίηση	Η τελική απόρριψη αυτού του προϊόντος πρέπει να γίνεται σύμφωνα με όλους τους εθνικούς νόμους και κανονισμούς.

CISCO CONFIDENTIAL - First Draft

אזהרה	סילוק סופי של מוצר זה חייב להיות בהתאם להנחיות ולחוקי המדינה.
Opomena	Крајното фрлање на овој производ треба да се изврши во согласност со сите национални закони и прописи.
Ostrzeżenie	Ostateczna likwidacja tego urządzenia po jego wycofaniu z eksploatacji powinna odbywać się zgodnie z przepisami krajowymi.
Upozornenie	Upozornenie Likvidácia tohto výrobku musí byť vykonaná podľa platných zákonov a predpisov.

Statement 1052—Installing and Grounding the Antenna**Warning**

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, because they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (for example, U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54). Statement 1052

Waarschuwing

Zorg dat antenne niet in de buurt wordt geplaatst van langs het plafond lopende stroomkabels of andere voorzieningen voor licht of elektriciteit of op een plaats waar contact met dergelijke stroomvoorzieningen mogelijk is. Wees bij het installeren van de antenne voorzichtig dat u niet in contact komt met dergelijke stroomvoorzieningen aangezien dit kan leiden tot ernstig lichamelijk of dodelijk letsel. Voor het juist installeren en aarden van de antenne, dient u de nationale en plaatselijke verordeningen te raadplegen (bijv. in de VS NFPA 70, National Electrical Code, Artikel 810, in Canada: Canadian Electrical Code, Sectie 54).

Varoitus

Älä sijoita antennia lähelle voimajohtoja, muita sähkövalo- tai virtapiirejä tai paikkaa, jossa se voi joutua kosketuksiin sellaisten piirien kanssa. Kun asennat antennia, varo, ettet joudu kosketuksiin mainittujen piirien kanssa, sillä seurauksena voi olla vakava vamma tai kuolema. Tarkista antennin asennus- ja maadoitustiedot kansallisista ja paikallisista sähkösäännöksistä (esimerkiksi Yhdysvalloissa NFPA 70, National Electrical Code, Article 810 ja Kanadassa Canadian Electrical Code, Section 54).

Attention

Ne placez pas l'antenne à proximité d'une ligne aérienne ou d'autres circuits d'éclairage ou d'alimentation, ou dans un endroit où elle risque d'être en contact avec des circuits de ce type. Lors de son installation, assurez-vous bien qu'elle ne touche pas de tels circuits car cela risquerait d'entraîner des blessures graves, voire mortelles. Pour une installation et mise à la terre correctes de l'antenne, veuillez consulter les codes nationaux et locaux (par exemple, États-Unis : NFPA 70, National Electrical Code, Article 810 ; Canada : Code électrique canadien, Section 54).

CISCO CONFIDENTIAL - First Draft

Warnung	Platzieren Sie die Antenne nicht in der Nähe von Starkstrom-Freileitungen oder Schwach- bzw. Starkstromkreisen oder an Stellen, wo sie damit in Kontakt kommen könnte. Gehen Sie bei der Installation der Antenne besonders vorsichtig vor, damit Sie nicht in Kontakt mit derartigen Stromkreisen kommt, da dies zu schweren Verletzungen sogar mit Todesfolge führen kann. Installieren und erden Sie die Antenne sachgerecht unter Einhaltung der jeweils gültigen Sicherheitsvorschriften (zum Beispiel USA: NFPA 70, National Electrical Code, Artikel 810 oder Kanada: Canadian Electrical Code, Abschnitt 54).
Avvertenza	Non sistemare l'antenna nelle vicinanze di circuiti elettrici generali o di altri circuiti di illuminazione o di alimentazione, o dove questa possa venire a contatto con tali circuiti. Durante l'installazione dell'antenna, prestare particolare attenzione a non entrare in contatto con tali circuiti, in quanto questo potrebbe provocare seri danni o morte. Per una corretta installazione e messa a terra dell'antenna, fare riferimento ai codici nazionali e locali (es. U.S.A.: NFPA 70, Codice Elettrico Nazionale, articolo 810, Canada: Codice Elettrico Canadese, sezione 54).
Advarsel	Plasser ikke antennen nær de overliggende strømledningene eller andre lys- eller strømkretser, eller der den kan komme i kontakt med slike kretser. Ved installering av antennen må du være ytterst forsiktig slik at du ikke kommer i kontakt med slike kretser. Dette kan føre til alvorlig skade eller død. For riktig installasjon og jording av antennen, se statlige og lokale forskrifter (for eksempel i USA: NFPA 70, National Electrical Code, Article 810, og i Canada: Canadian Electrical Code, Section 54).
Aviso	Não coloque a antena perto de linhas de alimentação, de outros circuitos ou onde possa entrar em contato com esses circuitos. Ao instalar a antena, tenha muito cuidado para não tocar nesses circuitos, visto que podem provocar ferimentos graves ou até a morte. Para obter informações sobre como instalar e aterrar corretamente a antena, consulte a legislação local e nacional (por ex., U.S.: NFPA 70, National Electrical Code, Artigo 810, Canadá: Canadian Electrical Code, Seção 54).
¡Advertencia!	No coloque la antena cerca de cables de tendido eléctrico u otros circuitos eléctricos, ni donde pueda entrar en contacto con los mismos. Al instalar la antena, extreme las precauciones para no entrar en contacto con dichos circuitos, ya que puede causar heridas graves e incluso la muerte. Para instalar la antena y conectarla a tierra correctamente, consulte los códigos nacionales y locales (p.ej., Estados Unidos: NFPA 70, National Electrical Code, Sección 810, Canadá: Canadian Electrical Code, Artículo 54).
Varning!	Placera inte antennen nära överhängande kraftledningar, andra elljus- eller strömkretsar eller där den kan komma i kontakt med sådan kretsar. Vid installation av antennen måste du vara mycket försiktig så att du inte kommer i kontakt med sådana kretsar eftersom de kan orsaka allvarlig kroppsskada eller dödsfall. För riktig installation och jordning av antennen, hänvisas du till nationella och lokala koder (t.ex. USA: NFPA 70, National Electrical Code, Article 810, Kanada: Canadian Electrical Code, Section 54).
Figyelem	Ne helyezze az antennát elektromos felsővezetékek és más elektromos világítási és tápellátási áramkörök közelébe, és semmilyen olyan környezetbe, ahol ilyen áramkörökkel érintkezhet. Az antenna felszerelésekor különösképpen ügyeljen arra, hogy ne kerüljön érintkezésbe ilyen áramkörökkel, mert az súlyos sérülést vagy halált okozhat. Az antenna helyes üzembe helyezésével és földelésével kapcsolatban az országos és helyi előírások tartalmazznak útmutatást (például az USA-ban: NFPA 70, National Electrical Code, Article 810, Kanadában: Canadian Electrical Code, Section 54).

CISCO CONFIDENTIAL - First Draft

- Предупреждение** Не размещайте антенну поблизости от линий электропередачи, проводов освещения и других силовых линий, а также в местах, где антенна может касаться таких линий. При установке антенны будьте предельно внимательны, чтобы не коснуться таких линий — это может привести к серьезным травмам и даже к смертельному исходу. Сведения о правилах установки и заземлении антенны содержатся в национальных и региональных электротехнических правилах и нормах (например в США — NFPA 70, National Electrical Code, статья 810; в Канаде — Canadian Electrical Code, раздел 54).
- 警告** 请勿将天线安放在过热的电线或其它电灯或电路附近，也不要将它安放在能与此类电路相接触的地方。安装天线时，要特别当心不要接触此类电路，因为它们会造成严重的伤害，甚至导致死亡。有关天线的正确安装和接地，请参阅国家和当地的规范（例如，美国：NFPA 70、美国国家电气规程 810 条款，加拿大：加拿大电气规程，第 54 部分）。
- 警告** 送電線またはその他の電灯/電力回線に近い場所や、これらの回線に接触する可能性のある場所には、アンテナを設置しないでください。アンテナを設置するときは、死傷事故のおそれがあるので、これらの回線に絶対に接触しないよう十分に注意する必要があります。アンテナの適切な設置およびアース接続の手順については、一般規定および地域の規定を参照してください（たとえば、NFPA 70, National Electrical Code, Article 810 [米国]、Canadian Electrical Code, Section 54 [カナダ]）。
-

CISCO CONFIDENTIAL - First Draft

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1300 Series Bridge.

This appendix contains the following sections:

- [Manufacturers Federal Communication Commission Declaration of Conformity Statement, page B-2](#)
- [Department of Communications—Canada, page B-3](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page B-3](#)
- [Declaration of Conformity for RF Exposure, page B-5](#)
- [Guidelines for Operating Cisco Aironet Access Points and Bridges in Japan, page B-5](#)

CISCO CONFIDENTIAL - First Draft

Manufacturers Federal Communication Commission Declaration of Conformity Statement



Models: AIR-BR1310G-A-K9-R or
AIR-BR1310G-A-K9

FCC Certification number: LDK102052P (AIR-MP21G-A-K9-B-P) or
LDK102052 (AIR-MP21G-A-K9-B)

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. Any changes or modification to said product not expressly approved by Cisco could void the user's authority to operate this device.

CISCO CONFIDENTIAL - First Draft**Department of Communications—Canada****Canadian Compliance Statement**

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

Cet appareil 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.

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

European Community, Switzerland, Norway, Iceland, and Liechtenstein**Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC**

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/EC.
Ελληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιαστικές απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.

CISCO CONFIDENTIAL - First Draft

Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.
Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-directiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

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

<http://www.ciscofax.com>

For the 1300 series bridge, the following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

The following CE mark is affixed to the 1100 series equipment:



The above CE mark is required as of April 8, 2000 but might change in the future.

**Note**

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

**Note**

Combinations of power levels and antennas resulting in a radiated power level of above 100 mW eirp are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and/or the CEPT recommendation Rec 70.03. For more details on legal combinations of power levels and antennas, contact Cisco Corporate Compliance.

CISCO CONFIDENTIAL - First Draft

Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements in CFR 47 Sections 2.1091, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The bridge should be installed more than 20 cm from your body or nearby persons.

Guidelines for Operating Cisco Aironet Access Points and Bridges in Japan

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

Japanese Translation

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

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

連絡先 : 03-5549-6500

43768

English Translation

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

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

Contact Number: 03-5549-6500

CISCO CONFIDENTIAL - First Draft**Administrative Rules for Cisco Aironet Bridges in Taiwan**

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

All Bridges**Chinese Translation**低功率電波輻射性電機管理辦法

第十四條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

93815

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

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

Article 17

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

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

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

Bridge Specifications

This appendix provides technical specifications for the Cisco Aironet 1300 Series Bridge, power injector, and power module. [Table C-1](#) lists the technical specifications - TBD.

Table C-1 Bridge, Power Injector, and Power Module Specifications

Category	Bridge	Power Injector and Power Module
Size	Integrated antenna configuration: 8.00 in. W x 8.10 in. H 2.31 in. D (20.32 cm W x 20.57 cm H 5.87 cm D)	Power injector: 4.62 in. W x 4.76 in. H x 1.07 in. D (11.74 cm W x 12.09 cm H x 2.72 cm D) Power module: TBD in. W x TBD in. H x TBD in. D TBD cm W x TBD cm H x TBD cm D
LEDs	Four LEDs on the back panel: Radio traffic, Ethernet traffic, bridge status, and Installation and Alignment Mode	One bi-color power LED on the side panel
Connectors	Bottom panel (left to right): Power injector dual-coax ports (two F-type connectors) and two reverse-TNC antenna connectors	Side panel (left to right): Two coaxial uplink F-type connectors, 48-VDC power connector, RJ-45 connector for 100BASE-T Ethernet, and a RJ45 serial console port connector
Operating Temperature	-22 to 131°F (-30 to 55°C)	Power Injector: -22 to 131°F (-30 to 55°C) Power Module: 32 to 122°F (0 to 50°C)
Cold Start Temperature	TBD°F (TBD°C)	—
Warm-up time (for full performance)	TBD minutes after cold start	—
Non-Operational Temperature	-40 to 185°F (-40 to 85°C)	Power Injector: -40 to 158°F (-40 to 70°C) Power Module: -40 to 185°F (-40 to 85°C)

CISCO CONFIDENTIAL - First Draft**Table C-1 Bridge, Power Injector, and Power Module Specifications (continued)**

Category	Bridge	Power Injector and Power Module
Humidity	0 to 90% (condensing)	Power Injector: 0 to 90% (non-condensing) Power Module: 0 to 95% (non-condensing)
Operational Vibration	0.001 G ² /Hz from 5-100 Hz	0.001 G ² /Hz from 5-100 Hz
Non-Operational Vibration	0.01 G ² /Hz from 5-100 Hz	0.01 G ² /Hz from 5-100 Hz
Environmental Testing Compliance	The enclosure has been successfully tested and is in compliance with a NEMA Type 4 (IP56) enclosure rating.	—
Weight	2.5 lbs (1.13 kg)	Power injector—0.8 lbs (0.36 kg) Power Module—1.0 lbs (0.5 kg)
Input Voltage	48 VDC nominal (supplied by dual-coax cables) 8.5 VDC (minimum) 53 VDC (maximum)	Power injector: 10 VDC to 53VDC Power module: 90 to 264 VAC at TBD to TBD Hz
Power Consumption	13W (typical) TBD W (maximum)	TBD W (maximum)
Radio Output Power	100, 50, 30, 20, 5, or 1 mW (at 1, 2, 5.5, and 11 Mbps) 30, 20, 10, 5, or 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) (Depending on the regulatory domain in which the access point is installed)	Power injector: 18W (maximum at 48 VDC) supplied to the bridge through dual-coax cables Power module: 18W (maximum at 48VDC)
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)	—
Modulation	IEEE 802.11b-compliant radio: Direct Sequence Spread Spectrum (DSSS) Complementary Code Keying (CCK) IEEE 802.11g-compliant radio: Orthogonal Frequency Division Multiplex (OFDM)	—
Subcarrier modulation	CCK (5.5 Mbps and 11 Mbps) BPSK (1 Mbps, 6 Mbps and 9 Mbps) QPSK (2 Mbps, 12 Mbps and 18 Mbps) 16-QAM (24 Mbps and 36 Mbps) 64-QAM (48 Mbps and 54 Mbps)	—

CISCO CONFIDENTIAL - First Draft

Table C-1 Bridge, Power Injector, and Power Module Specifications (continued)

Category	Bridge	Power Injector and Power Module
Data rates	IEEE 802.11g-compliant radio: 100, 50, 30, 20, 5, or 1 mW (at 1, 2, 5.5 and 11 Mbps) 30, 20, 10, 5, or 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) (Depending on the regulatory domain in which the access point is installed)	—
Non-overlapping channels	3	—
Antenna	Integrated antenna 13-dBi patch array Some external antennas: 2.2 dBi omnidirectional 5.2-dBi omnidirectional 12-dBi omnidirectional 9-dBi patch 10 dBi yagi 13.5 dBi yagi 15-dBi sector 21-dBi dish (Depending on the regulatory region)	—
Environmental Air Space	The 1300 series bridge provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the National Electrical Code (NEC) and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1.	 Caution The power injectors and the power modules are not tested to UL 2043 and should not be placed in a building's air-handling spaces, such as above suspended ceilings.
Safety	Bridge: UL 60950 UL 2043 CSA C22.2 No. 60950 IEC 60950 EN 60950	Power injector and power module: UL 60950 CSA C22.2 No. 60950 IEC 60950 EN 60950 Note The power injector and the power module must be used in an indoor environment.

CISCO CONFIDENTIAL - First Draft**Table C-1 Bridge, Power Injector, and Power Module Specifications (continued)**

Category	Bridge	Power Injector and Power Module
Electromagnetic Compatibility (EMC)	Bridge: FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) EN 55022 Class B EN 55024 AS/NZS 3548 Class B VCCI Class B EN 301.489-1 EN 301.489-17	Power injector and power module: FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) EN 55022 Class B EN 55024
Radio Type Approvals	Bridge radio: FCC Parts 15.247, 15.205, 15.209 FCC Bulletin OET-65C Canada RSS-102, and RSS-210 Japan ARIB-STD-33B Japan ARIB-STD-66 Europe EN 300.328	—

CISCO CONFIDENTIAL - First Draft**Operating Range - TBD**

Each regulatory region limits the equivalent isotropic radiated power (EIRP) that can be supported within their region. This restricts the bridge output power that can be used with the bridge antennas and affects the resulting operating range of the bridge.

Table C-2 and Table C-3 provide the calculated maximum operating ranges for IEEE 802.11b and IEEE 801.11g data rates. The calculations are based on 99.965% link availability.

Table C-2 Calculated Maximum Operating Range (in miles) for IEEE 802.11b Data Rates

Bridge Antenna Configuration	Data Rates (Mbps)		
	1	5.5	11
Point-to-point configuration 13 dBi integrated antennas	14.0 mi (22.5 Km)	11.1 mi (17.9 Km)	9.2 mi (14.8 Km)
Point-to-point configuration 21 dBi dish antennas	21.2 mi (34.1 Km)	16.8 mi (27.0 Km)	14.0 mi (22.5 Km)
Point-to-multipoint configuration 5.2 dBi omnidirectional antenna 13 dBi integrated antennas	9.4 mi (15.1 Km)	5.7 mi (9.2 Km)	3.6mi (5.8 Km)
Point-to-multipoint configuration 12 dBi omnidirectional antenna 13 dBi integrated antennas	12.9 mi (20.8 Km)	10.3 mi (16.6 Km)	7.8 mi (12.6 Km)
Point-to-multipoint configuration 12 dBi omnidirectional antenna 21 dBi dish antennas	13.1 mi (21.1 Km)	10.4 mi (16.7 Km)	8.1 mi (13.0 Km)

Table C-3 Calculated Maximum Operating Range (in miles) for IEEE 802.11g Data Rates

Bridge Antenna Configuration	Data Rate (Mbps)			
	6	18	36	54
Point-to-point configuration 13 dBi integrated antennas	4.3 mi (6.9 Km)	2.4 mi (3.9 Km)	1.1 mi (1.8 Km)	0.6 mi (0.96 Km)
Point-to-point configuration 21 dBi dish antennas	10.6 mi (17.1 Km)	7.6 mi (12.2 Km)	3.4 mi (5.5 Km)	1.9 mi (3.1 Km)
Point-to-multipoint configuration 5.2 dBi omnidirectional antenna 13 dBi integrated antennas	1.6 mi (2.6 Km)	0.9 mi (1.4 Km)	0.4 mi (0.64 Km)	0.2 mi (0.32 Km)

CISCO CONFIDENTIAL - First Draft**Table C-3** *Calculated Maximum Operating Range (in miles) for IEEE 802.11g Data Rates (continued)*

Bridge Antenna Configuration	Data Rate (Mbps)			
	6	18	36	54
Point-to-multipoint configuration 12 dBi omnidirectional antenna 13 dBi integrated antennas	3.5 mi (Km)	2.0 mi (3.2 Km)	0.9 mi (1.4 Km)	0.5 mi (0.80 Km)
Point-to-multipoint configuration 12 dBi omnidirectional antenna 21 dBi dish antennas	4.0 mi (6.4 Km)	2.3 mi (3.7 Km)	1.0 mi (1.6 Km)	0.6 mi (0.97 Km)

Channels and Antenna Settings

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

The following topics are covered in this appendix:

- [Channels, page D-2](#)
- [Maximum Power Levels and Antenna Gains, page D-3](#)

CISCO CONFIDENTIAL - First Draft

Channels

IEEE 802.11g (2.4-GHz Band)

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11g 22-MHz-wide channel are shown in [Table D-1](#).

Table D-1 Channels for IEEE 802.11g

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

**Note**

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

CISCO CONFIDENTIAL - First Draft

Maximum Power Levels and Antenna Gains

IEEE 802.11g (2.4-GHz Band)

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. [Table D-2](#) indicates the maximum power levels and antenna gains allowed for each IEEE 802.11g regulatory domain.

**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

Table D-2 Maximum Power Levels Per Antenna Gain for IEEE 802.11g

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)	
		CCK	OFDM
Americas (-A) (4 W EIRP maximum)	2.2	100	30
	6	100	30
	6.5	100	30
	10	100	30
	13.5	100	30
	15	50	20
	21	20	10
EMEA (-E) and Israel(-I) (100 mW EIRP maximum)	2.2	50	30
	6	30	10
	6.5	20	10
	10	10	5
	13.5	5	5
	15	5	1
	21	1	—
Japan (-J) (10 mW/MHz EIRP maximum)	2.2	5	5
	6	5	5
	6.5	5	5
	10	5	5
	13.5	5	5
	15	5	5
	21	5	5

CISCO CONFIDENTIAL - First Draft

Changing the Bridge's Output Power

This section provides instructions for changing the bridge output power to comply with the maximum power limits imposed by regulatory domains (see [“Maximum Power Levels and Antenna Gains” section on page D-3](#)). Follow these instructions to change the bridge output power settings using your browser:

**Note**

Administrator privileges may be required to change bridge settings.

**Note**

To meet regulatory restrictions, the external antenna BR1300 configuration and the external antenna must be professionally installed. The network administration or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

-
- Step 1** Open your Internet browser.
 - Step 2** Enter the bridge's IP address in the browser address or location line and press **Enter**. An Enter Network Password screen appears.
 - Step 3** Enter your username (default Cisco) in the User Name field.
 - Step 4** Enter the bridge password (default Cisco) in the Password field and press **Enter**. The Summary Status page appears.
 - Step 5** Click **Network Interfaces** and the network interface menu appears.
 - Step 6** Click **Radio0-802.11G** and the 802.11G Status screen appears.
 - Step 7** Click the **Settings** tab and the settings screen appears.
 - Step 8** On the CCK Transmit Power (mW) setting, select the maximum CCK power allowed for your antenna in your regulatory region.
 - Step 9** On the OFDM Transmit Power (mW) setting, select the maximum OFDM power allowed for your antenna in your regulatory region.
 - Step 10** Click **Apply**.
 - Step 11** Close your browser.
-

For additional configuration information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Bridges*.

Numeric

- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
- 802.11a** The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 6-, 9-, 12-, 18-, 24-, 36-, 48-, and 54-Mbps wireless LANs operating in the 2.4-GHz frequency band. This standard is also backward compatible with the IEEE 802.11 and IEEE 802.11b standards.

A

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

B

- beacon** A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.
- BOOTP** Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.
- BPSK** A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

CISCO CONFIDENTIAL - First Draft

broadcast packet	A single data message (packet) sent to all addresses on the same subnet.
bridge	A wireless LAN transceiver that is used to connect two or more wired Ethernet networks.

C

CCK	Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
cell	The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.
client	A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.
CSMA	Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates	The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).
dBi	A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.
dBm	An absolute power level described in decibels referenced to 1 mW. 0 dBm is equivalent to 1 mW.
DHCP	Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.
dipole	A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.
domain name	The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.
DNS	Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.
DSSS	Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

CISCO CONFIDENTIAL - First Draft

E

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

F

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

G

gateway	A device that connects two otherwise incompatible networks together.
GHz	Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

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

M

MAC	Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.
modulation	Any of several techniques for combining user information with a transmitter's carrier signal.

CISCO CONFIDENTIAL - First Draft

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

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

N

non-root bridge A wireless transceiver connected to a remote Ethernet network that communicates only with another wireless transceiver connected to the main Ethernet network.

O

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

orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant and IEEE 802.11g-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.

power injector A device that supplies DC power to another device over Ethernet communication lines.

Q

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

R

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

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

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

root bridge A wireless transceiver connected to the main Ethernet network that communicates with other wireless transceivers connected to remote Ethernet networks.

CISCO CONFIDENTIAL - First Draft

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

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

S

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

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

T

transmit power The power level of radio transmission.

U

UNII Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.

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

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

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

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

W

WEP Wired Equivalent Privacy. An optional security mechanism defined within the IEEE 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

workstation A computing device with an installed client adapter.

CISCO CONFIDENTIAL - First Draft

A

abbreviating commands [7-3](#)
antenna
 gains [D-3](#)
antennas [C-3](#)
Apply button [6-4](#)
audience [ix](#)

B

Back button [6-4](#)
basic settings, checking [8-5](#)
bridge, image [8-7](#)

C

Cancel button [6-4](#)
caution [x](#)
Cisco TAC [8-1](#)
CLI
 abbreviating commands [7-3](#)
 command modes [7-2](#)
 editing features
 enabling and disabling [7-6](#)
 keystroke editing [7-6](#)
 wrapped lines [7-7](#)
 error messages [7-4](#)
 filtering command output [7-8](#)
 getting help [7-3](#)

history
 changing the buffer size [7-5](#)
 described [7-4](#)
 disabling [7-5](#)
 recalling commands [7-5](#)
 no and default forms of commands [7-3](#)
command-line interface, see CLI
command modes [7-2](#)
commands
 abbreviating [7-3](#)
 no and default [7-3](#)
connectors [1-3](#), [C-1](#), [C-3](#)
conventions, document [x](#)

D

data rates [2-5](#), [C-3](#)
declarations of conformity [B-1](#)
default commands [7-3](#)
default configuration
 resetting to defaults [8-6](#)
documentation
 conventions [x](#)
 related publications [xi](#)

E

editing features
 enabling and disabling [7-6](#)
 keystrokes used [7-6](#)
 wrapped lines [7-7](#)
EIRP, maximum [5-9 to ??](#), [D-3 to ??](#)
environmental conditions [2-5](#)

CISCO CONFIDENTIAL - First Draft

error messages, during command entry [7-4](#)

F

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

FCC Safety Compliance [2-3](#)

filtering, show and more command output [7-8](#)

frequencies [D-2](#)

frequency range [C-2](#)

G

global configuration mode [7-2](#)

H

help, for the command line [7-3](#)

history

changing the buffer size [7-5](#)

described [7-4](#)

disabling [7-5](#)

recalling commands [7-5](#)

Home button [6-3](#)

I

inline power [1-3](#)

input power [C-2](#)

installation guidelines [2-3](#)

interface configuration mode [7-2](#)

IP address, finding and setting [5-10](#)

IPSU [5-9](#)

M

MAC [5-11, 5-12](#)

management options, CLI [7-1](#)

modulation [C-2](#)

N

network configurations [1-6](#)

no commands [7-3](#)

O

obtaining documentation [xi](#)

OK button [6-4](#)

operating temperature [C-1](#)

P

package contents [2-6](#)

password reset [8-6](#)

power

inline [1-3](#)

input [C-2](#)

power level, maximum [D-3](#)

privileged EXEC mode [7-2](#)

R

regulatory

domains [D-2](#)

regulatory information [B-1](#)

related publications [xi](#)

reloading bridge image [8-7](#)

RF exposure [B-5](#)

S

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

site survey [2-5](#)

size [C-1](#)

SSH [7-9](#)

SSH Communications Security, Ltd. [7-9](#)

SSID, troubleshooting [8-5](#)

CISCO CONFIDENTIAL - First Draft

T

TAC [8-1](#)

Telnet [5-13](#)

temperature, operating [C-1](#)

TFTP server [8-7](#)

troubleshooting [8-1](#)

U

unpacking [2-5](#)

user EXEC mode [7-2](#)

W

warning, defined [x to xi](#)

warnings [2-2, A-1](#)

Web-based interface

 common buttons [6-3](#)

weight [C-2](#)

CISCO CONFIDENTIAL - First Draft