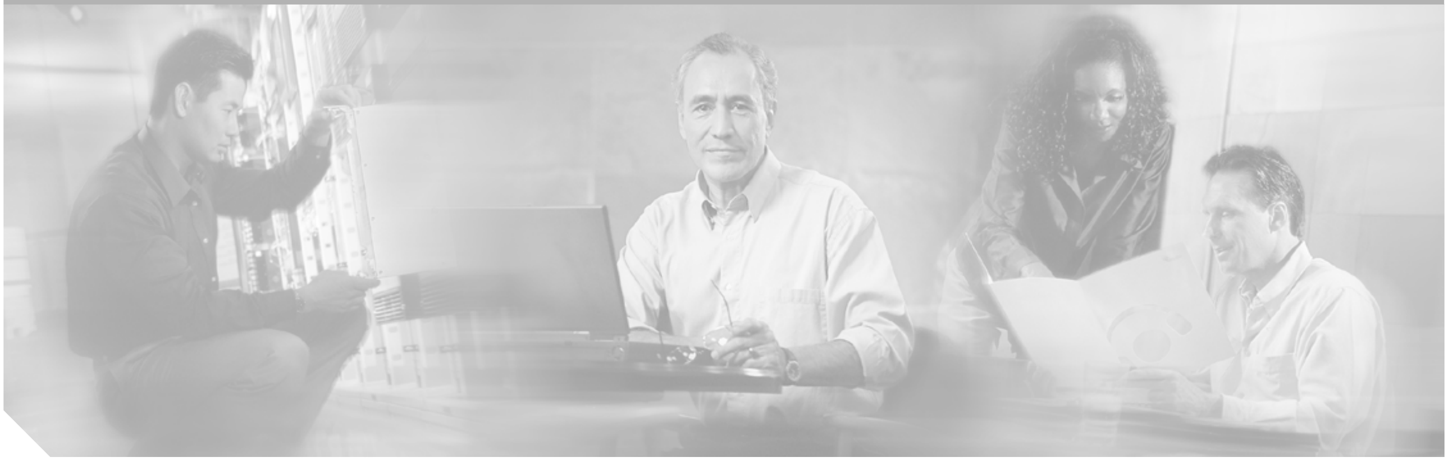


Cisco Aironet Access Point Hardware Installation Guide

340 Series and 350 Series

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-0738-02

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.

Cisco Aironet Access Point Hardware Installation Guide

CONTENTS

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Aironet Access Point Hardware Installation Guide*.

Objectives

This publication explains the steps for initial setup and configuration of the access point. This publication also provides troubleshooting information and detailed specifications.

Audience

This publication is for the person installing and configuring a Cisco Aironet Access Point 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 features and specifications of access points.

Chapter 2, “Installation,” provides basic installation instructions.

Chapter 3, “Basic Configuration,” describes how to enter basic configuration settings.

Chapter 4, “Troubleshooting,” provides solutions to potential problems encountered during setup.

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 access point conforms and provides guidelines for operating access points in Japan.

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 **The 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 Appendix A in this manual.

Related Publications

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

- *Quick Start Guide: Cisco Aironet Access Points* describes how to attach cables, power on, and assign an IP address and default gateway for the access point.
- *Cisco Aironet Access Point Software Configuration Guide* describes the access point's management system and explains how to configure the access point.
- *Release Notes for Cisco Aironet Access Points* describes features and caveats for access points running firmware release 10.14.
- *Cisco Secure Access Control Server for Windows 2000/NT Servers Version 2.6 User Guide* provides complete instructions for using Cisco Secure ACS, including steps for configuring Cisco Secure ACS to support access points.
- *Quick Start Guide: Cisco Aironet Wireless LAN Adapters* describes how to install and configure PC and PCI card client adapters for use in a wireless LAN.
- *Cisco Aironet Wireless LAN Adapters Hardware Installation Guide* provides hardware features, physical and performance characteristics, and installation instructions for PC and PCI card client adapters.
- *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* provides instructions for installing and using the wireless client adapter utilities.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation 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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  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 e-mail comments about technical documentation 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-a-day, 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. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website 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. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which 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 the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which 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.

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

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

- 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://cisco.com/univercd/cc/td/doc/pcat/

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

  http://www.ciscopress.com

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

  http://www.cisco.com/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/ipj

- 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

Overview

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

This chapter provides information on the following topics:

- Key features
- Network configuration examples
- Access point specifications

Key Features

This section describes the key features of the access point:

- Inline power
- Omni-directional antennas
- Ethernet and serial ports
- Indicators
- Industrial temperature range and UL 2043 rating for 350 series metal case access point

Inline Power

Cisco Aironet 350 series access points receive power through the Ethernet cable, so you do not need to run a separate power cord to the access point. Plug the Ethernet cable into the Ethernet port on the back of the access point and plug the other end into one of three possible power sources:

- A Cisco Aironet power injector
- A switch with inline power, such as the Cisco Catalyst 3524-PWR-XL switch
- A power patch panel, such as the Cisco Catalyst Inline Power Patch Panel

Note Cisco Aironet 340 series access points rely on a separate power supply plugged into the power port on the back of the access point.

Caution Cisco Aironet power injectors are designed for use with 350 series access points and bridges only. Using the power injector with other Ethernet-ready devices can damage the equipment.

Caution Cisco Aironet Power Injectors are not rated for operation in a building’s environmental air space, such as above suspended ceilings.

Caution The operational voltage range for Cisco Aironet 350 series access points and bridges is 24 to 60 VDC. Higher voltage can damage the equipment.

Omni-Directional Antennas

The access point’s omni-directional, 2.2 dBi antennas provide diversity coverage for your wireless LAN area. Diversity coverage helps maintain a clear radio signal between the access point and wireless client devices. Just as you can improve signal clarity on your car radio at a stoplight by creeping ahead a few inches, the access point can improve signal quality by choosing the antenna that is receiving the best signal from a client device.

Some access points models are equipped with dual reverse-polarity TNC connectors that you can use to connect to your own antennas for special applications.

Ethernet and Serial Ports

Ethernet Port

The access point's Ethernet port accepts an RJ-45 connector, linking the access point to your 10/100 Ethernet LAN. The 350 series access point receives power through the Ethernet cable from a switch with inline power, from a power patch panel, or from the access point's power injector.

Serial Port

The access point's serial port provides console access to the access point's management system. Use a nine-pin, straight-through, male-to-female serial cable to connect your computer's COM 1 or COM 2 port to the access point's serial port. Assign the following port settings to a terminal emulator to open the management system pages: 9600 baud, 8 data bits, No parity, 1 stop bit, and Xon/Xoff flow control.

Metal Enclosure

The 350 series metal case access point contains a metal enclosure having adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space in accordance with Section 300-22(c) of the NEC. The 350 series metal case access point also supports an industrial temperature operating range.

Indicators

The three indicators on top of the access point report Ethernet activity, association status, and radio activity. The indicators are labeled in Figure 1-1 and Figure 1-2.

Figure 1-1 Indicators on the 340 and 350 Series Access Point

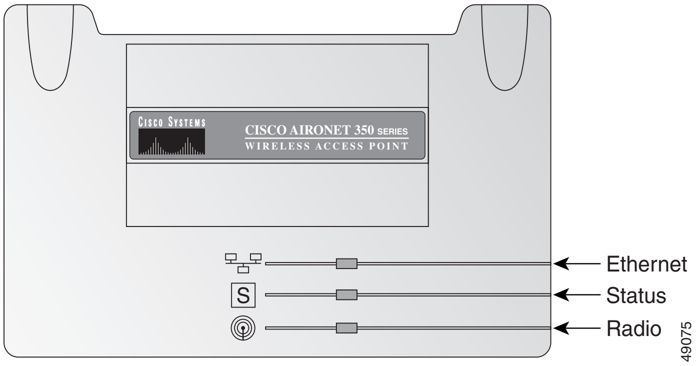
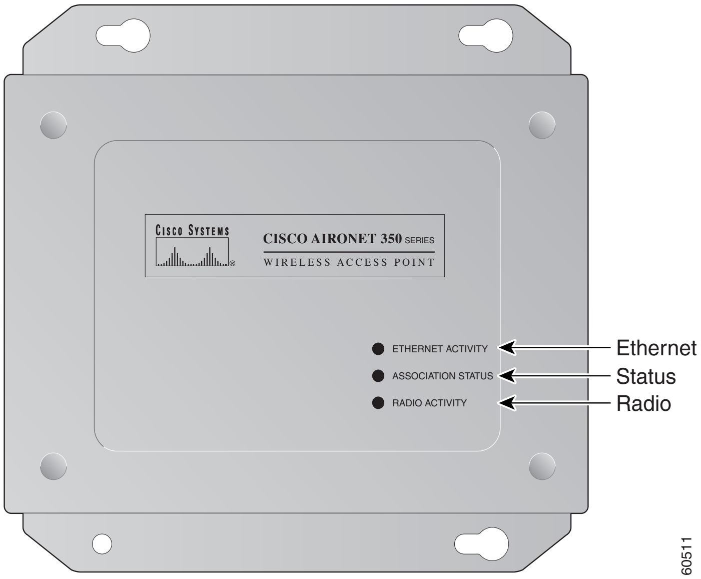


Figure 1-2 Indicators on the 350 Series Metal Case Access Point



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

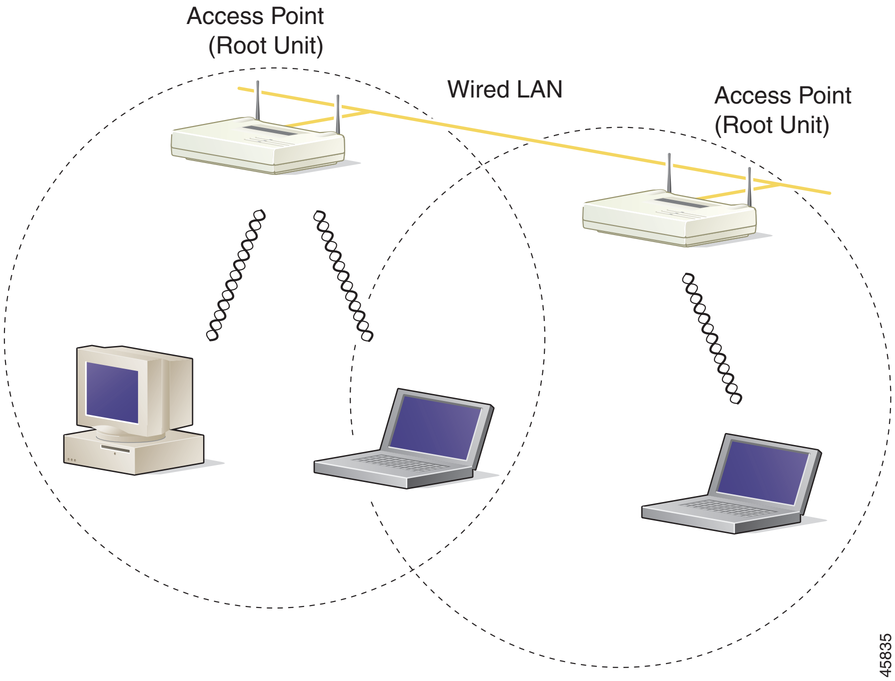
Network Configuration Examples

This section describes the access point's role in three common wireless network configurations. The access point's default configuration is as a root unit on a wired LAN. The other two possible roles, repeater unit and central unit in an all-wireless network, require specific changes to the default configuration.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-3 shows access points acting as root units on a wired LAN.

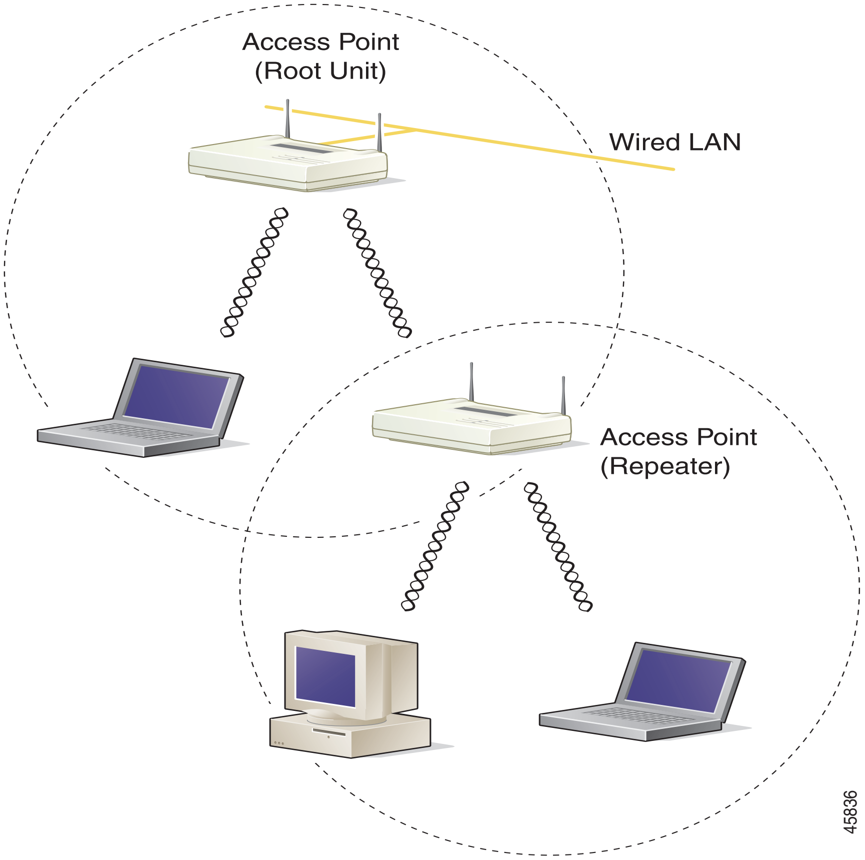
Figure 1-3 Access Points as Root Units on a Wired LAN



Repeater Unit That Extends Wireless Range

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the greatest performance for the client. Figure 1-4 shows an access point acting as a repeater.

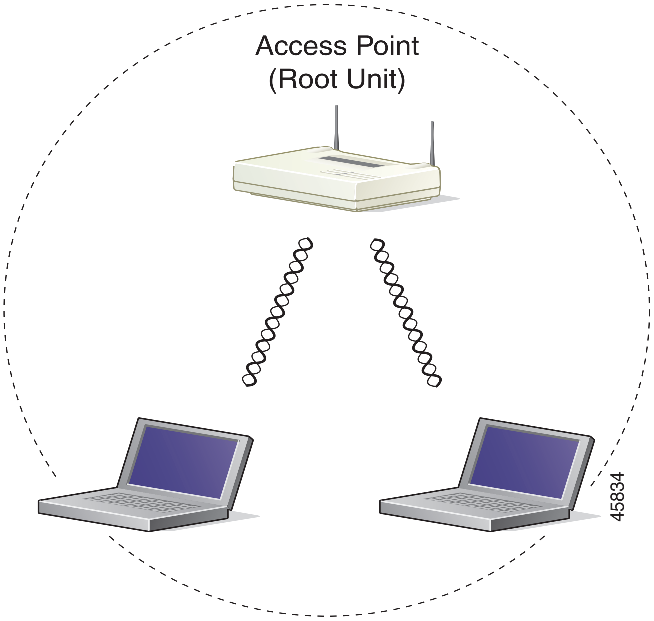
Figure 1-4 Access Point as Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-5 shows an access point in an all-wireless network.

Figure 1-5 Access Point as Central Unit in All-Wireless Network



Access Point Specifications

Table 1-1 lists specifications for the access point.

Table 1-1 Access Point Specifications

Category	Specification
Physical	
Size	6.30 in. (16 cm) W x 4.72 in. (12 cm) D x 1.45 in. (3.7 cm) H
Status indicators	Three indicators on the top panel: Ethernet traffic, status, and radio traffic
Connectors	On the back panel: An RJ-45 jack for 10/100 Ethernet connections; a nine-pin serial connector; a power connector (plug-in AC adapter) for a regulated 5V input (340 series only)
Voltage range	24 to 60 VDC (regulated 5 VDC for 340 series only)
Operating temperature range	32 to 122^{o}F (0 to 50^{o}C) for 340 and 350 series –4 to 131^{o}F (–20 to 55^{o}C) for 350 series metal case 32 to 104^{o}F (0 to 40^{o}C) for power injectors
Weight	Less than 1 lb (0.45 kg) for 340 and 350 series 1.43 lbs (0.64 kg) for 350 series metal case
Radio	
Power output	100, 50, 30, 20, 5, or 1 mW for 350 series 30, 20, 5, or 1 mW for 340 series (Depending on the regulatory domain in which the access point is installed)
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)
Range	Indoor: 150 ft at 11 Mbps (100 ft for 340 series only) 350 ft at 1 Mbps (300 ft for 340 series only) Outdoor: 800 ft at 11 Mbps (400 ft for 340 series only) 2000 ft at 1 Mbps (1500 ft for 340 series only)
Modulation	Direct Sequence Spread Spectrum
Data rates	1, 2, 5.5, and 11 Mbps

Table 1-1 Access Point Specifications (continued)

Category	Specification
Antenna	Two captured 2.2 dBi gain antennas or a diversity system with two reverse-TNC connectors (antennas for this model are sold separately). Some models in the 340 series have one 2.2 dBi gain antenna.
Compliance	Operates license-free under FCC Part 15 and complies as a Class B computing device. Complies with DOC regulations. Complies with the following: ETS 300.328, FTZ 2100, MPT 1349, FCC Part 15.107 and 15.109 Class B, ICES-003 Class B (Canada), CISPR 22 Class B, AS/NZS 3548 Class B, VCCI Class B, EN 50082-1, UL1950, CSA 22.2 No. 950, EN 60950, IEC 60950, VCCI, and others (see Appendix B). 350 series metal case access point complies with UL 2043 for products installed in air handling spaces, such as above suspended ceilings. ⚠ **Caution** Cisco Aironet Power Injectors are not rated for UL 2043 and should not be placed in air handling spaces, such as above suspended ceilings.

Installation

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

- Cautions and Warnings
- Installation Guidelines
- Unpacking the Access Point
- Connecting the Ethernet and Power Cables

Cautions and Warnings

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

Note The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to radiated frequency (RF) electromagnetic energy emitted by FCC-certified equipment. 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 will result in user exposure substantially below the FCC recommended limits.

Caution Cisco Aironet power injectors are designed for use with 350 series access points and bridges only. Using the power injector with other Ethernet-ready devices can damage the equipment.

Caution The operational voltage range for Cisco Aironet 350 series access points and bridges is 24 to 60 volts. Higher voltage can damage the equipment.

Caution Cisco Aironet Power Injectors are not rated for operation in a building’s environmental air space, such as above suspended ceilings.

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.**

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

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

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).**

Installation Guidelines

This section describes things to keep in mind when installing your access point. Sections include:

- Basic Guidelines
- Special Considerations
- Coverage Options
- Site Surveys

Basic Guidelines

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

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

Special Considerations

The 350 series metal case access point provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings. This access point is intended for indoor use and can be used in environments where the temperature ranges from -4 to 131°F (-20 to 55°C).

⚠ **Caution** Cisco Aironet Power Injectors are not rated for operation in a building's environmental air space, such as above suspended ceilings.

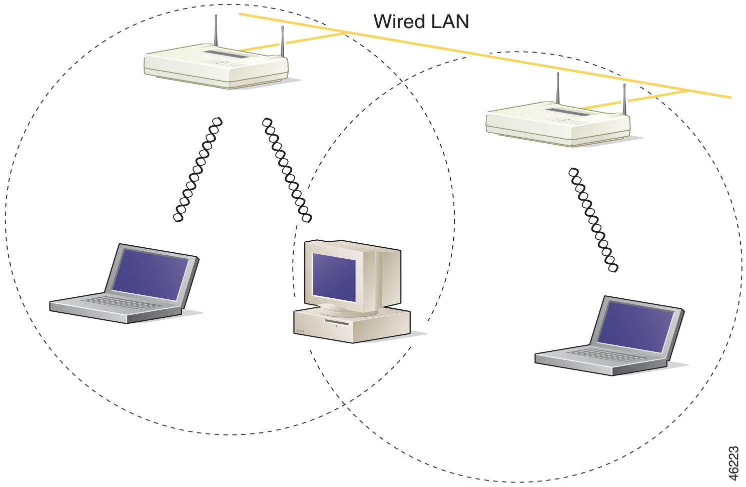
Coverage Options

The network architecture options of wireless stations and access points provide for a variety of coverage alternatives and flexibility. The network can be designed to provide a wide coverage area with minimal overlap or a narrow coverage area with heavy overlap. A narrow coverage area with heavy overlap improves network performance and protection against downtime if a component fails.

Minimal Overlap Coverage Option

By arranging the access points so that the overlap in a coverage area is minimized, a large area can be covered with minimal cost (see Figure 2-1). The total bandwidth available to each wireless client device depends on the amount of data each mobile station needs to transfer and the number of stations located in each cell. Seamless roaming is supported as a client device moves in and out of range of each access point, thereby maintaining a constant connection to the wired LAN. Each device in the radio network must be configured with the same SSID to provide roaming capability.

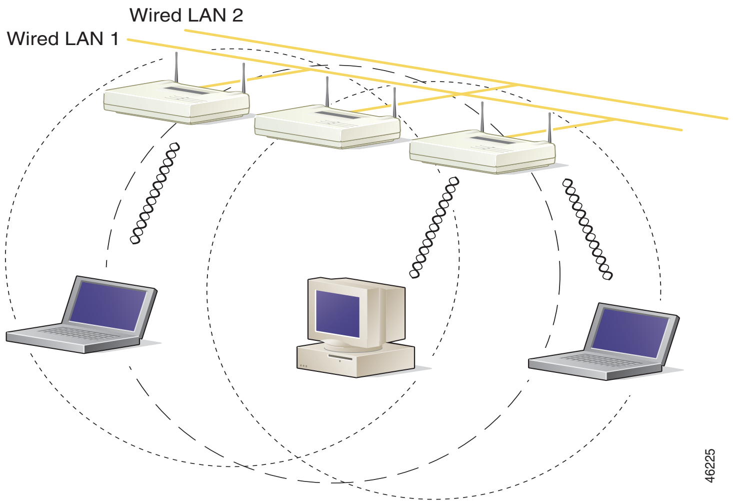
Figure 2-1 Minimal Overlap Coverage Option



Multiple Overlapping Networks Coverage Option

Multiple networks can operate in the same vicinity (see Figure 2-2). The architecture provides multiple channels that can exist in the same area with virtually no interference to each other. In this mode, each system must be configured with different SSIDs and different channels, which may (depending on configurations) prevent clients from roaming to access points of a different wireless network.

Figure 2-2 Multiple Overlapping Networks Coverage Option

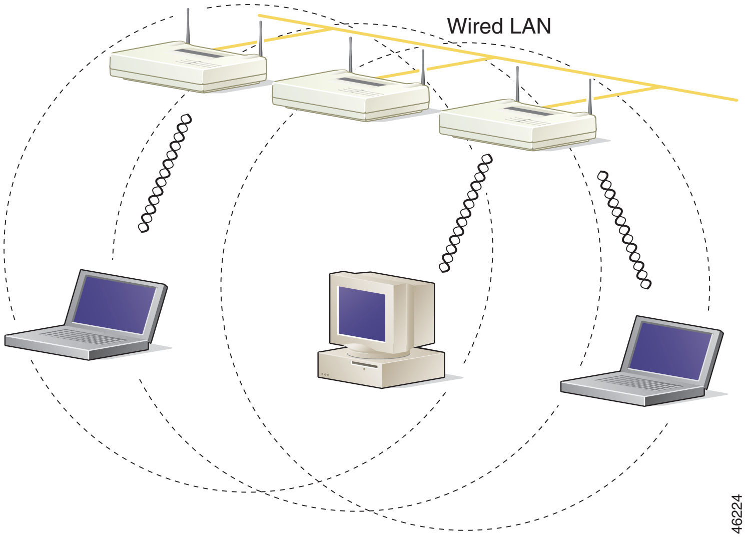


Heavy Overlap Coverage Option

By arranging the access points so the overlap in coverage area is nearly maximized, a large number of mobile stations can be supported in the same wireless infrastructure (see Figure 2-3). However, devices in overlapping coverage areas on the same frequency will detect adjacent cell traffic and delay transmissions that would cause collisions. This configuration reduces the aggregate radio system throughput. Heavy cell overlap is not recommended for maximum system throughput.

Because of the redundancy in coverage overlap, network access is not lost if an access point fails. Upon failure of the access point, the station automatically roams to an operational access point. With this architecture, each device in the RF network must be configured with the same SSID to provide the roaming capability.

Figure 2-3 Heavy Overlap Coverage Option



Site Surveys

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Before installing multiple access points, you should perform a site survey to determine the optimum utilization 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 threshold 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.
- Physical environment – Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- Obstructions – A physical obstruction such as metal shelving or a steel pillar can hinder performance of wireless devices. Avoid locating the devices in a location where there is a metal barrier between the sending and receiving antennas.

- Building materials – Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks. Metal or steel construction is a barrier to radio signals.

Unpacking the Access Point

Follow these steps to unpack the access point:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in the "Package Contents" section are included in the shipment. Check each item for damage.

Package Contents

Each access point is shipped with the following items:

- Cisco Aironet Access Point
- AC to DC power adapter (340 series only)
- Cisco Aironet power injector (350 series only)
- Nine-pin, male-to-female, straight-through serial cable
- *Quick Start Guide: Cisco Aironet Access Points*
- Cisco Aironet Access Point CD-ROM
- Cisco Information Packet, which contains warranty, safety, and support information
- Cisco product registration card

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

Connecting the Ethernet and Power Cables

Because of hardware differences, setup procedures differ for 340 series access points and 350 series access points. Cabling instructions for each series are included in the following sections:

- Connecting Cables on 340 Series Access Points
- Connecting Cables on 350 Series Access Points

Connecting Cables on 340 Series Access Points

Follow these steps to connect the Ethernet cable and power supply on 340 series access points:

Step 1 Plug the RJ-45 Ethernet connector into the Ethernet port on the back of the access point.

Step 2 Connect the other end of the Ethernet cable to the 10/100 Ethernet LAN.

⚠ **Caution** Do *not* connect the Ethernet cable when the access point is powered up. Always connect the Ethernet cable before you apply power to the access point.

✎ **Note** The access point does not have an on/off switch, so power is applied to the unit when you plug it in.

Step 3 Plug the power adapter into a suitable power receptacle.

Step 4 Plug the power connector into the back of the access point.

At start-up, all three LEDs on the top of the access point slowly blink amber, red, and green in sequence; the sequence takes a few minutes to complete. During normal operation, the LEDs blink green. Refer to Chapter 4, “Troubleshooting,” for LED descriptions.

Step 5 Follow the steps in Chapter 3, “Basic Configuration” to assign basic settings to the access point.

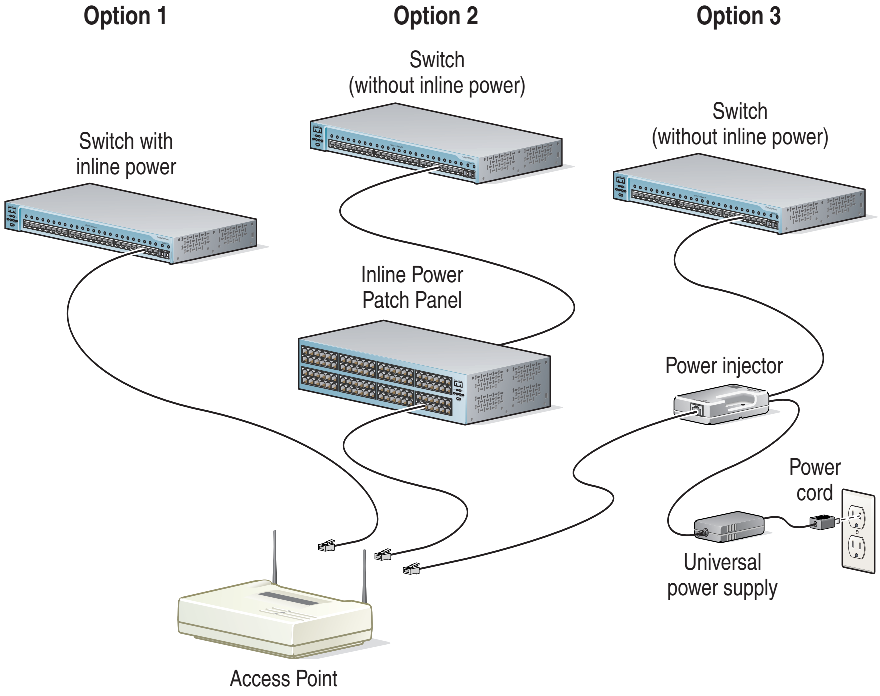
Connecting Cables on 350 Series Access Points

Follow these steps to connect the Ethernet cable and power supply on 350 series access points:

Step 1 Plug the RJ-45 Ethernet connector into the Ethernet port on the back of the access point.

Step 2 Choose a power option for the access point. The 350 series access point receives power through the Ethernet cable. Figure 2-4 shows the three power options for the access point.

Figure 2-4 Access Point Power Options



Power options include:

- A switch with inline power, such as a Cisco Catalyst 3524-PWR-XL
- An inline power patch panel, such as a Cisco Catalyst Inline Power Patch Panel
- A Cisco Aironet power injector

Caution Cisco Aironet power injectors are designed for use with 350 series access points and bridges only. Using the power injector with other Ethernet-ready devices can damage the equipment.

Caution The operational voltage range for Cisco Aironet 350 series access points and bridges is 24 to 60 VDC. Higher voltage can damage the equipment.

Step 3 Connect the other end of the Ethernet cable to the device that will supply power.

If you use a power injector, follow these additional steps:

a. Plug the cable from the access point into the end of the power injector labeled *To AP/Bridge*.

b. Run an Ethernet cable from the end of the power injector labeled *To Network* to the 10/100 Ethernet switch.

c. Plug the female end of the power cord into the universal power supply.

d. Plug the male end of the power cord into a power outlet or power strip.

At start-up, all three LEDs on the top of the access point slowly blink amber, red, and green in sequence; the sequence takes a few minutes to complete. During normal operation, the LEDs blink green. Refer to Chapter 4, "Troubleshooting," for LED descriptions.

Step 4 Follow the steps in Chapter 3, "Basic Configuration," to assign basic settings to the access point.

CHAPTER 3

Basic Configuration

This chapter describes initial configuration of the access point using the Internet browser-based management system. You can also reach the management system through the access point's serial port or through Telnet. Consult Chapter 2 in the *Cisco Aironet Access Point Software Configuration Guide* for complete instructions on using these interfaces.

This chapter includes the following sections:

- Before You Start
- Summary of Configuration Steps
- Using the IP Setup Utility
- Entering Basic Settings
- Default Basic Settings

Before You Start

Before configuring the access point, ask your network administrator for the following information:

- The service set identifier (SSID) for the access point.
- A system name for the access point. The name should describe the location or principal users of the access point.
- If your network does not use DHCP to assign IP addresses, you will need an IP address for the access point.
- If your network uses subnets, you will need a default gateway and an IP subnet mask for the access point.
- The access point's MAC address, which is printed on the label on the bottom of the access point.

Summary of Configuration Steps

You use the Express Setup page to assign basic settings to the access point. For instructions on setting up security, filtering, and other access point features, consult the *Cisco Aironet Access Point Software Configuration Guide* on the access point CD.

You will follow these steps to enter the access point's basic settings:

1. Connect the access point as described in the *Quick Start Guide: Cisco Aironet Access Points*.
2. Use an Internet browser to open the access point's management system by browsing to the access point's IP address. If your network uses a DHCP server, use the IP Setup Utility (IPSU) to find the access point's DHCP-assigned IP address. The "Using the IP Setup Utility" section on page 3-2 describes how to use IPSU.

   You can also use a nine-pin, straight-through, male-to-female serial cable to connect your computer's COM1 or COM2 port to the serial port on the back of the access point and use a terminal emulator to open the management system. The "Using a Terminal Emulator" section on page 3-7 describes using a terminal emulator to assign basic settings.
3. Enter basic settings on the Express Setup page.

Using the IP Setup Utility

The IP Setup utility (IPSU) allows you to find the access point's IP address when it has been assigned by a DHCP server. You can also use IPSU to set the access point's IP address and SSID if they have not been changed from the default settings.

Note IPSU can be used only on the following operating systems: Windows 95, 98, NT, 2000, ME, or XP. For other operating systems, you must use the access point console port and a terminal emulator program to configure the access point.

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

Obtaining and Installing IPSU

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

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

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

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

Step 3 Locate the access point firmware and utilities section and click **Cisco Aironet 350 Series (VXWorks)**.

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

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

Step 6 Click **Submit**.

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

Step 8 Select the file again to download it.

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

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

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

The IPSU icon appears on your computer desktop.

Finding the Access Point's IP Address

If your access point receives an IP address from a DHCP server, use IPSU to find its IP address. Run IPSU from a computer on the same network as the access point. Follow these steps to find the access point's IP address:

Step 1 When the utility window opens, make sure **Get IP addr** is selected in the Function box.

Step 2 Type the access point's MAC address in the Device MAC ID field. The access point's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point's MAC address might look like the following example:

004096xxxxxx

Note The MAC address field is not case-sensitive.

Step 3 Click **Get IP Address**.

Step 4 When the access point's IP address appears in the IP Address field, write it down.

If IPSU reports that the IP address is 10.0.0.1, the default IP address, then the access point did not receive a DHCP-assigned IP address. Steps for assigning an IP address are included in the "Default IP Address" section in Chapter 3 of the *Cisco Aironet Access Point Software Configuration Guide*.

Step 5 To check the IP address, browse to the access point's browser-based management pages. Open an Internet browser.

Step 6 Type or paste the access point's IP address in the browser's location or address field. (If you are using Netscape, the field is labeled *Netsite* or *Location*; if you are using Microsoft Explorer, the field is labeled *Address*.)

Step 7 Press **Enter.** The access point's home page appears.

Setting the Access Point's IP Address and SSID

If your access point does not receive an IP address from a DHCP server, or if you want to change the default IP address, you can use IPSU to assign an IP address. You can set the access point's SSID at the same time.

Note The computer you use to assign an IP address to the access point must have an IP address of its own.

Note IPSU can change the access point's IP address and SSID only from their default settings. After the IP address and SSID have been changed, IPSU cannot change them again. (For additional information see *Using an Internet Browser* or *Using a Terminal Emulator* sections.)

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

Step 1 Double-click the **IP Setup** icon on your computer desktop. (If IPSU is not installed on your computer, follow the steps in the "Obtaining and Installing IPSU" section on page 3-3 to install it.)

Step 2 When the utility window opens, make sure **Set Parameters** is selected in the Function box.

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

004096xxxxxx

Note The MAC address field is not case-sensitive.

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

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

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

Step 6 Click **Set Parameters**.

Step 7 To test the IP address, open an Internet browser.

Step 8 Type or paste the access point's IP address in the browser's location or address field. (If you are using Netscape, the field is labeled *Netsite* or *Location*; if you are using Microsoft Internet Explorer, the field is labeled *Address*.)

Step 9 Press **Enter.** The access point's home page appears.

Entering Basic Settings

You can open the access point's management system through your Internet browser or through the access point's serial port using a terminal emulator. Each method is described below.

Using an Internet Browser

Follow these steps to enter basic settings with an Internet browser:

Step 1 Open an Internet browser.

Step 2 Type or paste the access point's IP address in the browser's location field. (If you are using Netscape Communicator, the field is labeled *Netsite* or *Location*; if you are using Microsoft Explorer, the field is labeled *Address*.) Press **Enter**.

Step 3 When the access point's Summary Status page appears, click **Setup**. When the Setup page appears, click **Express Setup**.

Note If the access point is new and its factory configuration has not been changed, the Express Setup page appears instead of the Summary Status page when you first browse to the access point.

Step 4 Type a system name for the access point in the System Name field. A descriptive system name makes it easy to identify the access point on your network.

Step 5 Select a configuration server protocol from the Configuration Server Protocol pull-down menu. The configuration server protocol you select should match your network's method of IP address assignment. The **Configuration Server** link takes you to the Boot Server Setup page, which you use to configure the access point to work with your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

The Configuration Server Protocol pull-down menu options include:

- None—Your network does not have an automatic system for IP address assignment.
- BOOTP—With Bootstrap Protocol, IP addresses are hard-coded based on MAC addresses.
- DHCP—With Dynamic Host Configuration Protocol, IP addresses are "leased" for predetermined periods of time.

Step 6 Type an IP address in the Default IP address field. If DHCP is not enabled for your network, the IP address you enter in this field will be the access point's static IP address. If DHCP or BOOTP is enabled, the address you enter in this field provides the IP address only when no server responds with an IP address for the access point.

Step 7 Enter an IP subnet mask in the Default IP Subnet Mask field to identify the subnetwork so the access point's IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only when no server responds to the access point's DHCP or BOOTP request.

Step 8 Enter the IP address of your default internet gateway in the Default Gateway field. The entry 255.255.255.255 indicates no gateway. Clicking the Gateway link takes you to the Routing Setup page, which you use to configure the access point to communicate with the IP network routing system.

Step 9 Type an SSID for the access point in the Radio Service Set ID (SSID) field. The SSID is a unique identifier that client devices use to associate with the access point. The SSID can be any alphanumeric entry from two to 32 characters long.

Step 10 Select a network role for the access point from the Role in Radio Network pull-down menu. The menu contains the following options:

- Access Point/Root—A wireless LAN transceiver that connects an Ethernet network with wireless client stations. Use this setting if the access point will be connected to the wired LAN.
- Repeater/Non-Root—An access point that transfers data between a client and another access point. Use this setting for access points not connected to the wired LAN.
- Client/Non-root—A station with a wireless connection to an access point. Use this setting for diagnostics, such as when you need to test the access point by having it communicate with another access point.

Step 11 Select an Optimize Radio Network For option to assign either preconfigured settings or customized settings for the access point radio:

- Throughput—Maximizes the data volume handled by the access point but might reduce the access point's range.
- Range—Maximizes the access point's range but might reduce throughput.
- Custom—The access point will use the settings you enter on the AP Radio Hardware page. Click the Custom link to go to the AP Radio Hardware page.

Step 12 To automatically configure the access point to be compatible with other devices on your wireless LAN, select an Ensure Compatibility With option:

- 2-Mbps clients—Select this setting if your network contains Cisco Aironet devices that operate at 2 Mbps.
- non-Aironet 802.11—Select this setting if there are non-Cisco Aironet devices on your wireless LAN.

Step 13 To use Simplified Network Management Protocol (SNMP), enter a community name in the SNMP Admin. Community field. This name automatically appears in the list of users authorized to view and make changes to the access point's management system.

Click the **SNMP** link to go to the SNMP Setup page, where you can edit other SNMP settings.

You can define other SNMP communities with User Management. The "Security Setup" section in Chapter 3 of the *Cisco Aironet Access Point Software Configuration Guide* describes User Management.

Step 14 Click **OK**. The Setup page appears. If you changed the Role in Radio Network setting, your access point reboots.

Using a Terminal Emulator

This section provides instructions for Microsoft's HyperTerminal; other programs are similar.

Selecting Pages and Settings

When you type names and settings that appear in brackets you jump to that page or setting. HyperTerminal jumps to the page or setting as soon as it recognizes a unique name, so you need to type only the first few characters in the page or setting name. To jump from the home page to the Setup page, for example, you would only need to type **se**.

Applying Changes to the Configuration

The console interface's auto-apply feature is on by default, so changes you make to any page are applied automatically when you move to another management page. To apply changes and stay on the current page, type **apply** and press **Enter**.

Assigning Basic Settings

Follow these steps to assign basic settings to the access point with a terminal emulator:

Step 1 Connect a nine-pin, male-to-female, straight-through serial cable to the COM port on a computer and to the RS-232 serial port on the back of the access point. Figure 3-1 and Figure 3-2 show the location of the access point's serial port.

Figure 3-1 Connecting the Serial Cable for 340 Series and 350 Series Access Points

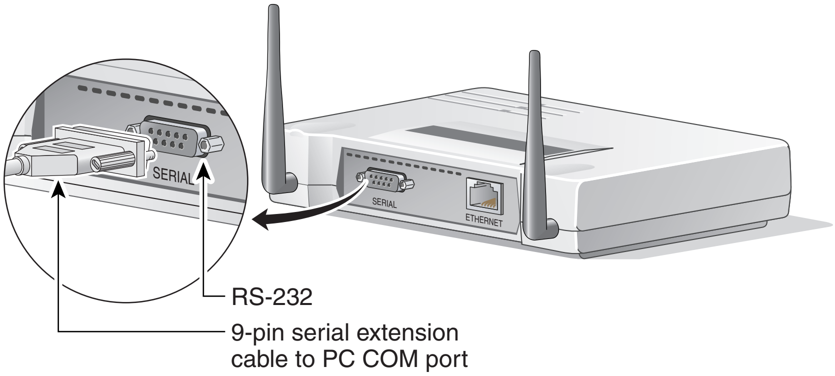
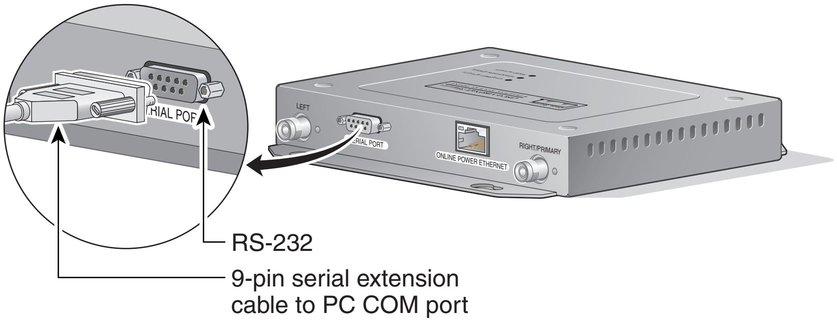


Figure 3-2 Connecting the Serial Cable for 350 Series Metal Case Access Points



Step 2 Open a terminal emulator.

Step 3 Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: No parity
- Stop bits: 1
- Flow control: Xon/Xoff

Step 4 Press **=** to display the home page of the access point. If the access point is new and its factory configuration has not been changed, the Express Setup page appears; if the access point has been configured, the Summary Status page appears.

Step 5 Press **n** to select System Name. Type a system name for the access point and press **Enter**. A descriptive system name makes it easy to identify the access point on your network.

Step 6 Press **t** and then press **Enter** to select Terminal Type. Press **t** and then press **Enter** to select teletype display on the console interface. Press **a** and then press **Enter** to select ANSI display on the console interface.

Step 7 Press **pr** and then press **Enter** to select Config Server Protocol. Press **n** to select none; press **b** to select BOOTP; press **d** to select DHCP. Press **Enter** after you make your selection.

Step 8 Press **ad** and then press **Enter** to select IP Address. Enter an IP address for the access point. If DHCP is not enabled for your network, the IP address you enter is the access point's static IP address. If DHCP is enabled, the address you enter provides the IP address only when no DHCP server responds with an IP address for the access point.

Step 9 Press **su** and then press **Enter** to select IP Subnet Mask. Enter an IP subnet mask to identify the subnetwork so the access point's IP address can be recognized on the LAN. If DHCP is not enabled, the subnet you enter is the static subnet mask. If DHCP is enabled, your entry provides the subnet mask only when no DHCP server responds to the access point's DHCP request.

Step 10 Press **g** and then press **Enter** to select Default Gateway. Enter the IP address of your default internet gateway. The entry 255.255.255.255 indicates no gateway.

Step 11 Press **ra** and then press **Enter** to select Radio Service Set ID (SSID). Enter an SSID for the access point. The SSID is a unique identifier that client devices use to associate with the access point. The SSID can be any alphanumeric entry from two to 32 characters long.

Step 12 Press **ro** and then press **Enter** to select Role in Radio Network. The network roles include the following options:

- Access Point/Root—Press **a** and then press **Enter** to select this setting. A wireless LAN transceiver that connects an Ethernet network with wireless client stations. Use this setting if the access point will be connected to the wired LAN.
- Repeater/Non-Root—Press **r** and then press **Enter** to select this setting. An access point that transfers data between a client and another access point. Use this setting for access points not connected to the wired LAN.
- Client/Non-root—Press **c** and then press **Enter** to select this setting. A station with a wireless connection to an access point. Use this setting for diagnostics, such as when you need to test the access point by having it communicate with another access point.

Step 13 Press **op** and then press **Enter** to select Optimize Radio Network For. These options assign either preconfigured settings or customized settings for the access point radio:

- Throughput—Press **t** and then press **Enter** to select this setting. Maximizes the data volume handled by the access point but might reduce the access point's range.
- Range—Press **r** and then press **Enter** to select this setting. Maximizes the access point's range but might reduce throughput.
- Custom—Press **c** and then press **Enter** to select this setting. The access point will use the settings you enter on the AP Radio Hardware page. Chapter 3 of the *Cisco Aironet Access Point Software Configuration Guide* describes the AP Radio Hardware page.

Step 14 Use the Ensure Compatibility With setting to automatically configure the access point to be compatible with other devices on your wireless LAN:

- 2-Mbps clients—Press **2** and then press **Enter** to select this setting. Select this setting if your network contains Cisco Aironet devices that operate at 2 Mbps.
- non-Aironet 802.11—Press **no** and then press **Enter** to select this setting. Select this setting if there are non-Cisco Aironet devices on your wireless LAN.

Step 15 Press **sn** and then press **Enter** to select SNMP Admin. Community. Enter an SNMP community name. This name automatically appears in the list of users authorized to view and make changes to the access point's management system.

You can define other SNMP communities with User Management. The "Security Setup" section in Chapter 3 of the *Cisco Aironet Access Point Software Configuration Guide* describes User Management.

Step 16 Press **ap** and press **Enter** to apply your basic settings. If you changed the Role in Radio Network setting, your access point reboots.

Default Basic Settings

Table 3-1 lists the default settings on the access point's Express Setup page.

Table 3-1 Default Settings on the Express Setup Page

Setting Name	Default Value
System Name	AIR-AP350_xxxxxx (the last six characters of the unit's MAC address)
Terminal Type (on Console interface only)	teletype
Config Server Protocol	DHCP
IP address	10.0.0.1
IP Subnet Mask	255.255.255.0
Default Gateway	255.255.255.255
SSID	tsunami
Role in Radio Network	Access Point/Root
Optimize Radio Network For	Throughput
Ensure Compatibility With	—
SNMP Admin. Community	admin

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at http://www.cisco.com/tac. Select **Wireless LAN** under Top Issues.

Sections in this chapter include:

- Checking the Top Panel Indicators
- Checking Basic Settings
- Resetting to the Default Configuration

Checking the Top Panel Indicators

If your access point is not communicating, check the three indicators on the top panel. You can use them to quickly assess the unit's status. Figure 4-1 and Figure 4-2 show the indicators, and Table 4-1 lists the meanings of the indicator signals.

Figure 4-1 Indicators on the 340 Series and 350 Series Access Point

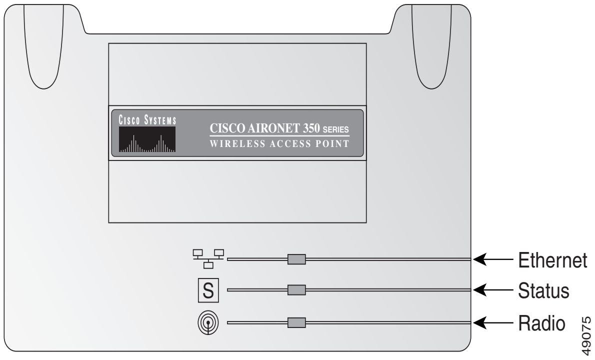
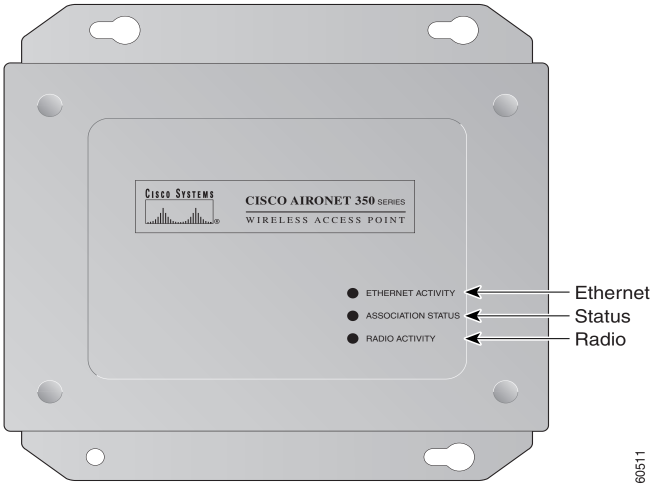


Figure 4-2 Indicators on 350 Series Metal Case Access Points



The indicators signals have the following meanings:

- The Ethernet indicator signals traffic on the wired LAN, or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.
- The status indicator signals operational status. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices. Steady green indicates that the access point is associated with a wireless client.

  For repeater access points, blinking 50% on, 50% off indicates the repeater is not associated with the root access point; blinking 7/8 on, 1/8 off indicates that the repeater is associated with the root access point but no client devices are associated with the repeater; steady green indicates that the repeater is associated with the root access point and client devices are associated with the repeater.
- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

Table 4-1 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Association status	–	Steady green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operational	–	Steady green	Blinking green	Transmitting/receiving radio packets
	Blinking green	Steady green	–	Transmitting/receiving packets.
	–	Steady green	Blinking amber	Maximum retries or buffer full occurred on the radio.
Error/warning	Blinking amber	Steady green	–	Transmit/receive errors.
	Blinking red	–	–	Ethernet cable is disconnected (340 series only).
	–	Blinking amber	–	General warning
Failure	Steady red	Steady red	Steady red	Firmware failure; disconnect power from the unit and reapply power.
Firmware upgrade	–	Steady red	–	Unit is loading new firmware.

Checking Basic Settings

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

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. The default SSID is *tsunami*.

WEP Keys

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

Refer to the "Security" section in Chapter 3 of the *Cisco Aironet Access Point Software Configuration Guide* for instructions on setting the access point's WEP keys.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you might need to completely reset the configuration. Follow the steps below to delete the current configuration and return all access point settings to the factory defaults.

Steps for Firmware Versions 11.07 or Later

Follow the steps in this section if your access point is running firmware version 11.07 or later.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. If you do not need to reset the entire configuration, use the Configuration Reset buttons on the System Configuration Setup page in the web-browser interface. Consult the *Cisco Aironet Access Point Software Configuration Guide* for more information on the reset buttons in the web-browser interface.

Step 1 Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.

Step 2 Open a terminal-emulation program on your computer.

Note These instructions describe HyperTeminal; other programs are similar.

Step 3 In the Connection Description window, enter a name and select an icon for the connection and click **OK**.

Step 4 In the Connect To window, select the port to which the cable is connected and click **OK**.

Step 5 In the Port Settings window, enter the following settings:

- **9600** baud,
- **8** data bits,
- **No** parity,
- **1** stop bit, and
- **Xon/Xoff** flow control

Step 6 Click **OK**, and press **Enter**.

Step 7 When the Summary Status screen appears, reboot the access point by unplugging the power connector and then plugging it back in.

Step 8 When the access point reboots and the Summary Status screen reappears, type **:resetall**, and press **Enter**.

Step 9 Type **yes**, and press **Enter** to confirm the command.

Note The **resetall** command is valid for only 2 minutes immediately after the access point reboots. If you do not enter and confirm the resetall command during that 2 minutes, reboot the access point again.

Step 10 After the access point reboots and the Express Setup screen appears, reconfigure the access point by using the terminal emulator or an Internet browser.

Steps for Firmware Versions 11.06 or Earlier

Follow the steps in this section if your access point is running firmware version 11.06 or earlier.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. If you do not need to reset the entire configuration, use the Configuration Reset buttons on the System Configuration Setup page in the web-browser interface. Consult the *Cisco Aironet Access Point Software Configuration Guide* for more information on the reset buttons in the web-browser interface.

Determining the Boot-Block Version

The steps you follow to reconfigure the access point depend on the version of the access point's boot block. Follow these steps to find out which boot block version is on your access point:

Step 1 Open a Telnet session to the access point.

Note You can also use these instructions while communicating with the access point through the console port or with an SNMP manager. Skip to Step 3 if you use an SNMP manager.

Step 2 Type **:cmd** and press **Enter** to switch from text-browser mode to SNMP mode.

Step 3 Type **bootblockVersion** and press **Enter**. Text appears with information about the system. If your access point's boot block version is 1.01, the text might look like this:

```
OID: iso.org.dod.internet.private.enterprises.aironet.awcVx.awcSystem.
bootblockVersion
Value [RO]: 1.01
```

Step 4 Type **exit** and press **Enter** to return to text-browser mode.

Step 5 If your boot block version is 1.01 or earlier, follow the instructions in the "Reconfiguration Steps for Boot Block Version 1.01 or Earlier" section on page 4-6. If your boot block version is 1.02 or later, follow the instructions in the "Reconfiguration Steps for Boot Block Version 1.02 or Later" section on page 4-7.

Reconfiguration Steps for Boot Block Version 1.01 or Earlier

Follow these steps to reconfigure your access point if the boot block version on your access point is version 1.01 or earlier and the firmware version on your access point is 11.06 or earlier. To find which boot block version is on your access point, follow the steps in the "Determining the Boot-Block Version" section on page 4-5.

Caution Failure to follow these instructions correctly can result in a nonoperational access point that must be returned to the factory. If your access point stops working after you attempt this procedure, contact Cisco TAC for assistance.

Step 1 Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.

Step 2 Open a terminal-emulation program on your computer.

Note These instructions describe HyperTeminal; other programs are similar.

Step 3 In the Connection Description window, enter a name and select an icon for the connection and click **OK**.

Step 4 In the Connect To window, select the port to which the cable is connected and click **OK**.

Step 5 In the Port Settings window, make the following settings: **9600** baud, **8** data bits, **No** parity, **1** stop bit, and **Xon/Xoff** flow control.

Step 6 Click **OK** and press **Enter** three times.

Step 7 When the Summary Status screen appears, reboot the access point by unplugging the power connector and then plugging it back in, or by pressing **Ctrl-X**.

Step 8 When the message "Type <esc> within 5 seconds for menu" appears, press **Esc**.

Step 9 Write down the list of files for future reference.

Caution Perform the next six steps carefully to avoid accidentally deleting the installation key files or the firmware files. You must carefully note the file selection letters, because they change during the following steps. If you forget to copy the access point's installation key file to DRAM in Step 10, or if you do not copy it back to configuration memory in Step 13, your access point will stop functioning.

Step 10 Copy the access point's installation key file to the access point's DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file called *AP Installation Key*.

Step 11 If the list of configuration files contains a file called *VAR Installation Key*, copy that file to DRAM along with the AP Installation Key. Copy the VAR installation key file to DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file called *VAR Installation Key*.

Caution Make sure you select the Configuration memory bank for formatting in Step 12. If you accidentally format a different memory bank your access point will stop functioning.

Step 12 Reformat the access point's configuration memory bank by pressing **!** to select **FORMAT memory bank**, then **2** to select **Config**, then upper-case **Y** to confirm the **FORMAT** command.

Step 13 Copy the installation key back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the AP Installation Key.

Step 14 If you copied a VAR installation key to DRAM in Step 11, copy it back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *VAR Installation Key*. If the access point does not have a VAR installation key file, skip to Step 15.

Step 15 Run the access point firmware by pressing **r** to select **Run**, then the selection letter for the firmware file which is displayed. The message "Inflating [firmware file name]" appears while the access point starts the firmware.

Step 16 When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.

Reconfiguration Steps for Boot Block Version 1.02 or Later

Follow these steps to reconfigure your access point if the boot block version on your access point is version 1.02 or later and the firmware version on your access point is 11.06 or earlier. To find which boot block version is on your access point, follow the steps in the "Determining the Boot-Block Version" section on page 4-5.

Caution Failure to follow these instructions correctly can result in a nonoperational access point that must be returned to the factory. If your access point stops working after you attempt this procedure, contact Cisco TAC for assistance.

Step 1 Use a straight-through cable with 9-pin male to 9-pin female connectors to connect the COM 1 or COM 2 port on your computer to the RS-232 port on the access point.

Step 2 Open a terminal-emulation program on your computer.

Note These instructions describe HyperTerminal; other programs are similar.

Step 3 In the Connection Description window, enter a name and select an icon for the connection and click **OK**.

Step 4 In the Connect To window, select the port to which the cable is connected and click **OK**.

Step 5 In the Port Settings window, make the following settings: **9600** baud, **8** data bits, **No** parity, **1** stop bit, and **Xon/Xoff** flow control.

Step 6 Click **OK** and press **Enter**.

Step 7 When the Summary Status screen appears, reboot the access point by pressing **Ctrl-X** or by unplugging the power connector and then plugging it back in.

Step 8 When the memory files are listed under the heading "Memory:File," press **Ctrl-W** within 5 seconds to reach the boot block menu.

Step 9 Write down the list of files for future reference.

⚠ **Caution** Perform the next six steps carefully to avoid accidently deleting the installation key files or the firmware files. You must carefully note the file selection letters, because they change during the following steps. If you forget to copy the access point's installation key file to DRAM in Step 10, or if you do not copy it back to configuration memory in Step 13, your access point will stop functioning.

Step 10 Copy the access point's AP Installation Key to the access point's DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file *AP Installation Key*.

Step 11 If the list of configuration files contains a file called *VAR Installation Key*, you must copy that file to DRAM along with the AP Installation Key file. If the access point does not have a VAR installation key file, skip to Step 12.

⚠ **Caution** If you forget to copy the access point's VAR installation key file to DRAM in Step 11, or if you do not copy it back to configuration memory in Step 14, your access point will stop functioning.

Copy the VAR Installation Key to DRAM by pressing **c** to select **Copy file**, then **1** to select **DRAM**, then the selection letter for the file *VAR Installation Key*.

Step 12 Reformat the access point's configuration memory bank by pressing **Ctrl-Z** to reach the reformat menu. When the menu appears, press **!** to select **FORMAT memory bank**, then **2** to select **Config**, then upper-case **Y** to confirm the **FORMAT** command.

⚠ **Caution** Make sure you select the Configuration memory bank for formatting. If you accidentally format a different memory bank your access point will stop functioning.

Step 13 Copy the installation key back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *AP Installation Key*.

Step 14 If you copied a VAR installation key to DRAM in Step 11, copy it back to the configuration memory bank by pressing **c** to select **Copy file**, then **2** to select **Config**, then the selection letter for the file *VAR Installation Key*. If the access point does not have a VAR installation key file, skip to Step 15.

Step 15 Run the access point firmware by pressing **r** to select **Run**, then the selection letter for the firmware file that is displayed. The message "Inflating [firmware file name]" appears while the access point starts the firmware.

Step 16 When the Express Setup screen appears, begin reconfiguring the access point using the terminal emulator or an Internet browser.

APPENDIX A

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.

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.**

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

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

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

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

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

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

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

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

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

Lightning Activity Warning

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

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.**

Installation Warning

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

Waarschuwing **Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.**

Varoitus **Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.**

Attention **Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.**

Warnung **Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.**

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 sua fonte de energia.**

¡Advertencia! **Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.**

Varning! **Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.**

Circuit Breaker (15A) Warning

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).**

Waarschuwing **Dit produkt is afhankelijk van de installatie van het gebouw voor kortsluit- (overstroom)beveiliging. Controleer of er een zekering of stroomverbreker van niet meer dan 120 Volt wisselstroom, 15 A voor de V.S. (240 Volt wisselstroom, 10 A internationaal) gebruikt wordt op de fasegeleiders (alle geleiders die stroom voeren).**

Varoitus **Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että vaihevirtajohtimissa (kaikissa virroitetuissa johtimissa) käytetään Yhdysvalloissa alle 120 voltin, 15 ampeerin ja monissa muissa maissa 240 voltin, 10 ampeerin sulaketta tai suojakytkintä.**

Attention **Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 10 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).**

Warnung **Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240 V Wechselstrom, 10 A (bzw. in den USA 120 V Wechselstrom, 15 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.**

Avvertenza **Questo prodotto dipende dall'installazione dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Verificare che un fusibile o interruttore automatico, non superiore a 120 VCA, 15 A U.S. (240 VCA, 10 A internazionale) sia stato usato nei fili di fase (tutti i conduttori portatori di corrente).**

Advarsel **Dette produktet er avhengig av bygningens installasjoner av kortslutningsbeskyttelse (overstrøm). Kontroller at det brukes en sikring eller strømbryter som ikke er større enn 120 VAC, 15 A (USA) (240 VAC, 10 A internasjonalt) på faselederne (alle strømførende ledere).**

Aviso **Este produto depende das instalações existentes para protecção contra curto-circuito (sobrecarga). Assegure-se de que um fusível ou disjuntor não superior a 240 VAC, 10A é utilizado nos condutores de fase (todos os condutores de transporte de corrente).**

¡Advertencia! **Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) deló propio edificio. Asegurarse de que se utiliza un fusible o interruptor automático de no más de 240 voltios en corriente alterna (VAC), 10 amperios del estándar internacional (120 VAC, 15 amperios del estándar USA) en los hilos de fase (todos aquéllos portadores de corriente).**

Varning! **Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att säkring eller överspänningsskydd används på fasledarna (samtliga strömförande ledare) för internationellt bruk max. 240 V växelström, 10 A (i USA max. 120 V växelström, 15 A).**

Power Injector Warning

Warning

The Cisco Aironet power injector is designed for use with Cisco Aironet 350 series access points and 350 series wireless bridges only. Using the power injector with other Ethernet-ready devices can damage the equipment.

Waarschuwing

De stroominjector van Cisco Aironet is uitsluitend ontworpen voor gebruik met toegangspunten en draadloze bruggen van de 350-serie van Ciso Aironet. Als u de stroominjector gebruikt met andere apparaten die geschikt zijn voor gebruik met het Ethernet, kunt u de apparatuur beschadigen.

Varoitus

Cisco Aironet Power Injector on suunniteltu käytettäväksi ainoastaan Cisco Aironet 350 -sarjan access point -tukiasemien sekä 350-sarjan langattomien siltojen kanssa. Jännitteensyöttöyksikön käyttäminen muiden Ethernet-valmiiden laitteiden kanssa voi vahingoittaa laitteistoa.

Attention

L'injecteur d'alimentation en ligne Cisco Aironet a été conçu pour être utilisé uniquement avec des points d'accès et des ponts sans fil Cisco Aironet 350. L'utilisation de l'injecteur avec d'autres périphériques compatibles Ethernet risque d'endommager l'appareil.

Warnung

Die Cisco Aironet-Einspeiseweiche sollte nur mit den Zugangspunkten der Cisco Aironet 350-Serie und den drahtlosen Bridges der 350-Serie verwendet werden. Die Verwendung der Einspeiseweiche mit anderen Ethernet-fähigen Geräten kann zu Schäden am Gerät führen.

Avvertenza

Il dispositivo per l'alimentazione di Cisco Aironet è ideato per l'utilizzo esclusivo con punti di accesso e bridge wireless Cisco Aironet 350 Series. L'utilizzo del dispositivo di alimentazione con altri dispositivi Ethernet potrebbe danneggiare l'apparecchiatura.

Advarsel

Cisco Aironet Power Injector er bare utviklet for bruk sammen med Cisco Aironet 350-serien av tilgangspunkter og 350-serien av trådløse broer. Bruk av strømforsyningen med andre Ethernet-forberedte enheter kan skade utstyret.

Aviso

O injector de potência da Cisco Aironet foi concebido para utilização exclusiva com os pontos de acesso 350 Series e as pontes sem fios 350 Series da Cisco Aironet. A utilização do injector de potência com outros dispositivos preparados para a Ethernet pode danificar o equipamento.

¡Advertencia! **El dispositivo de alimentación Aironet de Cisco está diseñado para ser utilizado únicamente con puntos de acceso y puentes inalámbricos de la serie Aironet 350 de Cisco. Si se utiliza con otros dispositivos para Ethernet, el equipo puede dañarse.**

Varning! **Cisco Aironets strömförsörjningsenhet är utformad för att endast användas med Cisco Aironets åtkomstpunkter ur 350-serien och trådlösa bryggor ur 350-serien. Om du använder enheten med något annat Ethernet-anpassat hjälpmedel kan utrustningen skadas.**

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for Cisco Aironet access points.

This appendix contains the following sections:

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

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Tested To Comply
With FCC Standards

FOR HOME OR OFFICE USE

Models:

AIR-AP340, AIR-AP341, AIR-AP342, AIR-AP352

FCC Certification number:

LDK102035 (AIR-AP34x),
LDK102040 (AIR-AP35x)

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.

Department of Communications – Canada

Canadian Compliance Statement

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

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

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

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

The device is certified to the requirements of RSS-139-1 and 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 entsprecheneden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Directiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directive 1999/5/EC.
Έλληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigencies essentialles et aux autres dispositions pertinantes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.
Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-directiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

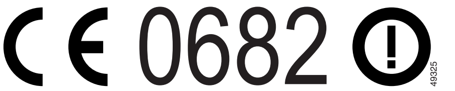
This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The Declaration of Conformity related to this product can be found at the following URL: http://www.ciscofax.com

For the 340 series, the following standards were applied:

- Radio: ETS 300.328
- EMC: ETS 300.826
- Safety: EN 60950

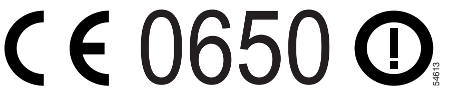
The following CE mark is affixed to the 340 series equipment:



For the 350 series, 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 350 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.

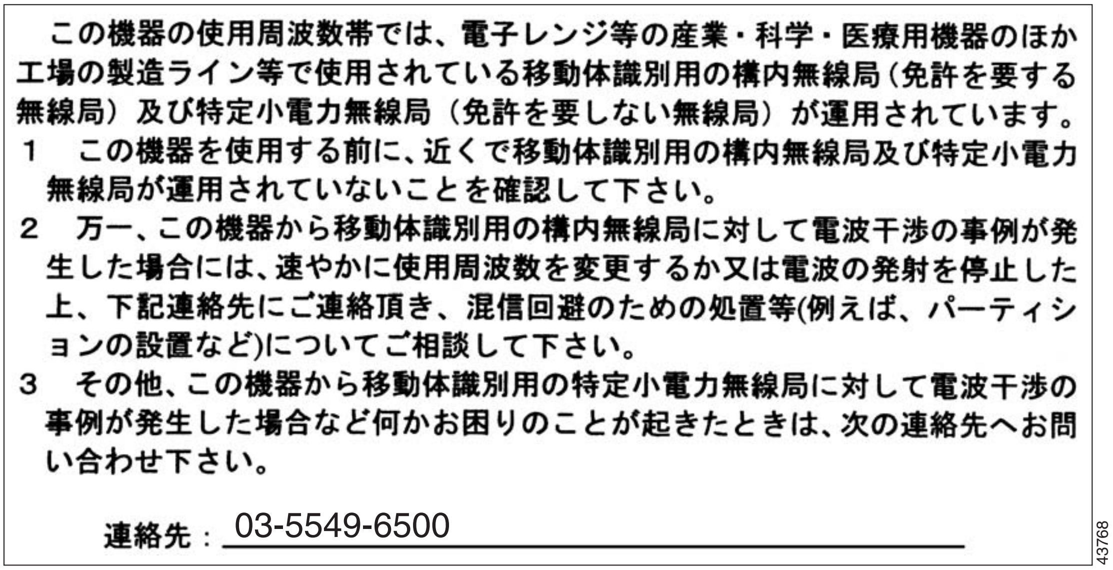
Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

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

English Translation

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

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

Contact Number: 03-5549-6500

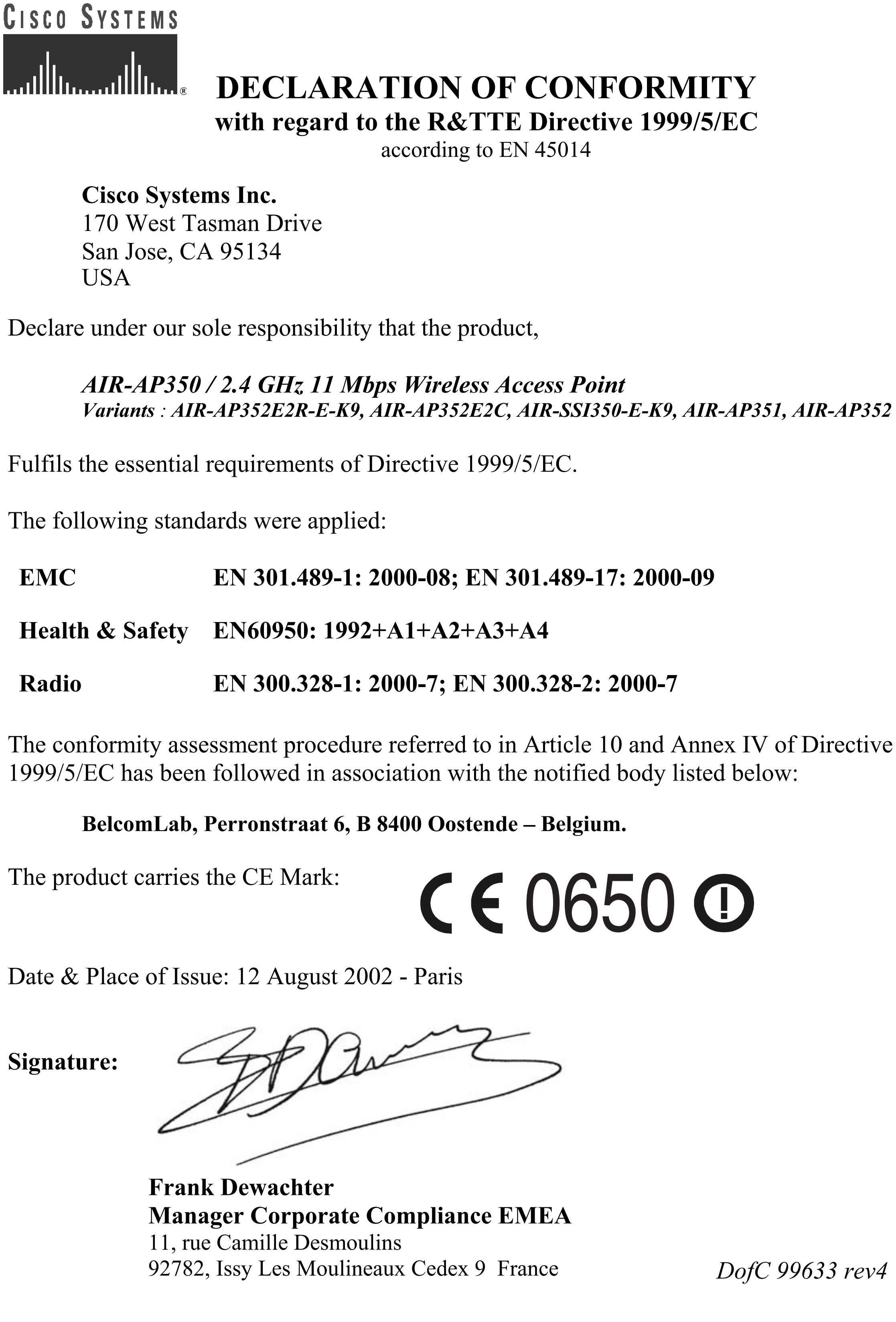
Declaration of Conformity Statements

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

http://www.ciscofax.com

Declaration of Conformity Statement for European Union Countries

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



CISCO SYSTEMS

DECLARATION OF CONFORMITY

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

according to EN 45014

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

Declare under our sole responsibility that the product,

AIR-AP350 / 2.4 GHz 11 Mbps Wireless Access Point
Variants : AIR-AP352E2R-E-K9, AIR-AP352E2C, AIR-SSI350-E-K9, AIR-AP351, AIR-AP352

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

The following standards were applied:

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

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

BelcomLab, Perronstraat 6, B 8400 Oostende – Belgium.

The product carries the CE Mark: CE 0650 (!)

Date & Place of Issue: 12 August 2002 - Paris

Signature:

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

DofC 99633 rev4

INDEX