Cisco Aironet Wireless LAN Client Adapters
Installation and Configuration Guide
for Windows CE

340 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

Customer Order Number:
Text Part Number: OL-1375-02
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

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

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

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

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

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

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

CCIP, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigatStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)
CONTENTS

Preface vii
  Audience viii
  Purpose viii
  Organization viii
  Conventions ix
  Related Publications xi
  Obtaining Documentation xi
    World Wide Web xi
    Documentation CD-ROM xi
    Ordering Documentation xii
    Documentation Feedback xii
  Obtaining Technical Assistance xii
    Cisco.com xii
    Technical Assistance Center xiii
    Cisco TAC Web Site xiii
    Cisco TAC Escalation Center xiv

CHAPTER 1

Product Overview 1-1
  Introduction to the Client Adapters 1-2
    Terminology 1-2
  Hardware Components 1-3
    Radio 1-3
    Radio Antenna 1-3
    LEDs 1-3
  Software Components 1-4
    Radio Firmware 1-4
    Driver 1-4
    Client Utilities 1-4
      Overview of the Client Utilities 1-5
      Buttons on the Client Utility Screens 1-5
  Network Configurations Using the Client Adapter 1-6
    Ad Hoc Wireless LAN 1-6
    Wireless Infrastructure with Workstations Accessing a Wired LAN 1-7
CHAPTER 5
Advanced Configuration 5-1
Configuring Your Client Adapter 5-2

CHAPTER 6
Performing Diagnostics 6-1
Overview of the Diagnostic Utilities 6-2
Viewing the Current Status of Your Client Adapter 6-2
Viewing Statistics for Your Client Adapter 6-3

CHAPTER 7
Routine Procedures 7-1
Inserting and Removing a PC Card 7-2
Inserting a PC Card into a Windows CE Device 7-2
Removing a PC Card from a Windows CE Device 7-2
Upgrading the Client Adapter Software 7-3
Upgrading the Firmware 7-3
Determining the Firmware Version 7-3
Loading New Firmware 7-4
Upgrading the Driver and Client Utilities 7-5
Determining the Driver and Client Utility Versions 7-6
Uninstalling the Current Driver and Client Utilities 7-6
Loading a New Driver and Client Utilities 7-7
Client Utility Procedures 7-12
Opening a Client Utility 7-12
Exiting a Client Utility 7-12
Determining the Version of a Client Utility 7-12
Deleting Client Utility Icons on HPC Devices 7-12
Restarting the Client Adapter 7-13

CHAPTER 8
Troubleshooting 8-1
Accessing the Latest Troubleshooting Information 8-2
Interpreting the Indicator LEDs 8-2
Troubleshooting the Client Adapter 8-3
Problems Obtaining an IP Address 8-3
Problems Associating to an Access Point 8-3
Problems Authenticating to an Access Point 8-4
Problems Connecting to the Network 8-4
Error Messages 8-4
Preface

The preface provides an overview of the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary.

The following topics are covered in this section:

- Audience, page viii
- Purpose, page viii
- Organization, page viii
- Conventions, page ix
- Related Publications, page xi
- Obtaining Documentation, page xi
- Obtaining Technical Assistance, page xii
Audience

This publication is for the person responsible for installing, configuring, and maintaining a Cisco Aironet 340 or 350 Series Wireless LAN Client Adapter on a Windows CE device. This person should be familiar with computing devices and with network terms and concepts.

Purpose

This publication describes the client adapters in the 340 and 350 series and explains how to install, configure, and troubleshoot them.

Organization

This publication is organized into the following chapters:

- **Chapter 1, “Product Overview,”** describes the hardware and software components of the client adapters and illustrates two common network configurations.
- **Chapter 2, “Preparing for Installation,”** provides information that you need to know before installing a client adapter, such as safety information and system requirements.
- **Chapter 3, “Installing the Client Adapter,”** provides instructions for installing the driver and client utilities as well as setting basic configuration parameters.
- **Chapter 4, “Enabling Security Features,”** explains how to use the client utilities to enable the client adapter’s security features.
- **Chapter 5, “Advanced Configuration,”** explains how to set the client adapter’s advanced configuration parameters.
- **Chapter 6, “Performing Diagnostics,”** explains how to use the client utilities to assess the performance of the client adapter.
- **Chapter 7, “Routine Procedures,”** provides procedures for common tasks related to the client adapter, such as updating client software and restarting the adapter.
- **Chapter 8, “Troubleshooting,”** provides information for diagnosing and correcting common problems encountered when installing or operating a client adapter.
- **Appendix A, “Technical Specifications,”** lists the physical, radio, power, and regulatory specifications for the client adapters.
- **Appendix B, “Translated Safety Warnings,”** provides translations of the client adapter’s safety warnings in nine languages.
- **Appendix C, “Declarations of Conformity and Regulatory Information,”** provides conformity and regulatory information for the client adapters.
- **Appendix D, “Channels, Power Levels, and Antenna Gains,”** lists the channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.
- **Appendix E, “Performing a Site Survey,”** shows people who are responsible for conducting a site survey how they can use the client utilities to determine the best placement for infrastructure devices within a wireless network.
Conventions

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

- Commands and keywords are in **boldface**.
- Variables are in *italics*.
- Configuration parameters are capitalized.
- Notes, cautions, and warnings use the following conventions and symbols:

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

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

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

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

  **Varoitus**
  Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkööytäntöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännettäkset löydät litiiteestä ”Translated Safety Warnings” (käännettyt turvallisuutta koskevat varoitukset).)

  **Attention**
Preface

Conventions

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

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

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

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

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

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

For more information about Cisco Aironet Wireless LAN Client Adapters and related products, refer to the following publications:

- *Release Notes for Cisco Aironet Client Utilities and Drivers for Windows CE*
- *Release Notes for Cisco Aironet Client Adapter Firmware*
- *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows*
- *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Linux*
- *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Mac OS*
- *Quick Start Guide: Cisco Aironet Access Points*
- *Cisco Aironet Access Point Hardware Installation Guide*
- *Cisco Aironet Access Point Software Configuration Guide*
- *Release Notes for Cisco Aironet Access Points*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:


Documentation CD-ROM

Other Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped separately from the Cisco Aironet Wireless LAN Client Adapters CD that shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.
Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
  
  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
  
  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the Fax or Email option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.
Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:


Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.
Product Overview

This chapter describes the Cisco Aironet 340 and 350 Series Wireless LAN Client Adapters and illustrates their role in a wireless network.

The following topics are covered in this chapter:

- Introduction to the Client Adapters, page 1-2
- Hardware Components, page 1-3
- Software Components, page 1-4
- Network Configurations Using the Client Adapter, page 1-6
Introduction to the Client Adapters

The Cisco Aironet 340 and 350 Series Wireless LAN Client Adapters are 30- and 100-milliwatt (mW) radio modules that provide transparent wireless data communications between fixed, portable, or mobile devices and other wireless devices or a wired network infrastructure. The client adapters are fully compatible when used in devices supporting Plug-and-Play (PnP) technology.

The primary function of the client adapters is to transfer data packets transparently through the wireless infrastructure through an access point connected to a wired LAN. The adapters operate similarly to a standard network product except that the cable is replaced with a radio connection and an access point is required to make the connection to the wire. No special wireless networking functions are required, and all existing applications that operate over a network can operate using the adapters.

This document covers two types of client adapters:

- **PC card** (model number: AIR-PCM3xx) – A PCMCIA card radio module that can be inserted into any device equipped with an *external* Type II or Type III PC card slot. Host devices can include laptops, notebook computers, personal digital assistants, and handheld or portable devices.

- **LM card** (model number: AIR-LMC3xx) – A PCMCIA card radio module that can be inserted into any device equipped with an *internal* Type II or Type III PC card slot. Host devices usually include handheld or portable devices.

**Note**

The first x in the product model number represents the client adapter series (340 or 350). The second x indicates the wired equivalent privacy (WEP) level of the card, where 0 = no WEP capability, 1 = 40-bit WEP, and 2 = 128-bit WEP. However, if the second x is a 0 but the model number contains K9, the card is 128-bit WEP capable.

Terminology

The following terms are used throughout this document:

- **client adapter** – Refers to both PC cards and LM cards.
- **PC card** or **LM card** – Refers to only a specific adapter.
- **workstation** (or **station**) – Refers to a computing device with an installed client adapter.
- **infrastructure device** – Refers to a device that connects client adapters to a wired LAN, such as an access point, bridge, or base station. Throughout this document, **access point** is used to represent infrastructure devices in general.
Hardware Components

The client adapter has three major hardware components: a radio, a radio antenna, and two LEDs.

Radio

The 340 and 350 series client adapters contain a direct-sequence spread spectrum (DSSS) radio that operates in the 2.4-GHz license-free Industrial Scientific Medical (ISM) band. The radio transmits data over a half-duplex radio channel operating at up to 11 Mbps.

DSSS technology distributes a radio signal over a wide range of frequencies and then returns the signal to the original frequency range at the receiver. The benefit of this technology is its ability to protect the data transmission from interference. For example, if a particular frequency encounters noise or interference or both, enough redundancy is built into the signal on other frequencies that the client adapter usually will still be successful in its transmission.

Radio Antenna

The type of antenna used depends on your client adapter:

- PC cards have an integrated, permanently attached diversity antenna. The benefit of the diversity antenna system is improved coverage. The system works by allowing the card to switch and sample between its two antenna ports in order to select the optimum port for receiving data packets. As a result, the card has a better chance of maintaining the radio frequency (RF) connection in areas of interference. The antenna is housed within the section of the card that hangs out of the PC card slot when the card is installed.
- LM cards are shipped without an antenna; however, an antenna can be connected through the card’s external connector.

Note

External antennas used in combination with a power setting resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are not allowed for use within the European community and other countries that have adopted the European R&TTE directive or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas in those countries, refer to the “Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC” section on page C-4 and the “Maximum Power Levels and Antenna Gains” section on page D-3.

LEDs

The client adapter has two LEDs that glow or blink to indicate the status of the adapter or to convey error messages. Refer to the Chapter 8 for an interpretation of the LED codes.
Software Components

The client adapter has three major software components: radio firmware, a driver, and client utilities.

Radio Firmware

The firmware, which is contained in the client adapter’s Flash memory, controls the adapter’s radio. The client adapter is shipped with the firmware installed; however, a more recent version of the firmware may be available from Cisco.com.

Note Cisco recommends using the most current version of radio firmware. Chapter 7 provides instructions for determining the version of your client adapter’s firmware and upgrading it if necessary.

Driver

The driver provides an interface between the Windows CE device and the client adapter, thereby enabling Windows CE and the applications it runs to communicate with the adapter. The driver is provided on the Cisco Aironet Wireless LAN Client Adapters CD that shipped with the client adapter and must be installed before the adapter can be used. Chapter 3 provides instructions for installing the driver.

Note The CD has the latest version of the driver available at the time of pressing; however, a more recent version of the driver may be available from Cisco.com. Cisco recommends installing the most current version of the driver. Chapter 3 provides instructions for installing the driver from either location.

Client Utilities

The client utilities are optional applications that interact with the radio firmware to adjust client adapter settings and display information about the adapter. The client utilities and online help files are installed with the driver.

Note The CD has the latest version of the client utilities available at the time of pressing; however, a more recent version of the client utilities may be available from Cisco.com. Cisco recommends installing the most current version of the client utilities. Chapter 3 provides instructions for installing the client utilities from either location.
Overview of the Client Utilities

Table 1-1 lists the client utilities supported by Windows CE, describes their function, and indicates the chapter where they are explained.

Table 1-1   Overview of the Client Utilities

<table>
<thead>
<tr>
<th>Client Utility</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aironet Client Utility (ACU)</td>
<td>Configures your client adapter for use in a wireless network and enables the adapter’s security features</td>
<td>Chapter 4 and Chapter 5</td>
</tr>
<tr>
<td>Cisco Link Status (CLS)</td>
<td>Enables you to view the current status of your client adapter</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>Client Encryption Manager (CEM)</td>
<td>Enables you to set a static Wired Equivalent Privacy (WEP) key for your client adapter</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>Client Statistics Utility (CSU)</td>
<td>Enables you to view statistics that indicate how data is being received and transmitted by your client adapter</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>Load New Firmware (LNF)</td>
<td>Enables you to load new firmware for your client adapter</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>Site Survey Tool (SST)</td>
<td>Enables people responsible for conducting a site survey to determine the best placement for infrastructure devices within a wireless network</td>
<td>Appendix E</td>
</tr>
<tr>
<td>Wireless Login Module (WLM)</td>
<td>Enables you to set a LEAP username and password to be used to authenticate to a RADIUS server</td>
<td>Chapter 4</td>
</tr>
</tbody>
</table>

Buttons on the Client Utility Screens

The buttons on the client utility screens are used to perform specific functions. Table 1-2 describes the most common buttons.

Table 1-2   Buttons on the Client Utility Screens

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About</td>
<td>Displays the version of the client utility</td>
</tr>
<tr>
<td>Cancel</td>
<td>Exits the screen without saving any changes</td>
</tr>
<tr>
<td>Defaults</td>
<td>Displays the default value of each parameter</td>
</tr>
<tr>
<td>OK</td>
<td>Saves any changes and exits the screen</td>
</tr>
<tr>
<td>Start</td>
<td>Initiates a test</td>
</tr>
<tr>
<td>Stop</td>
<td>Stops a test that is running</td>
</tr>
<tr>
<td>X</td>
<td>Exits the screen without saving any changes</td>
</tr>
<tr>
<td>? (available on HPCs only)</td>
<td>Provides information on the screen and its parameters</td>
</tr>
</tbody>
</table>
Network Configurations Using the Client Adapter

The client adapter can be used in a variety of network configurations. In some configurations, access points provide connections to your network or act as repeaters to increase wireless communication range. The maximum communication range is based on how you configure your wireless network.

This section describes and illustrates the two most common network configurations:

- Ad hoc wireless local area network (LAN)
- Wireless infrastructure with workstations accessing a wired LAN

For examples of more complex network configurations involving client adapters and access points, refer to the *Cisco Aironet Access Point Hardware Installation Guide*.

**Note** Refer to Chapter 5 for information on setting the client adapter’s network mode.

Ad Hoc Wireless LAN

An ad hoc (or peer-to-peer) wireless LAN (see Figure 1-1) is the simplest wireless LAN configuration. In a wireless LAN using an ad hoc network configuration, all devices equipped with a client adapter can be linked together and communicate directly with each other.

*Figure 1-1  Ad Hoc Wireless LAN*
Wireless Infrastructure with Workstations Accessing a Wired LAN

A microcellular network can be created by placing two or more access points on a LAN. Figure 1-2 shows a microcellular network with workstations accessing a wired LAN through several access points. This configuration is useful with portable or mobile stations because it allows them to be directly connected to the wired network even while moving from one microcell domain to another. This process is transparent, and the connection to the file server or host is maintained without disruption. The mobile station stays connected to an access point as long as it can. However, once the transfer of data packets needs to be retried or beacons are missed, the station automatically searches for and associates to another access point. This process is referred to as seamless roaming.

Figure 1-2  Wireless Infrastructure with Workstations Accessing a Wired LAN
Preparing for Installation

This chapter provides information that you need to know before installing a client adapter. The following topics are covered in this chapter:

- Safety information, page 2-2
- Unpacking the Client Adapter, page 2-3
- System Requirements, page 2-4
- Site Requirements, page 2-5
Safety information

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

FCC Safety Compliance Statement

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

Safety Guidelines

- Do not touch or move the antenna while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 12 inches (30 cm) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.
Warnings

Observe the following warnings when operating the client adapter:

<table>
<thead>
<tr>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to comply with FCC radio frequency (RF) exposure limits, dipole antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to comply with RF exposure limits established in the ANSI C95.1 standards, it is recommended when using a laptop with a PC card client adapter that the adapter’s integrated antenna is positioned more than 2 inches (5 cm) from your body or nearby persons during extended periods of transmitting or operating time. If the antenna is positioned less than 2 inches (5 cm) from the user, it is recommended that the user limit exposure time.</td>
</tr>
</tbody>
</table>

Translated versions of these safety warnings are provided in Appendix B.

Unpacking the Client Adapter

Follow these steps to unpack the client adapter:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open the shipping container and carefully remove the contents.</td>
</tr>
<tr>
<td>2</td>
<td>Return all packing materials to the shipping container and save it.</td>
</tr>
<tr>
<td>3</td>
<td>Ensure that all items listed in the “Package Contents” section below are included in the shipment. Check each item for damage.</td>
</tr>
</tbody>
</table>

Note

If any item is damaged or missing, notify your authorized Cisco sales representative. Any remote antenna and its associated wiring are shipped separately.

Package Contents

Each client adapter is shipped with the following items:

- Quick Start Guide: Cisco Aironet Wireless LAN Client Adapters
- Cisco Aironet Wireless LAN Client Adapters CD
- Cisco product registration card
System Requirements

In addition to the items shipped with the client adapter, you will also need the following in order to install and use the adapter:

- One of the following Windows CE devices equipped with a Type II or Type III PC card slot:
  - Handheld PC (HPC) running Windows CE 2.11 with an ARM, StrongARM, Mips, SH3, SH4, or x86 processor
  - Handheld PC (HPC) running Windows CE 3.0 with an ARM, StrongARM, Mips, SH4, or x86 processor
  - Pocket PC (PPC) running Windows CE 3.0 with an ARM, StrongARM, Mips, or SH3 processor

  **Note**
  All drivers and supporting software (Card and Socket Services) for the PC card slot must be loaded and configured.

- Laptop or PC with a CD-ROM drive and running a Windows operating system and ActiveSync
- Serial or USB connection to the Windows CE device
- The following information from your system administrator:
  - The logical name for your Windows CE device (also referred to as \textit{client name})
  - The case-sensitive service set identifier (SSID) for your RF network
  - The primary and secondary Domain Name System (DNS) and Windows Internet Name Service (WINS) to be assigned to your Windows CE device
  - If your Windows CE device is not connected to a DHCP server, the IP address, subnet mask, and default gateway address to be assigned to your device
  - The Wired Equivalent Privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security
  - The username and password for your RADIUS server account, if your wireless network uses server-based authentication
Site Requirements

This section discusses the site requirements for both infrastructure and client devices.

For Infrastructure Devices

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Therefore, before you install any wireless infrastructure devices (such as access points, bridges, and base stations, which connect your client adapters to a wired LAN), a site survey must be performed to determine the optimum placement of these devices to maximize range, coverage, and network performance. Appendix E, which is provided for people who are responsible for conducting a site survey, explains how the Site Survey Tool (SST) client utility can be used to determine the best placement for infrastructure devices within a wireless network.

Note

As a rule, infrastructure devices are installed and initially configured prior to client devices.

For Client Devices

Because the client adapter is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

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

This chapter provides instructions for installing the client adapter driver and the client utilities. The following topics are covered in this chapter:

- Determining the Windows CE Version, page 3-2
- Determining the Latest Driver and Client Utility Versions, page 3-2
- Installing the Driver and Client Utilities, page 3-3
- Installing the Driver and Client Utilities on Other Windows CE Devices, page 3-8
- Verifying Installation, page 3-8
Determining the Windows CE Version

When you install the driver for your client adapter, you need to know which version of Windows CE your device is running because the Cisco Aironet drivers are specific to different versions of Windows CE. Follow the instructions below to determine the version of Windows CE that your device is using.

- If your Windows CE device is a Pocket PC (PPC) device, select Start > Settings > the System tab > About. The Windows CE version is displayed.
- If your Windows CE device is a Handheld PC (HPC) device, select Start > Settings > Control Panel > System; then select the System tab. The core system version indicates the version of Windows CE that the device is running (such as 2.11).

Determining the Latest Driver and Client Utility Versions

The driver and client utilities are provided on the Cisco Aironet Wireless LAN Client Adapters CD that shipped with the client adapter; however, a more recent version of both may be available from Cisco.com. Cisco recommends installing the most current versions of the driver and client utilities. Follow the steps below to determine the most recent version of the driver and client utilities on your CD and Cisco.com.

Step 1
To determine the version of the driver and client utilities on the Cisco Aironet Wireless LAN Client Adapters CD, open the FileList.txt file on the CD’s root directory. This file lists the version numbers for all of the software files provided on the CD.

Note
If the FileList.txt file is not present on the root directory, your CD is obsolete, and more recent versions of the software are available on Cisco.com. Go to the “Installing the Driver and Client Utilities” section on page 3-3.

Step 2
To determine the latest driver and client utility versions available on Cisco.com, follow the steps below:

a. Use your computer’s web browser to access the following URL:
b. Locate the section for client adapter drivers and utilities.
c. Click the link for Windows CE 2.11 or 3.0, depending on which version of Windows CE your device is running.
d. Look at the release numbers of the driver and client utilities in the description below the filename. These are the latest available versions on Cisco.com.

Step 3
Go to the “Installing the Driver and Client Utilities” section on page 3-3. If the driver or client utility version on Cisco.com is greater than the version on the CD, follow the instructions for installing the driver and client utilities from Cisco.com.
Installing the Driver and Client Utilities

The WinCE2.11-PCM-LMC-vx.xx.exe and WinCE3.0-PCM-LMC-vx.xx.exe files, which are used to install the driver and client utilities, consist of individual *.cab files. Each *.cab file contains the driver, client utility, and online help files for a specific Windows CE CPU/device combination. When the *.exe file is executed, all of the *.cab files are extracted, and the *.cab file specific to the attached Windows CE device is copied to the device.

Follow the steps below to install the driver and client utilities for your client adapter.

---

**Note**  
This procedure is meant to be used the first time the driver and client utilities are installed on a Windows CE device. If Cisco Aironet client adapter software is already installed on your Windows CE device, follow the instructions in Chapter 7 to first uninstall any existing software and then to upgrade to new software.

---

**Note**  
The driver and client utilities must be installed before you insert a client adapter into a Windows CE device.

---

**Step 1**  
Use a serial or USB cable to connect your Windows CE device to a laptop or PC running Microsoft ActiveSync. A message appears on the Windows CE device indicating that it is connecting to the host. After the Windows CE device is connected, the New Partnership window appears on the laptop or PC. This window asks if you want to set up a partnership.

---

**Note**  
Cisco recommends that you install the latest version of ActiveSync.

---

**Step 2**  
Perform one of the following:

- If you want to establish a partnership that allows you to synchronize files between the laptop or PC and the Windows CE device, select Yes, click Next, and follow the instructions on the screen to specify the files to be synchronized and to finish setting up the partnership.
- If you do not want to synchronize files and want to connect as a “guest,” select No and click Next. The screen indicates that you are connected as a guest.

---

**Step 3**  
Perform one of the following:

- If you are installing the driver and client utilities from the Cisco Aironet Wireless LAN Client Adapters CD that shipped with the client adapter, follow the steps below:
  a. Insert the CD into the laptop or PC’s CD-ROM drive.
  b. Use Windows Explorer to access the WinCE directory.
  c. Select the folder for your version of Windows CE (CE211 or CE300).
  d. Go to Step 4.
- If you are installing the driver and client utilities from Cisco.com, follow the steps below:
  a. Use the laptop or PC’s web browser to access the following URL:  
  b. Locate the section for client adapter drivers and utilities.
Installing the Client Adapter

Chapter 3

Installing the Driver and Client Utilities

c. Click the link for Windows CE 2.11 or 3.0, depending on which version of Windows CE your device is running.
e. Read and accept the terms and conditions of the Software License Agreement.
f. Select the WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe file to download it.
g. Save the file to a floppy disk or to the hard drive of your laptop or PC.
h. Use Windows Explorer to locate the saved file.
i. Go to Step 4.

Step 4

Double-click the *.exe file for your version of Windows CE (WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe). The application creates an Install directory under the ActiveSync directory, extracts the .cab files contained in the *.exe file, and copies them to the Install directory.

Note: All of the *.cab files for the supported Windows CE CPU/device combinations are contained in one of these two executable files. The “System Requirements” section on page 2-4 lists the Windows CE devices that are supported for use with 340 and 350 series client adapters. Check this list to ensure that a *.cab file is available for your device.

Step 5

Click Next to start the Windows CE Application Manager (CeAppMgr), which is installed with ActiveSync. CeAppMgr interrogates the Windows CE device to determine its processor type.

Note: If a Windows CE device is not connected to the laptop or PC (as instructed in Step 1), click Exit to quit the setup program and connect a Windows CE device or click Next to continue the installation. If you select Next, a message appears indicating that the software will be downloaded the next time a mobile device is connected. Click OK. The next time a Windows CE device is connected to the laptop or PC via ActiveSync, CeAppMgr starts automatically, and you are prompted to install the software. If you select Exit, click OK to shut down CeAppMgr and start again beginning with Step 1.

Step 6

When a dialog box appears asking if you want to install the client adapter using the default application installation directory, click Yes. The default directory is \Windows\Programs\Cisco on HPC devices and \Windows\Start Menu\Programs\Cisco on PPC devices.

Note: If you click No on an HPC device, CeAppMgr transfers the *.cab file to the Windows CE device and executes it. This process takes awhile and shows no evidence of activity. Eventually a screen appears on the Windows CE device that asks you where the application files should be installed.

A message and a progress bar appear indicating that the client adapter is being installed. CeAppMgr copies the processor-specific *.cab file to the Windows CE device. Then the driver and help files are copied to the \Windows directory, and the client utilities are installed in the \Windows\Programs\Cisco directory on HPC devices or the \Windows\Start Menu\Programs\Cisco directory on PPC devices. Shortcuts to the Aironet Client Utility (ACU) and the Client Encryption Manager (CEM) are automatically added to the desktop on HPC devices.
Step 7 When the installation process is complete on the laptop or PC, a message appears asking you to check the screen of the Windows CE device to see if any additional steps are required to complete the installation. Click OK to terminate the installation process on the laptop or PC.

Step 8 Complete any required steps on the Windows CE device.

Step 9 Remove the CD, if installed.

Step 10 Disconnect the Windows CE device.

Step 11 Insert the client adapter (with the Cisco logo facing up) into the PC card slot of the Windows CE device. Refer to Chapter 7 for specific instructions on inserting the client adapter.

The Windows CE device should configure the client adapter, and the green LED on the adapter should blink. If this does not happen, remove the client adapter, reset the Windows CE device, and reinsert the client adapter.

Step 12 The Cisco Wireless LAN Adapter Settings dialog box appears. (If the dialog box does not appear, select Start, Settings, Control Panel, Network, the Adapters tab, the Cisco Aironet wireless LAN adapter, and Properties on HPC devices or Start, Settings, the Connections tab, Network, and the Cisco Aironet wireless LAN adapter on PPC devices.) Perform one of the following:

- If your device is connected to a DHCP server, select Obtain an IP address via DHCP or Use server-assigned IP address and click OK.

- If your device is not connected to a DHCP server, select Specify an IP address or Use specific IP address and follow the steps below:
  a. Enter the IP address, subnet mask, and default gateway address you want to assign to your device. They can be obtained from your system administrator.
  b. Select the Name Servers tab and enter the primary and secondary DNS and WINS you want to assign to your device. They can be obtained from your system administrator.
  c. Click OK.

Step 13 Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility to open ACU. The ACU screen appears (see Figure 3-1).

Figure 3-1 ACU Screen
### Step 14
Select **SSID** under Property. Then enter your RF network’s case-sensitive SSID in the Value box.

| **SSID**   | The service set identifier (SSID) identifies the specific wireless network that you want to access.  
**Range:** Up to 32 characters (case sensitive)  
**Note** If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (see the AP Radio Hardware page in the access point management system). If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter cannot access the network. |

### Step 15
Select **Client Name** under Property. Then enter your Windows CE device’s unique client name in the Value box.

| **Client Name** | A logical name for your Windows CE device. It allows an administrator to determine which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point’s list of connected devices.  
**Range:** Up to 16 characters  
**Note** Each computer on the network should have a unique client name. |
Step 16  Select **Data Rates** under Property. Make sure that **Auto** is selected in the list of options in the Value box.

**Data Rates**

Specifies the rate at which you want your client adapter to transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).

Auto is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.

**Default**: Auto

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Uses the 11-Mbps data rate when possible but drops to lower rates when necessary</td>
</tr>
<tr>
<td>1 Mb Only</td>
<td>Offers the greatest range but the lowest throughput</td>
</tr>
<tr>
<td>2 Mb Only</td>
<td>Offers less range but greater throughput than the 1 Mbps Only option</td>
</tr>
<tr>
<td>5.5 Mb Only</td>
<td>Offers less range but greater throughput than the 2 Mbps Only option</td>
</tr>
<tr>
<td>11 Mb Only</td>
<td>Offers the greatest throughput but the lowest range</td>
</tr>
</tbody>
</table>

**Note**

Your client adapter’s data rate must be set to Auto or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.

Step 17  Click **OK**. The driver and client utility installation is complete. The client adapter has been installed and configured for basic operation. Go to the “**Verifying Installation**” section on page 3-8 to determine if the installation was successful. Then if you want to enable security features for the client adapter, go to **Chapter 4**.

**Note**

If you want to be able to use the client adapter on another Windows CE device, you can install the driver and client utilities on that device without having to complete all of the previous steps. Refer to the “**Installing the Driver and Client Utilities on Other Windows CE Devices**” section below for instructions.
Installing the Driver and Client Utilities on Other Windows CE Devices

After you have installed the driver and client utilities for your client adapter on a Windows CE device, you can prepare other Windows CE devices with the same operating system (2.11 or 3.0) to be used with your client adapter without having to repeat all of the steps provided in the previous section. You can follow an abbreviated procedure because the driver and client utility files for many different Windows CE CPU/device combinations were copied to the Cisco Aironet Wireless LAN Adapter directory on the laptop or PC when you executed WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe.

Note

After the WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe file has been executed once on the laptop or PC, this procedure can be used to install the driver and client utilities on Windows CE devices that are running the corresponding operating system (2.11 or 3.0).

Follow the steps below to install the driver and client utilities on other Windows CE devices using an abbreviated procedure.

Step 1
Make sure the Windows CE device is connected to a laptop or PC on which the WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe file was already executed.

Step 2
On the laptop or PC, open Windows Explorer and navigate to the C:\Program Files\Microsoft ActiveSync directory.

Note
This step assumes that the default install was used for ActiveSync.

Step 3
Double-click CeAppMgr.exe. After the laptop or PC retrieves data from the Windows CE device, the Add/Remove Programs screen appears on the laptop or PC.

On the Add/Remove Programs screen, empty checkboxes indicate the programs that are installed on the PC, and selected checkboxes indicate the programs that are installed on the Windows CE device.

Step 4
In the Add/Remove Programs screen, select the Cisco Wireless LAN Adapter checkbox and click OK to copy the client adapter’s driver and client utility files from the laptop or PC to the Windows CE device.

Step 5
Go to Step 6 of the “Installing the Driver and Client Utilities” section to complete the installation process.

Verifying Installation

To verify that you have properly installed the driver and client utilities and minimally configured your client adapter, check the client adapter’s LEDs. If the installation was successful, the client adapter’s green LED blinks.

Note
If your installation was unsuccessful or you experienced problems during or after driver installation, refer to Chapter 8 for troubleshooting information.
Enabling Security Features

This chapter explains how to use the client utilities to enable the client adapter’s security features. The following topics are covered in this chapter:

- Overview of Security Features, page 4-2
- Using Static WEP, page 4-6
- Using LEAP, page 4-11
Overview of Security Features

When you use your client adapter with Windows CE, you can protect your data as it is transmitted through your wireless network by encrypting it through the use of wired equivalent privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the LEAP authentication process. The information in the “Static WEP Keys” and “Dynamic WEP Keys with LEAP” sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with LEAP offer a higher degree of security than static WEP keys.

WEP keys, whether static or dynamic, are either 40 or 128 bits in length. 128-bit WEP keys contain more information than 40-bit keys and, therefore, offer a greater level of security.

Note

Refer to the “Additional WEP Key Security Features” section on page 4-4 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

Each device within your wireless network can be assigned up to four static WEP keys. If a device receives a packet that is not encrypted with the appropriate key (as the WEP keys of all devices that are to communicate with each other must match), the device discards the packet and never delivers it to the intended receiver.

Static WEP keys are write-only and temporary; therefore, they cannot be read back from the client adapter and they are lost when power to the adapter is removed or the Windows CE device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows CE device is rebooted. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows CE device. When the driver loads and reads the client adapter’s registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

Note

Prior versions of the client software for Windows CE permitted WEP keys to be stored in either Flash memory (persistent) or volatile memory (temporary). If your client adapter has WEP keys that are stored in Flash memory from a prior release, Client Encryption Manager (CEM) version 2.10 or greater allows you to store WEP keys only in volatile memory, and these keys are used instead of those stored in Flash memory.

The CEM utility enables you to view the current WEP key settings for the client adapter and then to assign new WEP keys or overwrite existing WEP keys, and the Aironet Client Utility (ACU) allows you to enable or disable static WEP. Refer to the “Using Static WEP” section on page 4-6 for instructions.
Overview of Security Features

Dynamic WEP Keys with LEAP

The new standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE), is called 802.1X for 802.11, or simply 802.1X. An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

The 802.1X authentication type that is available on Windows CE devices is EAP-Cisco Wireless, or LEAP. Support for LEAP is provided not in the Windows CE operating system but in your client adapter’s firmware and the Cisco software that supports it. RADIUS servers that support LEAP include Cisco Secure ACS version 2.6 and greater, Cisco Access Registrar version 1.7 and greater, and Funk Steel-Belted RADIUS version 3.0 and greater.

LEAP is enabled in ACU, and a LEAP username and password are entered in the Wireless Login Module (WLM). The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The LEAP username and password are stored in the client adapter’s volatile memory; therefore, they are temporary and need to be re-entered whenever power is removed from the adapter, typically due to the client adapter being ejected or the system powering down.

Note

Prior versions of the client software for Windows CE stored the LEAP username and password in the client adapter’s nonvolatile Flash memory, which was referred to as device-level LEAP. If a LEAP username and password are stored in your client adapter’s Flash memory from a prior release, WLM version 2.10 or greater erases them before a new username and password are written to the adapter’s volatile memory, thereby disabling device-level LEAP.

When you enable Network-EAP on your access point and LEAP on your client adapter, authentication to the network occurs in the following sequence:

1. The client adapter associates to an access point and begins the authentication process.

   Note
   The client does not gain access to the network until mutual authentication between the client and the RADIUS server is successful.

2. Communicating through the access point, the client and RADIUS server complete a mutual authentication process, with the password being the shared secret for authentication. The password is never transmitted during the process.

3. If mutual authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.

4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.

5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets that travel between them.

Refer to the “Using LEAP” section on page 4-11 for instructions on enabling or disabling LEAP and entering the LEAP username and password.

Note

Refer to the IEEE 802.11 Standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm
Additional WEP Key Security Features

Client adapter firmware version 4.25.23 and greater and Windows CE driver version 2.2x and greater support three new security features designed to prevent sophisticated attacks on your wireless network’s WEP keys. These features (MIC, TKIP, and broadcast key rotation) do not need to be enabled on the client adapter; they are supported automatically in the driver and firmware versions listed above. However, they must be enabled on the access point.

Note
Access point firmware version 11.10T or greater is required to enable these security features. Refer to the Cisco Aironet Access Point Software Configuration Guide for instructions on enabling these security features on the access point.

Message Integrity Check (MIC)

MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC adds a few bytes to each packet to make the packets tamper-proof.

The ACU screen displays the word “(MIC)” next to the current status if MIC is supported by the client adapter’s driver and firmware and is enabled on the access point. See Figure 4-1.

Note
If you enable MIC on the access point, your client adapter’s driver must support MIC; otherwise, the client cannot associate.
**Temporal Key Integrity Protocol (TKIP)**

This feature, also referred to as *WEP key hashing*, defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. It protects both unicast and broadcast WEP keys.

**Note**

If you enable TKIP on the access point, your client adapter’s firmware must support TKIP; otherwise, the client cannot associate.

**Broadcast Key Rotation**

EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. When you enable this feature, only wireless client devices using LEAP or EAP-TLS authentication can associate to the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot associate.

**Synchronizing Security Features**

In order to use any of the security features discussed in this section, both your client adapter and the access point to which it will associate must be set appropriately. Table 4-1 indicates the client and access point settings required for each security feature. This chapter provides specific instructions for enabling the security features on your client adapter. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for instructions on enabling the features on the access point.

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>Client Setting</th>
<th>Access Point Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static WEP with open authentication</td>
<td>Create a WEP key and enable Use Static WEP Keys and Open Authentication</td>
<td>Set up and enable WEP and enable Open Authentication</td>
</tr>
<tr>
<td>Static WEP with shared key authentication</td>
<td>Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication</td>
<td>Set up and enable WEP and enable Shared Key Authentication</td>
</tr>
<tr>
<td>LEAP authentication</td>
<td>Enable LEAP</td>
<td>Set up and enable WEP and enable Network-EAP</td>
</tr>
<tr>
<td>MIC</td>
<td>Use driver version 2.2x or greater</td>
<td>Set up and enable WEP with full encryption, set MIC to MMH, and set Use Aironet Extensions to Yes</td>
</tr>
<tr>
<td>TKIP</td>
<td>Use firmware version 4.25.23 or greater</td>
<td>Set up and enable WEP, set TKIP to Cisco, and set Use Aironet Extensions to Yes</td>
</tr>
<tr>
<td>Broadcast key rotation</td>
<td>Use firmware version 4.25.23 or greater and enable LEAP</td>
<td>Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)</td>
</tr>
</tbody>
</table>
Using Static WEP

This section provides instructions for entering new static WEP keys or overwriting existing static WEP keys. Follow the procedures in the order listed below:

1. Open CEM; see below
2. View the client adapter’s current static WEP key settings; see page 4-7
3. Perform one of the following:
   - Enter a new static WEP key and enable WEP; see page 4-7
   - Overwrite an existing static WEP key; see page 4-9
4. Change the CEM password (optional); see page 4-10

Opening CEM

Follow the steps below to open CEM.

**Step 1** Double-click the Cisco CEM icon or select Start > Programs > Cisco > Client Encryption Manager. The Enter Password screen appears (see Figure 4-2), provided a client adapter is installed in the Windows CE device and is running.

**Figure 4-2 Enter Password Screen**

![Enter Password Screen](image)

**Step 2** Enter the correct password in the Password field and click OK.

Passwords are case sensitive and can contain up to 256 alphanumeric characters. The default password is Cisco (uppercase C followed by lowercase isco). For security reasons, the characters you enter are displayed as asterisks.

**Note** Refer to the “Changing the CEM Password” section on page 4-10 for instructions on changing the default password.
Viewing the Client Adapter’s Current Static WEP Key Settings

Follow the steps below to view the client adapter’s current static WEP key settings.

**Step 1** If you entered the password correctly in the Enter Password screen, the CEM screen appears (see Figure 4-3).

*Figure 4-3 CEM Screen*

A checkmark appears in the Already Set? box for all existing static WEP keys.

**Note** For security reasons, the codes for existing static WEP keys do not appear on the screen.

**Step 2** Perform one of the following:

- If no static WEP keys have been set, go to the “Entering a New Static WEP Key and Enabling Static WEP” section on page 4-7 to set up one or more static WEP keys.
- If you want to use an existing static WEP key, make sure the Transmit Key button to the left of the key is selected and click OK. This is the key that will be used to transmit packets. Then open ACU and make sure WEP is enabled.
- If you want to overwrite an existing static WEP key, go to the “Overwriting an Existing Static WEP Key” section on page 4-9.

Entering a New Static WEP Key and Enabling Static WEP

Follow the steps below to enter a new static WEP key for your client adapter.

**Step 1** If you entered the password correctly in the Enter Password screen, the CEM screen appears (see Figure 4-4).
Chapter 4      Enabling Security Features

Using Static WEP

Figure 4-4  CEM Screen

This screen allows you to create up to four static WEP keys.

Step 2  For the static WEP key that you are entering (1, 2, 3, or 4), select a WEP key size of 40 or 128 on the right side of the screen. 128-bit client adapters can use 40- or 128-bit keys, but 40-bit adapters can use only 40-bit keys. If 128 bit is not supported by the client adapter, this option is grayed out, and you are unable to select it.

Step 3  Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:

- WEP keys can consist of the following hexadecimal characters: 0-9, A-F, and a-f.
- WEP keys must contain the following number of characters:
  - 10 hexadecimal characters for 40-bit keys  
    Example: 12345abcde
  - 26 hexadecimal characters for 128-bit keys  
    Example: AB34CD78EFab01cd23ef456789

- Your client adapter’s WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.

- When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.

  Note  After you enter a WEP key, you can write over it, but you cannot edit or delete it.

Step 4  Click the Transmit Key button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.

Step 5  Click OK to write your WEP key(s) to the client adapter’s volatile memory and the Windows CE registry and to exit the utility or click Cancel to exit the utility without updating the keys.

Step 6  Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility. The ACU screen appears (see Figure 4-5).
Figure 4-5  ACU Screen

Step 7  Select **WEP** under Property. Select **Enabled** from the list of options in the Value box to enable static WEP.

Step 8  Click **OK** to save your changes and to exit the utility.

Overwriting an Existing Static WEP Key

Follow the steps below to overwrite an existing static WEP key.

Step 1  If you entered the password correctly in the Enter Password screen, the CEM screen appears (see Figure 4-6).

Figure 4-6  CEM Screen

A checkmark appears in the Already Set? box for all existing static WEP keys.

Note  For security reasons, the codes for existing static WEP keys do not appear on the screen. Also, you can write over existing keys, but you cannot edit or delete them.
Step 2  Decide which existing static WEP key you want to overwrite.

Step 3  Click within the blank field of that key.

Step 4  Enter a new key, following the guidelines outlined in Step 3 of the “Entering a New Static WEP Key and Enabling Static WEP” section on page 4-7.

Step 5  Make sure the Transmit Key button to the left of your key is selected, if you want this key to be used to transmit packets.

Step 6  Click OK to write your new static WEP key to the client adapter’s volatile memory and the Windows CE registry and to exit the utility or click Cancel to exit the utility without overwriting any keys.

Step 7  Open ACU and make sure WEP is enabled.

---

**Changing the CEM Password**

Follow the steps below if you want to change the password that allows you to access CEM.

**Note**  For security reasons, Cisco recommends that you change the default password.

---

Step 1  Double-click the Cisco CEM icon or select Start > Programs > Cisco > Client Encryption Manager.

Step 2  Enter the correct password in the Enter Password screen (see Figure 4-2) and click OK. The CEM screen appears (see Figure 4-6).

Step 3  Click the Change Password button. The Change Password screen appears (see Figure 4-7).

**Figure 4-7  Change Password Screen**

---

Step 4  Enter the current password in the Existing Password field.

Step 5  Enter a new password in the New Password field.

**Note**  Passwords are case sensitive and can contain up to 256 alphanumeric characters.
Step 6  Re-enter the new password in the Confirm New Password field.
Step 7  Click OK to save your new password or click Cancel to exit the screen without changing the password. If your password is accepted, the following message appears, “Password Successfully Changed.”
Step 8  Click OK to exit the utility.

Disabling Static WEP

Follow the steps below if you ever need to disable static WEP.

Step 1  Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility. The ACU screen appears (see Figure 4-5).
Step 2  Select WEP under Property. Select Disabled from the list of options in the Value box to disable WEP.
Step 3  Click OK to save your changes and to exit the utility.

Using LEAP

This section provides instructions for enabling LEAP and entering the LEAP username and password.

Note  LEAP is supported only on client adapters that support WEP and use firmware version 4.13 or greater.

Note  In order to use LEAP authentication, your client adapter and access point firmware must have matching 802.1X draft standards. That is, if the access point uses draft 8 firmware (prior to 11.06) or has draft 8 selected, the client adapter must use draft 8 firmware (prior to 4.25.x). Similarly, if the access point uses draft 10 firmware (11.06 or later) and has draft 10 selected, the client adapter must use draft 10 firmware (4.25.x or later).
Enabling LEAP

Follow the steps below to enable LEAP for your client adapter.

**Step 1** Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility. The ACU screen appears (see Figure 4-8).

**Step 2** Select LEAP under Property.

**Step 3** Select Enabled in the Value box.

**Step 4** Click OK to enable LEAP and exit the utility. When LEAP is enabled, the following parameters in the ACU screen are changed automatically:
- WEP is set to Enabled.
- Authentication Type is set to Open.

Entering the LEAP Username and Password

Follow the steps below to enter the LEAP username and password.

**Step 1** WLM starts automatically whenever you start ACU with a client adapter inserted, change the LEAP parameter from Disabled to Enabled, and click OK. If LEAP is already enabled, WLM starts automatically whenever you insert the client adapter, reboot or reset the Windows CE device, or load new firmware.

*Note* You can also start WLM by selecting Start > Programs > Cisco > Wireless Login Module. You may want to do this if you inadvertently exited WLM after it started or if you roam to a different part of the network where a different login is required.

When WLM starts, the Wireless Login Module screen appears (see Figure 4-9).
Step 2 Obtain the username and password for your RADIUS server account from your system administrator.

*Note* The password is optional because not all host accounts on the RADIUS server are set up with a password.

Step 3 Enter the username in the User Name field.

*Note* Usernames and passwords are case sensitive and can contain up to 32 alphanumeric characters.

*Note* If your device is running Windows CE 3.0 version 2002 and your RADIUS server account specifies a domain, enter the domain name before the username and separate the two with a forward slash (e.g., `domain/username`).

Step 4 Enter the password in the Password field if the RADIUS server account for the Windows CE device was set up with a password.

*Note* For security reasons, the characters entered for the password are displayed as asterisks.

Step 5 Click **OK**. If the username and password were entered correctly, they are written to volatile memory on the client adapter. The username and password remain on the client adapter until power is removed from the adapter, typically due to the client adapter being ejected or the system powering down.

*Note* If a username and password are stored in the client adapter’s Flash memory from a prior release, they are erased before the new username and password are written to the adapter’s volatile memory, thereby disabling device-level LEAP.
Using LEAP

Step 6 One of three scenarios occurs:

1. The client adapter authenticates to the RADIUS server using your username and password and receives a dynamic, session-based WEP key. The bottom of the ACU screen indicates that your client adapter is authenticated to an access point.

2. If you enter the username and password incorrectly or enter ones that are not valid for the RADIUS server on the network, the Wireless Login Module screen reappears with a message indicating that your login was incorrect. You are able to retry immediately by re-entering the username and password.

3. The client adapter times out while trying to authenticate, possibly because it is out of range of an access point. After 60 seconds, a message appears indicating that the first attempt to authenticate failed and that the client adapter will continue trying.

Note During the 60 seconds before the timeout occurs, WLM is running in the background. It is hidden and does not appear as a running program. If you try to start WLM during this time, nothing happens because it is already running.

Disabling LEAP

Follow the steps below if you ever need to disable LEAP.

Step 1 Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility. The ACU screen appears (see Figure 4-8).

Step 2 Select LEAP under Property.

Step 3 Select Disabled in the Value box.

Step 4 Click OK to disable LEAP and to exit the utility.
Advanced Configuration

This chapter explains how to set the client adapter’s advanced configuration parameters. The following topic is covered in this chapter:

- Configuring Your Client Adapter, page 5-2
Configuring Your Client Adapter

The Aironet Client Utility (ACU) enables you to change the configuration parameters of your client adapter. Follow the steps below to open ACU and make any configuration changes.

Note

The driver and client utility installation process, which is documented in Chapter 3, provides instructions to initially configure your client adapter and make it operational. Therefore, the information in this chapter is necessary only if you need to configure your client adapter to utilize an advanced feature.

Step 1

Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility. The ACU screen appears (see Figure 5-1).

Figure 5-1 ACU Screen

The Property box lists the configuration parameters that can be changed, and the Value box contains the highlighted parameter’s current value. The Value box can appear as a drop-down list with several possible values from which to choose or as a blank field in which characters are to be entered.

Table 5-1 lists and describes the client adapter’s configuration parameters. Follow the instructions in the table to initially set or change any parameters.
### Table 5-1  Client Adapter Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>The service set identifier (SSID) identifies the specific wireless network that you want to access.</td>
</tr>
<tr>
<td><strong>Range:</strong></td>
<td>You can key in up to 32 characters (case sensitive)</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>A blank field</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (see the AP Radio Hardware page in the access point management system). If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter cannot access the network.</td>
</tr>
<tr>
<td>Client Name</td>
<td>A logical name for your Windows CE device. It allows an administrator to determine which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point’s list of connected devices.</td>
</tr>
<tr>
<td><strong>Range:</strong></td>
<td>You can key in up to 16 characters</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>A blank field</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Each computer on the network should have a unique client name.</td>
</tr>
<tr>
<td>Infrastructure Mode</td>
<td>Specifies the type of network in which your client adapter is installed.</td>
</tr>
<tr>
<td><strong>Options:</strong></td>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infrastructure Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td>
</tr>
<tr>
<td>No</td>
<td>Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point (referred to as ad hoc mode).</td>
</tr>
</tbody>
</table>
### Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Save Mode</td>
<td>Sets your client adapter to its optimum power-consumption setting.</td>
</tr>
<tr>
<td><strong>Options:</strong> CAM, Fast PSP, or Max PSP</td>
<td></td>
</tr>
<tr>
<td><strong>Default:</strong> CAM (Constantly Awake Mode)</td>
<td></td>
</tr>
<tr>
<td>CAM (Constantly Awake Mode)</td>
<td>Keeps the client adapter powered up continuously so there is little lag in message response time. Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.</td>
</tr>
<tr>
<td>Fast PSP (Power Save Mode)</td>
<td>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved. Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</td>
</tr>
<tr>
<td>Max PSP (Max Power Savings)</td>
<td>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep. Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</td>
</tr>
<tr>
<td>WEP</td>
<td>Enables or disables WEP for your client adapter.</td>
</tr>
<tr>
<td><strong>Options:</strong> Enabled or Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Default:</strong> Disabled</td>
<td></td>
</tr>
</tbody>
</table>

This parameter can be used in two ways:

- If you set a WEP key using CEM, you must also select Enabled for this parameter to enable WEP for your client adapter.
- If you enabled LEAP for your client adapter, this parameter is changed automatically to Enabled, and the RADIUS server assigns a dynamic, session-based WEP key to the adapter.
### Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>Defines how your client adapter will attempt to authenticate to an access point.</td>
</tr>
<tr>
<td><strong>Options</strong>: Open or Shared Key</td>
<td></td>
</tr>
<tr>
<td><strong>Default</strong>: Open</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Open Authentication</td>
<td>Allows your client adapter, regardless of its WEP settings, to associate with an access point. If LEAP is enabled on your client adapter, Open Authentication is the only available option.</td>
</tr>
<tr>
<td>Shared Key Authentication</td>
<td>Allows your client adapter to associate only with access points that have the same WEP key. This option is available only if the client adapter has been assigned a static WEP key in CEM, static WEP is enabled, and LEAP is not enabled. The access point sends a known unencrypted “challenge packet” to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter.</td>
</tr>
</tbody>
</table>

**Note**: Cisco recommends that shared key authentication not be used because it presents a security risk.

<table>
<thead>
<tr>
<th>LEAP</th>
<th>Enables or disables LEAP authentication for your client adapter.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Options</strong>: Enabled or Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Default</strong>: Disabled</td>
<td></td>
</tr>
<tr>
<td>LEAP</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables LEAP after you enter a username and password in WLM.</td>
</tr>
<tr>
<td><strong>Note</strong>: This parameter must be enabled before you set a LEAP username and password in WLM.</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>Disables LEAP. LEAP can be disabled as desired.</td>
</tr>
</tbody>
</table>
Mixed Mode Indicates if the client adapter can associate to an access point that allows both WEP and non-WEP associations.

- If the access point with which the client adapter is to associate has WEP set to Optional, you must enable Mixed Mode on the adapter (regardless of whether WEP is enabled on the adapter). Otherwise, the client adapter cannot establish a connection with the access point.
- If the access point with which the client adapter is to associate does not have WEP set to Optional, Mixed Mode should be set to Disabled on the adapter.

**Options:** Enabled or Disabled  
**Default:** Disabled  
**Note** For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets will be sent unencrypted, even to clients running WEP.

World Mode Enables the client adapter to adopt the maximum transmit power level and the frequency range of the access point to which it is associated, provided the access point is also configured for world mode. This parameter is available only in infrastructure mode and is designed for users who travel between countries and want their client adapters to associate to access points in different regulatory domains.

**Options:** Enabled or Disabled  
**Default:** Disabled  
**Note** When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation’s regulatory agency.
Chapter 5      Advanced Configuration

Configuring Your Client Adapter

Data Rates Specifies the rate at which your client adapter should transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).

Auto is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.

Options: Auto, 1 Mb Only, 2 Mb Only, 5.5 Mb Only, or 11 Mb Only

Default: Auto

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Uses the 11-Mbps data rate when possible but drops to lower rates when necessary</td>
</tr>
<tr>
<td>1 Mb Only</td>
<td>Offers the greatest range but the lowest throughput</td>
</tr>
<tr>
<td>2 Mb Only</td>
<td>Offers less range but greater throughput than the 1 Mbps Only option</td>
</tr>
<tr>
<td>5.5 Mb Only</td>
<td>Offers less range but greater throughput than the 2 Mbps Only option</td>
</tr>
<tr>
<td>11 Mb Only</td>
<td>Offers the greatest throughput but the lowest range</td>
</tr>
</tbody>
</table>

Note  Your client adapter's data rate must be set to Auto or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.

Note  If ACU is running but a client adapter is not currently inserted in the Windows CE device, the data rate options are based on the last adapter that was running in the system.
Chapter 5 Advanced Configuration

Configuring Your Client Adapter

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Power</td>
<td>Defines the power level at which your client adapter transmits. This value must not be higher than that allowed by your country’s regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, MKK in Japan, etc.).</td>
</tr>
<tr>
<td><strong>Options:</strong></td>
<td>Dependent on the power table programmed into the client adapter; see the table below</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>Max (the maximum level programmed into the client adapter and allowed by your country’s regulatory agency)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power Levels</th>
<th>Client Adapter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max, 100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW</td>
<td>350 series PC and LM cards</td>
</tr>
<tr>
<td>Max, 30 mW, or 1 mW</td>
<td>340 series PC cards</td>
</tr>
<tr>
<td>Max, 30 mW, 15 mW, 5 mW, or 1 mW</td>
<td>340 series LM cards</td>
</tr>
</tbody>
</table>

**Note** Reducing the transmit power level conserves battery power but decreases radio range.

**Note** If the client adapter is running, ACU queries the adapter and displays the settings programmed into the adapter. If the client adapter is not running, ACU displays power level options based on the last known radio type.

**Note** When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation’s regulatory agency.

**Note** If you are using an older version of a 340 or 350 series client adapter, your power level options may be different than those listed here.

**Step 2** Click **OK** at the bottom of the ACU screen to save any changes you have made.
Performing Diagnostics

This chapter explains how to use the client utilities to perform user-level diagnostics. The following topics are covered in this chapter:

- Overview of the Diagnostic Utilities, page 6-2
- Viewing the Current Status of Your Client Adapter, page 6-2
- Viewing Statistics for Your Client Adapter, page 6-3
Overview of the Diagnostic Utilities

The diagnostic utilities enable you to assess the performance of your client adapter within the wireless network. These utilities perform the following functions:

- Display your client adapter’s current status
- Display statistics pertaining to your client adapter’s transmission and reception of data

Viewing the Current Status of Your Client Adapter

The Cisco Link Status (CLS) utility enables you to view the current status of your client adapter.

**Step 1** To view your client adapter’s status, select Start > Programs > Cisco > Cisco Link Status. The Cisco Link Status screen appears (see Figure 6-1).

![Figure 6-1 Cisco Link Status Screen](image)

Table 6-1 interprets each element of the Cisco Link Status screen.
Table 6-1  Client Adapter Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first line of the Cisco Link Status screen</td>
<td>Indicates the operational mode of your client adapter and the name or MAC address of any associated access point. Value: Associated, Not Associated, Authenticated, or Ad Hoc Mode</td>
</tr>
</tbody>
</table>
| Signal Strength                | The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal. The histogram below the bar graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest).
|                               | **Range:** 0 to 100%                                                        |
| Signal Quality (Beacons Received is displayed instead if your firmware version is less than 4.05) | The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal. The histogram below the bar graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).
|                               | **Range:** 0 to 100%                                                        |
| Overall Link Quality           | The client adapter’s ability to communicate with the access point, which is determined by the combined result of the adapter’s signal strength and signal quality. Value: Not Associated, Poor, Fair, Good, Excellent |

Step 2  Click **OK** to exit the utility.

Viewing Statistics for Your Client Adapter

The Client Statistics Utility (CSU) enables you to view statistics that indicate how data is being received and transmitted by your client adapter. It also shows message integrity check (MIC) statistics if your client adapter’s driver and firmware support MIC and MIC is enabled on the access point.

Note  The receive and transmit statistics are host statistics. That is, they show packets and errors received or sent by the Windows CE device. Link status tests from the access point or SST are performed at the firmware level; therefore, they have no effect on the statistics shown by this utility.
Step 1

To view your client adapter’s statistics, select **Start > Programs > Cisco > Client Statistics Utility**. The Receive Statistics screen appears (see **Figure 6-2**).

**Figure 6-2  Receive Statistics Screen**

![Receive Statistics Screen](image)

The statistics are calculated as soon as your client adapter is started. **Table 6-2** describes each receive statistic that is displayed for your client adapter.

**Table 6-2  Receive Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Packets</td>
<td>The number of multicast packets that were received successfully.</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>The number of broadcast packets that were received successfully.</td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets that were received successfully.</td>
</tr>
<tr>
<td>Bytes Received</td>
<td>The number of bytes of data that were received successfully.</td>
</tr>
<tr>
<td>Beacons Received</td>
<td>The number of beacon packets that were received successfully.</td>
</tr>
<tr>
<td>PLCP CRC Errors</td>
<td>The number of times the client adapter started to receive an 802.11 Physical Layer Convergence Protocol (PLCP) header but the rest of the packet was ignored due to a cyclic redundancy check (CRC) error in the header.</td>
</tr>
</tbody>
</table>

**Note**

CRC errors can be attributed to packet collisions caused by a dense population of client adapters, overlapping access point coverage on a channel, high multipath conditions due to bounced signals, or the presence of other 2.4-GHz signals from devices such as microwave ovens, wireless handset phones, etc.
To view the transmit statistics for your client adapter, click the drop-down arrow in the bottom left corner of the screen and select Transmit Stats. The Transmit Statistics screen appears (see Figure 6-3).

**Table 6-3 Transmit Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Packets</td>
<td>The number of multicast packets that were transmitted successfully.</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>The number of broadcast packets that were transmitted successfully.</td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets that were transmitted successfully.</td>
</tr>
<tr>
<td>Bytes Transmitted</td>
<td>The number of bytes of data that were transmitted successfully.</td>
</tr>
<tr>
<td>Packets Retry Long</td>
<td>The number of normal data packets that were retransmitted.</td>
</tr>
</tbody>
</table>

Table 6-3 describes each transmit statistic that is displayed for your client adapter.
Viewing Statistics for Your Client Adapter

**Table 6-3  Transmit Statistics (continued)**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Retry Short</td>
<td>The number of request-to-send (RTS) packets that were retransmitted.</td>
</tr>
<tr>
<td>Packets Max Retries</td>
<td>The number of packets that failed to be transmitted successfully after exhausting the maximum number of retries.</td>
</tr>
<tr>
<td>Up Time (hh:mm:ss)</td>
<td>The amount of time (in hours:minutes:seconds) since your client adapter was started. If the client adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.</td>
</tr>
</tbody>
</table>

**Step 3**  To view the MIC statistics for your client adapter, click the drop-down arrow in the bottom left corner of the screen and select **MIC Stats**. The MIC Statistics screen appears (see Figure 6-4).

**Note**  The MIC Stats option is available only if your client adapter’s driver and firmware support MIC and MIC is enabled on the access point. See “Message Integrity Check (MIC)” section on page 4-4 for additional information.

**Figure 6-4  MIC Statistics Screen**

![MIC Statistics Screen](image)

**Table 6-4  MIC Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets MIC OK</td>
<td>The number of packets that were received successfully with a valid MIC.</td>
</tr>
<tr>
<td>Packets No MIC</td>
<td>The number of packets that were discarded due to no MIC being found.</td>
</tr>
<tr>
<td>Packets Incorrect MIC</td>
<td>The number of packets that were discarded due to an incorrect MIC value.</td>
</tr>
</tbody>
</table>
### Table 6-4  MIC Statistics (continued)

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets No MIC Seed</td>
<td>The number of packets that were discarded due to no MIC seed being received.</td>
</tr>
<tr>
<td>Packets Wrong MIC Seq</td>
<td>The number of packets that were discarded due to the MIC sequence number being wrong.</td>
</tr>
</tbody>
</table>

**Step 4** Click **OK** to exit the utility.
Viewing Statistics for Your Client Adapter
Routine Procedures

This chapter provides procedures for common tasks related to the client adapter. The following topics are covered in this chapter:

- Inserting and Removing a PC Card, page 7-2
- Upgrading the Client Adapter Software, page 7-3
- Client Utility Procedures, page 7-12
- Restarting the Client Adapter, page 7-13
Inserting and Removing a PC Card

This section provides instructions for inserting a PC card into or removing a PC card from a Windows CE device.

Inserting a PC Card into a Windows CE Device

Follow the steps below to insert a PC card into a Windows CE device.

⚠️ **Caution**

This procedure and the physical connections it describes apply generally to conventional PC card slots. In cases of custom or nonconventional equipment, be alert to possible differences in PC card slot configurations.

**Step 1**

Before you begin, examine the PC card. One end has a dual-row, 68-pin PC card connector. The card is keyed so it can be inserted only one way into the PC card slot.

⚠️ **Caution**

Do not force the PC card into your computer’s PC card slot. Forcing it will damage both the card and the slot. If the PC card does not insert easily, remove the card and reinsert it.

**Step 2**

Hold the PC card with the Cisco logo facing up and insert it into the PC card slot, applying just enough pressure to make sure it is fully seated (see Figure 7-1).

*Figure 7-1  Inserting a PC Card into a Computing Device*

Removing a PC Card from a Windows CE Device

Follow the instructions below whenever you need to remove the PC card from your Windows CE device.

To remove a PC card after it is successfully installed and configured, press the Eject button and pull the card out of the PC card slot. When the PC card is reinserted, your connection to the network should be re-established.
Upgrading the Client Adapter Software

This section provides instructions for the following procedures:

- Upgrading the firmware, see below
- Upgrading the driver and client utilities, see page 7-5

Upgrading the Firmware

The client adapter is shipped with the firmware installed in its Flash memory; however, a more recent version of the firmware may be available from Cisco.com. Cisco recommends using the most current version of radio firmware. Follow the instructions in this section to determine the version of your client adapter’s firmware and to upgrade it if a more recent version is available from Cisco.com.

Determining the Firmware Version

Follow the steps below to determine if you need to upgrade the client adapter’s firmware.

Step 1
To determine the version of firmware that your client adapter is currently using, double-click the Cisco ACU icon or select Start > Programs > Cisco > Load New Firmware. The current version of your adapter’s firmware is shown on the ACU screen and the Select New Firmware screen, provided a client adapter is inserted in your Windows CE device.

Step 2
To determine the latest firmware version available on Cisco.com, follow the steps below:

a. Use your computer’s web browser to access the following URL:
b. Locate the section for client adapter firmware.
c. Click the link for your client adapter’s series (for example, 350 Series).
d. Look at the available filenames for radio firmware. The numbers that follow the “v” indicate the version number. For example, v42530 indicates a firmware version of 4.25.30.

Note
In order to use LEAP authentication, your client adapter and access point firmware must have matching 802.1X draft standards. That is, if the access point uses draft 8 firmware (prior to 11.06) or has draft 8 selected, the client adapter must use draft 8 firmware (prior to 4.25.x). Similarly, if the access point uses draft 10 firmware (11.06 or later) and has draft 10 selected, the client adapter must use draft 10 firmware (4.25.x or later).

Step 3
If the firmware available from Cisco.com has a higher number than the firmware currently installed in your client adapter, follow the instructions in the “Loading New Firmware” section on page 7-4 to upgrade the firmware.
Loading New Firmware

Follow the instructions below to load new firmware into your client adapter.

**Step 1**  Use a serial or USB cable to connect your Windows CE device to a laptop or PC running ActiveSync. A message appears on the Windows CE device indicating that it is connecting to the host. After the Windows CE device is connected, the New Partnership window appears on the laptop or PC. This window asks if you want to set up a partnership.

**Step 2** Perform one of the following:
- If you want to establish a partnership that allows you to synchronize files between the laptop or PC and the Windows CE device, select Yes, click Next, and follow the instructions on the screen to specify the files to be synchronized and to finish setting up the partnership.
- If you do not want to synchronize files and want to connect as a “guest,” select No and click Next. The screen indicates that you are connected as a guest.

**Step 3** Use the laptop or PC’s web browser to access the following URL:


**Step 4** Locate the section for client adapter firmware.

**Step 5** Click the link for your client adapter’s series (for example, 350 Series).

**Step 6** Click the firmware file for your client adapter.

**Note** If your wireless network uses LEAP, remember to select a firmware file of the same draft standard as the access points to which your client adapters will be authenticating.

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

**Step 8** Select the firmware file to download it.

**Step 9** Save the file to a floppy disk or to the hard drive of your laptop or PC.

**Step 10** Locate the file using Windows Explorer, double-click it, and extract the image file (*.img) to a folder.

**Step 11** In the ActiveSync window on the laptop or PC, click the Explore button to view the files on the Windows CE device.

**Step 12** Drag and drop the firmware image from Windows Explorer to a location in the ActiveSync window.

**Note** If your Windows CE device is a PPC running Windows CE 3.0, you must copy the firmware image to the My Documents folder or a folder under My Documents.

**Step 13** After the file is copied, disconnect the Windows CE device.

**Step 14** Make sure the client adapter is installed in your Windows CE device and is operational.

**Step 15** On your Windows CE device, select Start > Programs > Cisco > Load New Firmware. The Load New Firmware screen appears (see Figure 7-2).
Chapter 7    Routine Procedures

Upgrading the Client Adapter Software

Figure 7-2  Load New Firmware Screen

![Load New Firmware Screen]

**Step 16** Click the **Select Firmware** button.

The Open window appears (see Figure 7-3).

**Note** The window shown below is on a Windows CE HPC device. The screen looks slightly different on a Windows CE PPC device.

Figure 7-3  Open Window

![Open Window]

**Step 17** Find the location of the new firmware image in the Open window.

**Step 18** Click the new firmware image file (*.img) so it appears in the Name box at the bottom of the Open window.

**Step 19** Click **OK**. If the selected image is loaded successfully into the client adapter’s Flash memory, a “Firmware Upgrade Complete!” message appears on the Load New Firmware screen.

Upgrading the Driver and Client Utilities

Follow the instructions in this section to determine the versions of your client adapter’s driver and client utilities and to upgrade them if more recent versions are available from Cisco.com.

**Note** The driver, client utilities, and online help files are installed together.
Determining the Driver and Client Utility Versions

Follow the instructions in this section to determine if you need to upgrade the client adapter’s driver or client utilities.

**Step 1** To determine the version of the driver that your client adapter is currently using, double-click the Cisco ACU icon or select **Start > Programs > Cisco > Aironet Client Utility**. The current version of your adapter’s driver is shown on the ACU screen, provided the client adapter is installed in the Windows CE device and is operational.

**Step 2** To determine the version of a client utility that your client adapter is using, open the utility and click the **About** button at the bottom of the screen. The About screen displays the current version of the utility.

**Step 3** To determine the latest driver and client utility versions available on Cisco.com, follow the steps below:

a. Use your computer’s web browser to access the following URL:


b. Locate the section for client adapter drivers and utilities.

c. Click the link for Windows CE 2.11 or 3.0, depending on which version of Windows CE your device is running.

   **Note** If you are not sure which version of Windows CE your device is running, refer to the “Determining the Windows CE Version” section on page 3-2 for instructions.

d. Look at the release numbers of the driver and client utilities in the description below the filename. These are the latest available versions on Cisco.com.

**Step 4** If the driver or client utility version available from Cisco.com is greater than the version currently being used by your client adapter, follow the instructions in the “Uninstalling the Current Driver and Client Utilities” section below to remove the current driver and client utilities and the instructions in the “Loading a New Driver and Client Utilities” section on page 7-7 to install the new driver and client utilities.

Uninstalling the Current Driver and Client Utilities

Cisco recommends that you uninstall the existing driver and client utilities for your client adapter before upgrading to more recent versions. This section provides instructions for uninstalling your client adapter’s current driver and client utilities. The instructions vary depending on your client adapter’s current driver version.

Uninstalling Driver Version 1.4 for Windows CE 2.11

**Step 1** Terminate any Cisco Aironet applications running on the Windows CE device and eject the client adapter.

**Step 2** Select **Start > Programs > Cisco > Cisco Aironet Uninstall**. The Cisco Aironet Uninstall screen appears.

**Step 3** Select the **Uninstall Cisco Aironet Wireless LAN Adapter** checkbox.
Upgrading the Client Adapter Software

Chapter 7      Routine Procedures

Step 4 Click OK. The utility informs you that the adapter has been uninstalled. The registry entries (but no files) are removed.

Step 5 Delete the aironet.dll driver file and the following help files from the \Windows directory of the Windows CE device: AuthType.htm, CEM.htm, Cisco Setup.htm, ClicName.htm, DataRate.htm, DHCP.htm, InfrStru.htm, LEAP.htm, LeapLogin.htm, PSMode.htm, SSID.htm, TxPowe.htm, WEP.htm, and WorldMode.htm.

Step 6 Delete the following client utility files, which are probably in the \Windows\Programs\Cisco directory on the Windows CE device: Aironet Client Utility.exe, Cisco Aironet Uninstall.exe, Cisco Link Status.exe, Client Encryption Manager.exe, Client Statistics Utility.exe, Load New Firmware.exe, and Site Survey Tool.exe.

Step 7 Delete the Cisco directory from \Windows\Programs.

Step 8 Go to the “Loading a New Driver and Client Utilities” section below for instructions on loading a new driver and client utilities.

Uninstalling Driver Version 1.5 or Later for Windows CE 2.11 or 3.0

Step 1 Eject the client adapter and remove it from the Windows CE device.

Step 2 Select Start > Settings > Control Panel > Remove Programs (on an HPC device) or Start > Settings > System tab > Remove Programs (on a PPC device).

Step 3 Select Cisco Wireless LAN Adapter.

Step 4 Click Remove.

Step 5 When asked to verify your decision to remove the adapter, click Yes.

Step 6 Click OK. The driver, client utilities, registry entries, and Cisco directory are removed.

Step 7 Go to the “Loading a New Driver and Client Utilities” section below for instructions on loading a new driver and client utilities.

Loading a New Driver and Client Utilities

Follow the instructions below to install a new driver and client utilities for your client adapter.

Step 1 Make sure that the client adapter is removed from the Windows CE device.

Step 2 Use a serial or USB cable to connect your Windows CE device to a laptop or PC running ActiveSync. A message appears on the Windows CE device indicating that it is connecting to the host. After the Windows CE device is connected, the New Partnership window appears on the laptop or PC. This window asks if you want to set up a partnership.

Step 3 Perform one of the following:

- If you want to establish a partnership that allows you to synchronize files between the laptop or PC and the Windows CE device, select Yes, click Next, and follow the instructions on the screen to specify the files to be synchronized and to finish setting up the partnership.
- If you do not want to synchronize files and want to connect as a “guest,” select No and click Next. The screen indicates that you are connected as a guest.
Chapter 7  Routine Procedures

Upgrading the Client Adapter Software

Step 4  Use the laptop or PC’s web browser to access the following URL:

Step 5  Locate the section for client adapter drivers and utilities.

Step 6  Click the link for Windows CE 2.11 or 3.0, depending on which version of Windows CE your device is running.

Step 7  Select the WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe file.

Step 8  Read and accept the terms and conditions of the Software License Agreement.

Step 9  Select the WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe file to download it.

Step 10  Save the file to a floppy disk or to the hard drive of your laptop or PC.

Step 11  Use Windows Explorer to locate the saved file.

Step 12  Double-click the *.exe file for your version of Windows CE (WinCE2.11-PCM-LMC-vx.xx.exe or WinCE3.0-PCM-LMC-vx.xx.exe). The application creates an Install directory under the ActiveSync directory, extracts the .cab files contained in the *.exe file, and copies them to the Install directory.

Step 13  Click Next to start the Windows CE Application Manager (CeAppMgr). CeAppMgr interrogates the Windows CE device to determine its processor type.

Note  If a Windows CE device is not connected to the laptop or PC (as instructed in Step 2), click Exit to quit the setup program and connect a Windows CE device or click Next to continue the installation. If you select Next, a message appears indicating that the software will be downloaded the next time a mobile device is connected. Click OK. The next time a Windows CE device is connected to the laptop or PC via ActiveSync, CeAppMgr starts automatically and you are prompted to install the software. If you select Exit, click OK to shut down CeAppMgr and start again beginning with Step 1.

Step 14  When a dialog box appears asking if you want to install the client adapter using the default application installation directory, click Yes. The default directory is \Windows\Programs\Cisco on HPC devices and \Windows\Start Menu\Programs\Cisco on PPC devices.

Note  If you click No on an HPC device, CeAppMgr transfers the *.cab file to the Windows CE device and executes it. This process takes awhile and shows no evidence of activity. Eventually a screen appears on the Windows CE device that asks you where the application files should be installed.

A message and a progress bar appear indicating that the client adapter is being installed. CeAppMgr copies the processor-specific *.cab file to the Windows CE device. Then the driver and help files are copied to the \Windows directory, and the client utilities are installed in the \Windows\Programs\Cisco directory on HPC devices or the \Windows\Start Menu\Programs\Cisco directory on PPC devices. Shortcuts to ACU and CEM are automatically added to the desktop on HPC devices.

Step 15  When the installation process is complete on the laptop or PC, a message appears asking you to check the screen of the Windows CE device to see if any additional steps are required to complete the installation. Click OK to terminate the installation process on the laptop or PC.

Step 16  Complete any required steps on the Windows CE device.

Step 17  Disconnect the Windows CE device.
**Step 18** Insert the client adapter (with the Cisco logo facing up) into the PC card slot of the Windows CE device. Refer to the “Inserting a PC Card into a Windows CE Device” section on page 7-2 for specific instructions on inserting the client adapter.

The Windows CE device should configure the client adapter, and the green LED on the adapter should blink. If this does not happen, remove the client adapter, reset the Windows CE device, and reinsert the client adapter.

**Step 19** The Cisco Wireless LAN Adapter Settings dialog box appears. (If the dialog box does not appear, select Start, Settings, Control Panel, Network, the Adapters tab, the Cisco Aironet wireless LAN adapter, and Properties on HPC devices or Start, Settings, the Connections tab, Network, and the Cisco Aironet wireless LAN adapter on PPC devices.)

Perform one of the following:

- If your device is connected to a DHCP server, select Obtain an IP address via DHCP or Use server-assigned IP address and click OK.
- If your device is not connected to a DHCP server, select Specify an IP address or Use specific IP address and follow the steps below:
  
  a. Enter the IP address, subnet mask, and default gateway address you want to assign to your device. They can be obtained from your system administrator.
  
  b. Select the Name Servers tab and enter the primary and secondary DNS and WINS you want to assign to your device. They can be obtained from your system administrator.
  
  c. Click OK.

**Step 20** Double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility to open ACU. The ACU screen appears (see Figure 7-4).

*Figure 7-4 ACU Screen*
Step 21
Select **SSID** under Property. Then enter your RF network’s case-sensitive SSID in the Value box.

<table>
<thead>
<tr>
<th>SSID</th>
<th>The service set identifier (SSID) identifies the specific wireless network that you want to access.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range:</strong></td>
<td>Up to 32 characters (case sensitive)</td>
</tr>
</tbody>
</table>

*Note* If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (see the AP Radio Hardware page in the access point management system). If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter cannot access the network.

Step 22
Select **Client Name** under Property. Then enter your Windows CE device’s unique client name in the Value box.

<table>
<thead>
<tr>
<th>Client Name</th>
<th>A logical name for your Windows CE device. It allows an administrator to determine which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point’s list of connected devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Range:</strong></td>
<td>Up to 16 characters</td>
</tr>
</tbody>
</table>

*Note* Each computer on the network should have a unique client name.
### Step 23
Select **Data Rates** under Property. Make sure that **Auto** is selected in the list of options in the Value box.

**Data Rates**

Specifies the rate at which you want your client adapter to transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).

**Auto** is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.

**Default:** Auto

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Uses the 11-Mbps data rate when possible but drops to lower rates when necessary</td>
</tr>
<tr>
<td>1 Mb Only</td>
<td>Offers the greatest range but the lowest throughput</td>
</tr>
<tr>
<td>2 Mb Only</td>
<td>Offers less range but greater throughput than the 1 Mbps Only option</td>
</tr>
<tr>
<td>5.5 Mb Only</td>
<td>Offers less range but greater throughput than the 2 Mbps Only option</td>
</tr>
<tr>
<td>11 Mb Only</td>
<td>Offers the greatest throughput but the lowest range</td>
</tr>
</tbody>
</table>

**Note**

Your client adapter’s data rate must be set to Auto or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.

### Step 24
Click **OK**. The driver and client utility installation is complete. If the installation was successful, the client adapter’s green LED blinks.

### Step 25
Go to **Chapter 4** for instructions on setting the client adapter’s security features, if desired.
Client Utility Procedures

This section provides instructions for the following procedures:

- Opening a client utility
- Exiting a client utility
- Determining the version of a client utility
- Deleting client utility icons on HPC devices

Opening a Client Utility

To open any of the client utilities on your Windows CE device, select Start > Programs > Cisco and the utility you wish to open. The screen for that utility appears.

Exiting a Client Utility

To exit any of the client utilities, click OK at the bottom of the screen.

Determining the Version of a Client Utility

To determine which version of a utility you are running, open the utility and click the About button at the bottom of the screen. For example, if you click the About button on the ACU screen, the About screen appears (see Figure 7-5). Click OK to return to the utility’s main screen.

Deleting Client Utility Icons on HPC Devices

Icons for ACU and CEM are automatically added to the desktop of HPC devices when you install the client utilities. If you wish to remove these icons from your desktop, hold down the Alt key and tap the icon, click Delete, and click Yes to confirm your decision.

Note: You can also use File Explorer to browse to the desktop, select the icon, and delete it.
Restarting the Client Adapter

ACU enables you to restart the client adapter when necessary. For example, you might want to restart the adapter for the following reasons:

- If your client adapter is experiencing poor throughput, you might want to restart the client adapter to try to force it to disassociate from the access point to which it is currently associated in the hope that it will reassociate to an access point with a stronger signal.

- If you use LEAP and then disable it in ACU, you might want to restart the client adapter to ensure that the adapter starts to use the static WEP key set in CEM instead of the dynamic WEP key assigned during LEAP authentication.

Follow the steps below to restart the client adapter.

---

**Step 1**
Open ACU by double-clicking the **Cisco ACU icon** or selecting **Start > Programs > Cisco > Aironet Client Utility**.

**Step 2**
Click **OK** on the ACU screen. The driver stops the client adapter’s radio, writes the configuration (although no parameter settings have been changed), and restarts the radio.

---

**Note**
When you click **OK**, the ACU screen closes. You have to re-open ACU to determine if the client adapter is associated to an access point.
Restarting the Client Adapter
Troubleshooting

This chapter provides information for diagnosing and correcting common problems encountered when installing or operating the client adapter.

The following topics are covered in this chapter:

- Accessing the Latest Troubleshooting Information, page 8-2
- Interpreting the Indicator LEDs, page 8-2
- Troubleshooting the Client Adapter, page 8-3
- Error Messages, page 8-4
- Getting Help, page 8-7
Accessing the Latest Troubleshooting Information

This chapter provides basic troubleshooting tips for your client adapter. For more up-to-date and complex troubleshooting information, refer to the TAC web site at http://www.cisco.com/public/support/tac/home.shtml. Select Wireless Technologies under Top Issues.

Interpreting the Indicator LEDs

The client adapter shows messages and error conditions through its two LEDs:

- **Link Integrity/Power LED (green)** – This LED lights when the client adapter is receiving power and blinks slowly when the adapter is linked with the network.

- **Link Activity LED (amber)** – This LED blinks quickly when the client adapter is receiving or transmitting data and blinks in a repeating pattern to indicate an error condition.

Table 8-1 interprets the LED messages during normal operation. Table 8-2 interprets the LED error condition messages.

**Table 8-1  LED Normal Operating Messages**

<table>
<thead>
<tr>
<th>Green LED</th>
<th>Amber LED</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking quickly</td>
<td>Blinking quickly</td>
<td>Power is on, self-test is OK, and client adapter is scanning for a network.</td>
</tr>
<tr>
<td>Blinking slowly</td>
<td>Blinking quickly</td>
<td>Client adapter is associated to an access point.</td>
</tr>
<tr>
<td>Continuously on or blinking slowly</td>
<td>Blinking</td>
<td>Client adapter is transmitting or receiving data while associated to an access point.</td>
</tr>
<tr>
<td>Off</td>
<td>Blinking quickly</td>
<td>Client adapter is in power save mode.</td>
</tr>
<tr>
<td>On continuously</td>
<td>Blinking quickly</td>
<td>Client adapter is in ad hoc mode.</td>
</tr>
</tbody>
</table>

**Table 8-2  LED Error Condition Messages**

<table>
<thead>
<tr>
<th>Green LED</th>
<th>Amber LED</th>
<th>Condition/Recommended Action</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Off</td>
<td>Client adapter is not receiving power or an error has occurred.</td>
<td></td>
</tr>
<tr>
<td>Off</td>
<td>1 blink at 2-second rate</td>
<td>RAM failure. Refer to the “Obtaining Technical Assistance” section in the Preface for technical support information.</td>
<td></td>
</tr>
<tr>
<td>Off</td>
<td>2-second pause, 2 fast blinks, 1-second pause, 1 blink</td>
<td>A configuration error has occurred (for example, WEP is enabled in ACU, but the client adapter has not been programmed with a valid WEP key). Recheck your client adapter’s configuration settings in ACU.</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting the Client Adapter

This section provides troubleshooting tips if you encounter problems with your client adapter.

Problems Obtaining an IP Address

If your network is set up to use DHCP to acquire an IP address, the DHCP lease renewal may fail, especially in suspend/resume situations. To force DHCP to try to reacquire an IP address, power your Windows CE device off and on or eject and reinser your client adapter.

Problems Associating to an Access Point

Follow the instructions below if your client adapter fails to associate to an access point.

- If possible, move your Windows CE device a few feet closer to an access point and try again.
- Make sure the client adapter is securely inserted in your device’s PC card slot.
- Make sure the access point is turned on and operating.
- Ensure that all parameters are set properly for both the client adapter and the access point. These include the SSID, LEAP activation, WEP activation, infrastructure mode, etc.
- If the client adapter still fails to establish contact, refer to the “Obtaining Technical Assistance” section in the Preface for technical support information.
Problems Authenticating to an Access Point

If your client adapter is a 40-bit card and LEAP is enabled, the adapter can associate to but not authenticate to access points using 128-bit encryption. To authenticate to an access point using 128-bit encryption, you have two options:

- Purchase a 128-bit client adapter. This is the most secure option.
- Disable static WEP for the client adapter and configure the adapter and the access point to associate to mixed cells. This option presents a security risk because your data is not encrypted as it is sent over the RF network.

Problems Connecting to the Network

After you have installed the appropriate driver and client utilities, contact your IS department if you have a problem connecting to the network. Proxy server, DNS or WINS, and further authentication information might be needed to connect to the network.

Error Messages

This section provides a list of error messages that may appear during the installation, configuration, or use of your client adapter. The error messages are listed in alphabetical order, and an explanation as well as a recommended user action are provided for each message.

**Error Message** Cisco Aironet Wireless LAN Adapter does not support the connected device type. Application Manager will make the application available for installation when a supported device type is connected.

**Explanation** The client adapter’s software does not support the Windows CE device on which the adapter is being installed. Refer to the “System Requirements” section on page 2-4 for the list of Windows CE devices that are supported by the client adapter.

**Recommended Action** Click OK to acknowledge the message and terminate the installation process. To install the client adapter’s driver and client utilities on a supported Windows CE device, follow the instructions in the “Installing the Driver and Client Utilities on Other Windows CE Devices” section on page 3-8.

**Error Message** Cisco Wireless LAN Adapter Not Found!

**Explanation** An attempt was made to start a client utility other than ACU without a client adapter being inserted in the Windows CE device. These utilities cannot execute if a client adapter is not running because they need to be able to read from and write to the adapter.

**Recommended Action** Click OK to acknowledge the message and terminate the utility. Then insert a client adapter into the Windows CE device and start the utility.
Error Message  Cisco Wireless LAN Adapter removed!

Explanation  The client adapter was ejected while a client utility other than ACU or WLM was running.

Recommended Action  Click OK to acknowledge the message and terminate the utility. Then reinsert the client adapter and restart the utility.


Explanation  The client adapter timed out while trying to authenticate, possibly because it is out of range of an access point. The client adapter continues trying to authenticate.

Recommended Action  Click OK to acknowledge the message and terminate WLM. Then perform one of the following: 1) move the Windows CE device closer to an access point so that WLM will continue trying to authenticate or 2) double-click the WLM icon and enter a different username and password.

Error Message  Incorrect Login -- Please Re-Enter

Explanation  The LEAP username or password was entered incorrectly in the Wireless Login Module screen or was not valid for the RADIUS server on the network.

Recommended Action  Re-enter the LEAP username and password and click OK.

Error Message  LEAP Not Enabled on the Cisco Wireless LAN Adapter! Start ACU and Enable LEAP First.

Explanation  An attempt was made to start WLM before LEAP was enabled on the client adapter.

Recommended Action  Click OK to acknowledge the message and terminate the utility. Then enable LEAP in ACU. WLM restarts automatically.

Error Message  Must set a User Name

Explanation  A password was entered in the Wireless Login Module screen, but a username was not entered. The password is an optional entry, but if a password is entered, a username must also be entered.

Recommended Action  Click OK to acknowledge the message; then fill in the User Name field in the Wireless Login Module screen and click OK.

Error Message  New password doesn’t match confirm password!

Explanation  In CEM’s Change Password screen, the characters entered in the New Password and Confirm New Password fields are not identical.

Recommended Action  Click OK to acknowledge the message; then correct the entries for these fields.
Chapter 8  Troubleshooting

Error Message  Password Not Changed - Cancelled By User

Explanation  CEM’s Change Password screen was exited, but the existing password was not changed.

Recommended Action  Click OK to acknowledge the message and return to the CEM screen.

Error Message  Please enter the correct password!

Explanation  The password required to access CEM was entered incorrectly.

Recommended Action  Click OK to acknowledge the message; then re-enter the password. If the password is entered incorrectly three times in a row, the utility terminates.

Error Message  Please enter a valid existing password!

Explanation  In CEM’s Change Password screen, the existing password was entered incorrectly.

Recommended Action  Click OK to acknowledge the message; then re-enter the existing password.

Error Message  WEP Key x must be 10 Hex digits!

Explanation  An invalid number of characters or an incorrect character was entered for the WEP key indicated. 40-bit keys must have 10 characters.

Recommended Action  Click OK to acknowledge the message; then re-enter the characters for the invalid key.

Error Message  WEP Key x must be 26 Hex digits!

Explanation  An invalid number of characters or an incorrect character was entered for the WEP key indicated. 128-bit keys must have 26 characters.

Recommended Action  Click OK to acknowledge the message; then re-enter the characters for the invalid key.

Error Message  Windows CE Services not found on this computer. Setup cannot continue and will now exit.

Explanation  The driver installation utility cannot locate the ActiveSync directory on the laptop or PC. This directory and the files it contains are needed to copy the client adapter’s driver and client utility files from the laptop or PC to a Windows CE device.

Recommended Action  Click OK to acknowledge the message and terminate the installation utility. Then install Windows CE Services on the laptop or PC and start the driver installation procedure again.

Note  Windows CE Services can be obtained from the CD that shipped with your Windows CE device or from the device manufacturer.
Error Message  You must enter a WEP Key!

Explanation  The OK button on the CEM screen was clicked although a WEP key was not entered.

Recommended Action  Click OK to acknowledge the message. Then enter a WEP key in the CEM screen and click OK to save the WEP key settings or click Cancel to exit the CEM screen without entering a WEP key.

Getting Help

To access online help for ACU or CEM, follow the instructions below for your specific Windows CE device.

On HPC Devices

To access help related to ACU, CEM, or SST on an HPC device, open ACU, CEM, or SST and click the ? button on the top of the screen. Select the topic for which you want information.

On PPC Devices

To access help related to ACU, CEM, or SST on a PPC device, open ACU, CEM, or SST and select Start > Help. Select the topic for which you want information.
Technical Specifications

This appendix provides technical specifications for the Cisco Aironet 340 and 350 Series Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Physical Specifications, page A-2
- Radio Specifications, page A-3
- Power Specifications, page A-5
- Safety and Regulatory Compliance Specifications, page A-5
Table A-1 lists the technical specifications for the Cisco Aironet 340 and 350 Series Wireless LAN Client Adapters.

**Note**

If a distinction is not made between series or client adapter type, the specification applies to both 340 and 350 series PC and LM cards.

### Table A-1 Technical Specifications for the 340 and 350 Series Client Adapters

#### Physical Specifications

<table>
<thead>
<tr>
<th></th>
<th>340 series</th>
<th>350 series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>1.3 oz (0.037 kg)</td>
<td>1.3 oz (0.037 kg)</td>
</tr>
<tr>
<td>Enclosure</td>
<td>Extended Type II PC card</td>
<td>Standard Type II PC card with RF connectors</td>
</tr>
<tr>
<td>Connector</td>
<td>68-pin PCMCIA</td>
<td>68-pin PCMCIA</td>
</tr>
<tr>
<td>Status indicators</td>
<td>Green and amber LEDs; see Chapter 8</td>
<td>Green and amber LEDs; see Chapter 8</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>32°F to 158°F (0°C to 70°C)</td>
<td>–22°F to 158°F (–30°C to 70°C)</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>–40°F to 185°F (–40°C to 85°C)</td>
<td>–40°F to 185°F (–40°C to 85°C)</td>
</tr>
<tr>
<td>Humidity (non-operational)</td>
<td>95% relative humidity</td>
<td>95% relative humidity</td>
</tr>
<tr>
<td>Altitude</td>
<td>Operational</td>
<td>Non-operational</td>
</tr>
<tr>
<td></td>
<td>9843 ft (3000 m) @ room temperature for 2 hours</td>
<td>15,000 ft (4572 m) @ room temperature for 20 hours</td>
</tr>
<tr>
<td>ESD</td>
<td>15 kV (human body model)</td>
<td>15 kV (human body model)</td>
</tr>
</tbody>
</table>
### Radio Specifications

<table>
<thead>
<tr>
<th>Type</th>
<th>Direct-sequence spread spectrum (DSSS) IEEE 802.11b compliant</th>
</tr>
</thead>
</table>

**Power output**

**Note** Refer to Appendix D for limitations on radiated power (EIRP) levels in the European community and other countries.

**Note** If you are using an older version of a 340 or 350 series client adapter, your power level options may be different than those listed here.

<table>
<thead>
<tr>
<th>Series</th>
<th>Power Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>350 series</td>
<td>100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)</td>
</tr>
<tr>
<td>340 series PC card</td>
<td>30 mW (15 dBm) 1 mW (0 dBm)</td>
</tr>
<tr>
<td>340 series LM card</td>
<td>30 mW (15 dBm) 15 mW (12 dBm) 5 mW (7 dBm) 1 mW (0 dBm)</td>
</tr>
</tbody>
</table>

**Operating frequency** 2.400 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)

**Usable channels** 2412 to 2484 MHz in 5-MHz increments

**Interference rejection** –35 dBC adjacent channel rejection

**Data rates** 1, 2, 5.5, and 11 Mbps

**Modulation**
- Binary Phase Shift Keying (BPSK) - 1 Mbps
- Quaternary Phase Shift Keying (QPSK) - 2 Mbps
- Complementary Code Keying (CCK) - 5.5 and 11 Mbps

**Receiver sensitivity**

<table>
<thead>
<tr>
<th>Series</th>
<th>Sensitivity at Various Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>350 series</td>
<td>–94 dBm @ 1 Mbps</td>
</tr>
<tr>
<td></td>
<td>–91 dBm @ 2 Mbps</td>
</tr>
<tr>
<td></td>
<td>–89 dBm @ 5.5 Mbps</td>
</tr>
<tr>
<td></td>
<td>–85 dBm @ 11 Mbps</td>
</tr>
<tr>
<td>340 series</td>
<td>–90 dBm @ 1 Mbps</td>
</tr>
<tr>
<td></td>
<td>–88 dBm @ 2 Mbps</td>
</tr>
<tr>
<td></td>
<td>–87 dBm @ 5.5 Mbps</td>
</tr>
<tr>
<td></td>
<td>–83 dBm @ 11 Mbps</td>
</tr>
</tbody>
</table>
### Table A-1  Technical Specifications for the 340 and 350 Series Client Adapters (continued)

| Receiver delay spread (multipath) | 500 ns @ 1 Mbps  
|                                  | 400 ns @ 2 Mbps  
|                                  | 300 ns @ 5.5 Mbps  
|                                  | 140 ns @ 11 Mbps (350 series)  
|                                  | 70 ns @ 11 Mbps (340 series)  
| Range                            |  
| 350 series                       | **Outdoor**  
|                                  | 2000 ft (609.6 m) @ 1 Mbps  
|                                  | 1500 ft (457.2 m) @ 2 Mbps  
|                                  | 1000 ft (304.8 m) @ 5.5 Mbps  
|                                  | 800 ft (243.8 m) @ 11 Mbps  
|                                  | **Indoor**  
|                                  | 350 ft (106.7 m) @ 1 Mbps  
|                                  | 250 ft (76.2 m) @ 2 Mbps  
|                                  | 200 ft (61 m) @ 5.5 Mbps  
|                                  | 150 ft (45.7 m) @ 11 Mbps  
| **Note**                         | The above range numbers assume the use of a snap-on antenna with the LM card.  
| 340 series                       | **Outdoor**  
|                                  | 1500 ft (457.2 m) @ 1 Mbps  
|                                  | 1200 ft (365.8 m) @ 2 Mbps  
|                                  | 800 ft (243.8 m) @ 5.5 Mbps  
|                                  | 400 ft (121.9 m) @ 11 Mbps  
|                                  | **Indoor**  
|                                  | 300 ft (91.4 m) @ 1 Mbps  
|                                  | 225 ft (68.6 m) @ 2 Mbps  
|                                  | 150 ft (45.7 m) @ 5.5 Mbps  
|                                  | 100 ft (30.5 m) @ 11 Mbps  
| **Note**                         | The above range numbers assume the use of a snap-on antenna with the LM card.  
| Antenna                          |  
| PC card                          | Integrated diversity antenna  
| LM card                          | Two MMCX antenna connectors  

*OL-1375-02 Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE*
### Table A-1  Technical Specifications for the 340 and 350 Series Client Adapters  (continued)

#### Power Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational voltage</td>
<td>5.0 V (+ or – 0.25 V)</td>
</tr>
<tr>
<td>Receive current steady state</td>
<td>Typically 250 mA</td>
</tr>
<tr>
<td>Transmit current steady state</td>
<td></td>
</tr>
<tr>
<td>350 series</td>
<td>Typically 450 mA @ 20 dBm</td>
</tr>
<tr>
<td>340 series</td>
<td>Typically 350 mA @ 15 dBm</td>
</tr>
<tr>
<td>Sleep mode steady state</td>
<td></td>
</tr>
<tr>
<td>350 series</td>
<td>Typically 15 mA</td>
</tr>
<tr>
<td>340 series</td>
<td>Typically 15 mA</td>
</tr>
</tbody>
</table>

#### Safety and Regulatory Compliance Specifications

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety</td>
<td>Designed to meet:</td>
</tr>
<tr>
<td></td>
<td>• UL 1950 Third Ed.</td>
</tr>
<tr>
<td></td>
<td>• CSA 22.2 No. 950-95</td>
</tr>
<tr>
<td></td>
<td>• IEC 60950 Second Ed., including Amendments 1-4 with all deviations</td>
</tr>
<tr>
<td></td>
<td>• EN 60950 Second Ed., including Amendments 1-4</td>
</tr>
<tr>
<td>EMI and susceptibility</td>
<td>FCC Part 15.107 &amp; 15.109 Class B</td>
</tr>
<tr>
<td></td>
<td>ICES-003 Class B (Canada)</td>
</tr>
<tr>
<td></td>
<td>EN 55022 B</td>
</tr>
<tr>
<td></td>
<td>AS/NZS 3548 Class B</td>
</tr>
<tr>
<td></td>
<td>VCCI Class B</td>
</tr>
<tr>
<td></td>
<td>EN 55024</td>
</tr>
<tr>
<td>Radio approvals</td>
<td>FCC Part 15.247</td>
</tr>
<tr>
<td></td>
<td>Canada RSS-139-1, RSS-210</td>
</tr>
<tr>
<td></td>
<td>Japan Telec 33B</td>
</tr>
<tr>
<td></td>
<td>EN 300.328</td>
</tr>
<tr>
<td>RF exposure</td>
<td>OET-65C</td>
</tr>
<tr>
<td></td>
<td>RSS-102</td>
</tr>
<tr>
<td></td>
<td>ANSI C95.1</td>
</tr>
</tbody>
</table>
Translated Safety Warnings

This appendix provides translations of the safety warnings that appear in this publication. The following topics are covered in this appendix:

- Explosive Device Proximity Warning, page B-2
- Dipole Antenna Installation Warning, page B-3
- Warning for Laptop Users, page B-4
### Explosive Device Proximity Warning

<table>
<thead>
<tr>
<th>Language</th>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>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.</td>
</tr>
<tr>
<td>Waarschuwing</td>
<td>Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermd ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.</td>
</tr>
<tr>
<td>Varoitus</td>
<td>Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.</td>
</tr>
<tr>
<td>Attention</td>
<td>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.</td>
</tr>
<tr>
<td>Warnung</td>
<td>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.</td>
</tr>
<tr>
<td>Avvertenza</td>
<td>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.</td>
</tr>
<tr>
<td>Advarsel</td>
<td>Ikke bruk den trådløse nettverkseffekten nær inntil uisolerde fenghatter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.</td>
</tr>
<tr>
<td>Aviso</td>
<td>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.</td>
</tr>
<tr>
<td>¡Advertencia!</td>
<td>No utilice 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.</td>
</tr>
<tr>
<td>Warning!</td>
<td>Använd inte den trådlösa nätverkseffekten i närheten av oskyddade tändhållar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.</td>
</tr>
</tbody>
</table>
Dipole Antenna Installation Warning

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

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

**Varoitus**  
FCC:n antamien radiotaajuksille altistumista koskevien rajoitusten mukaan dipoliantennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.

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

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

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

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

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

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

**Warning!**  
För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör dipolsantener placeras på minst 20 cm avstånd från alla människor.
Warning for Laptop Users

<table>
<thead>
<tr>
<th>Language</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>In order to comply with RF exposure limits established in the ANSI C95.1 standards, it is recommended when using a laptop with a PC card client adapter that the adapter’s integrated antenna is positioned more than 2 inches (5 cm) from your body or nearby persons during extended periods of transmitting or operating time. If the antenna is positioned less than 2 inches (5 cm) from the user, it is recommended that the user limit exposure time.</td>
</tr>
<tr>
<td>Dutch</td>
<td>In het kader van een in de ANSI C95.1 norm vastgelegde limiet voor blootstelling aan straling veroorzaakt door radiofrequenties, dient u bij langdurig gebruik van een laptop met client adapter pc-kaart een afstand van meer dan 5 centimeter aan te houden tussen de geïntegreerde antenne van de adapter en uzelf en enige andere personen. Als deze afstand niet kan worden aangehouden, dient u de tijd dat het apparaat gebruikt wordt te beperken.</td>
</tr>
<tr>
<td>Finnish</td>
<td>ANSI C95.1 -standardin radiotaajuksille asettamien altistumisrajojen mukaisesti on suositeltavaa, että käytettäessä kannettavaa tietokonetta, jossa on PC-kortti-asiakas-adapteri, adapterin integroitu antenni on käännetty yli viisi cm pois vartalosta tai läheillä olevista henkilöistä pitkäaikaistenlähetyks- tai käyttöjaksojen aikana. Jos antenni on käännetty alle viisi 5 cm käyttäjästä, on suositeltavaa, että käyttäjä rajoittaa altistumisaikaa.</td>
</tr>
<tr>
<td>French</td>
<td>Afin de respecter les limitations en matière d’exposition aux fréquences radioélectriques définies par les normes ANSI C95.1, il est recommandé aux utilisateurs d’ordinateurs portables dotés d’adaptateurs client pour carte PC ou aux personnes se trouvant à proximité de se placer à plus de 5 cm de l’antenne de l’adaptateur lors de longues périodes de transmission ou de fonctionnement. Si l’utilisateur se trouve à moins de 5 cm de l’antenne, il est préférable de limiter le temps d’exposition.</td>
</tr>
<tr>
<td>German</td>
<td>In Übereinstimmung mit den in den Sicherheitsstandards ANSI C95.1 verzeichneten Höchstwerten für den Kontakt mit Radiofrequenz (RF) wird für die Benutzung eines Laptops mit PC-Adapterkarten für Clients empfohlen, bei längerer Inbetriebnahme oder Datenübertragung die integrierte Antenne des Adapters mindestens 5 cm vom Benutzer und anderen sich in der Nähe aufhaltenden Personen entfernt aufzustellen. Befindet sich die Antenne weniger als 5 cm vom Benutzer entfernt, sollte die Benutzungsdauer des Geräts eingeschränkt werden.</td>
</tr>
<tr>
<td>Italian</td>
<td>In conformità con i limiti sull’esposizione a frequenze radio stabiliti nelle direttive ANSI C95.1, quando si utilizza un computer portatile con una scheda PC dotata di adattatore client è consigliabile mantenere l’antenna integrata dell’adattatore a più di 5 cm di distanza durante periodi di esposizione prolungati. Se l’antenna è posizionata a meno di 5 cm di distanza dall’utente, è consigliabile limitare i tempi di esposizione alle frequenze.</td>
</tr>
<tr>
<td>Norwegian</td>
<td>Du må overholde begrensningene for RF-eksponering som er fastsatt i ANSI C95.1-standardene. Derfor anbefaler vi, når du bruker en bærbar PC med et klientkort i PC-format, at kortets innebygde antenne plasseres mer enn 5 cm fra deg eller personer i nærheten under lengre perioder med overføring eller bruk. Hvis antennen er plassert mindre enn 5 cm fra brukeren, anbefaler vi at brukeren begrenser eksponeringstiden.</td>
</tr>
</tbody>
</table>
Warning for Laptop Users

Aviso
Para estar em conformidade com os limites de exposição RF estabelecidos nas normas ANSI C95.1 recomenda-se que, aquando da utilização de um laptop com um adaptador de cliente PC card, a antena integrada do adaptador esteja posicionada a mais de 5 cm do seu corpo ou de pessoas na vizinhança durante longos períodos de tempo de transmissão ou operação. Se a antena estiver posicionada a menos de 5 cm do utilizador, recomenda-se que o utilizador limite o tempo de exposição.

¡Advertencia!
Para cumplir los límites de exposición a radiofrecuencia (RF) que se establecen en la norma ANSI C95.1, al utilizar un equipo portátil con un adaptador cliente de tarjeta PC, sitúe la antena del adaptador al menos a 2 pulgadas (5 cm) del usuario o de las personas adyacentes durante periodos largos de transmisión o funcionamiento. Si la distancia es inferior a 2 pulgadas (5 cm), se recomienda limitar el tiempo de exposición.

Warning!
För att följa de regler för radiosändare som utfärdats enligt ANSI-standarden C95.1, rekommenderar vi att PC Card-adapterns inbyggda antenn befinner sig minst 5 cm från dig själv och andra personer när du använder en bärbar dator med PC Card-adapter under en längre tid. Om antennen befinner sig mindre än 5 cm från användaren, rekommenderar vi inte användning under längre tid.
Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 340 and 350 Series Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Department of Communications – Canada, page C-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein, page C-4
- Declaration of Conformity for RF Exposure, page C-5
- Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan, page C-6
Manufacturer’s Federal Communication Commission Declaration of Conformity Statement


FCC Certification Number: LDK102038 (AIR-PCM34x), LDK102035 (AIR-LMC34x), LDK102040 (AIR-xxx35x)

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 modifications to said product not expressly approved by Cisco, including the use of non-Cisco antennas, 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 numérique 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.

- **Nederlands**: Deze apparatuur voldoet aan de essentiële vereisten en andere relevante voorzieningen van EU-richtlijn 1999/5/EC.

- **Suomalainen**: Tämä laite noudattaa direktiivin 1999/5/EC keskeisiä vaatimuksia ja sen muita olennaisia määräyksiä.

- **Français**: Cet équipement répond aux exigences et provisions de la Directive 1999/5/EC.

- **Deutsch**: Diese Geräte entsprechen den Anforderungen und anderen relevanten Bestimmungen der Richtlinie 1999/5/EC.

- **Italiano**: Questa apparecchiatura rispetta i requisiti essenziali e le altre clausole rilevanti della Direttiva 1999/5/CE.

- **Dansk**: Dette utstyret er i samsvar med de grunnleggende kravene og andre relevante forskrifter i 1999/5/EC-direktivet.

- **Português**: Este equipamento está de acordo com os requisitos essenciais e outras provisões relevantes da Diretiva 1999/5/EC.

- **Español**: Este equipo cumple con los requisitos esenciales y otras provisiones relevantes de la Directiva 1999/5/EC.

- **Svenska**: Denna utrustning uppfyller de väsentliga kraven och andra relevanta förordningar i Direktiv 1999/5/EC.

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

![CE mark for 340 series]

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:

![CE mark for 350 series]

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 your customer service representative.

Note
Combinations of power levels and antennas resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and other countries that have adopted the European R&TTE directive 1999/5/EC or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas, refer to the “Maximum Power Levels and Antenna Gains” section on page D-3.

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 Wireless LAN Client Adapters in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet Wireless LAN Client Adapters 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: 03-5219-6000
Channels, Power Levels, and Antenna Gains

This appendix lists the channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.

The following topics are covered in this appendix:

- Channels, page D-2
- Maximum Power Levels and Antenna Gains, page D-3
Channels

The channel identifiers, channel center frequencies, and regulatory domains of each 22-MHz-wide channel are shown in Table D-1.

Table D-1 Channels

<table>
<thead>
<tr>
<th>Channel Identifier</th>
<th>Frequency</th>
<th>Americas (-A)</th>
<th>ETSI (-E)</th>
<th>Israel (-I)</th>
<th>China (-C)</th>
<th>Japan (-J)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412 MHz</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>2417 MHz</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>2422 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>2427 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>2432 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>2437 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7</td>
<td>2442 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>2447 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>9</td>
<td>2452 MHz</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td>2457 MHz</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>11</td>
<td>2462 MHz</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>12</td>
<td>2467 MHz</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>13</td>
<td>2472 MHz</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>14</td>
<td>2484 MHz</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

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

Note: France is included in the ETSI regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of France.
Maximum Power Levels and Antenna Gains

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

Table D-2  Maximum Power Levels Per Antenna Gain

<table>
<thead>
<tr>
<th>Regulatory Domain</th>
<th>Antenna Gain (dBi)</th>
<th>Maximum Power Level (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas (-A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(4 watts EIRP maximum)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>8.5</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>13.5</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>20</td>
</tr>
<tr>
<td>ETSI (-E)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(100 mW EIRP maximum)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>8.5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>13.5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>Israel (-I)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(100 mW EIRP maximum)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>8.5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>13.5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>1</td>
</tr>
</tbody>
</table>
### Table D-2  Maximum Power Levels Per Antenna Gain (continued)

<table>
<thead>
<tr>
<th>Regulatory Domain</th>
<th>Antenna Gain (dBi)</th>
<th>Maximum Power Level (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>China (-C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10 mW EIRP maximum)</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>8.5</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>13.5</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>n/a</td>
</tr>
<tr>
<td>Japan (-J)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10 mW/MHz EIRP maximum)</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>8.5</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>13.5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Performing a Site Survey

This appendix explains how the Site Survey Tool (SST) utility can be used when conducting a site survey.

The following topics are covered in this appendix:

- Overview, page E-2
- Using Passive Mode, page E-3
- Using Active Mode, page E-5
- Forcing the Client Adapter to Reassociate, page E-10
Overview

This appendix applies only to people who are responsible for conducting a site survey to determine the best placement of infrastructure devices within a wireless network.

The Site Survey Tool (SST) utility can assist you in conducting a site survey. SST operates at the RF level and is used to determine the best placement and coverage (overlap) for your network’s infrastructure devices. During a site survey, the current status of the network is read from the client adapter and displayed four times per second so you can accurately gauge network performance. The feedback that you receive can help you to eliminate areas of low RF signal levels that can result in a loss of connection between the client adapter and its associated access point (or other infrastructure device).

SST can be operated in two modes:

- **Passive Mode** – This is the default site survey mode. It does not initiate any RF network traffic; it simply listens to the traffic that the client adapter hears and displays the results. Follow the instructions in the “Using Passive Mode” section on page E-3 to activate the passive mode.

- **Active Mode** – This mode causes the client adapter to actively send or receive low-level RF packets to or from its associated access point and provides information on the success rate. It also enables you to set parameters governing how the site survey is performed (such as the data rate). Follow the instructions in the “Using Active Mode” section on page E-5 to activate the active mode.

Guidelines

Keep the following guidelines in mind when preparing to perform a site survey:

- Use the active mode when performing a site survey.
- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.
- Conduct the site survey with all variables set to operational values.

Additional Information

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

- **Data rates** – Sensitivity and range are inversely proportional to data bit rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and 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 the performance of wireless devices. Avoid placing these devices in a location where a metal barrier is 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, and metal or steel construction is a barrier to radio signals.

**Note** Refer to the Hardware Installation Guide for your infrastructure device for additional information on factors affecting placement.

### Using Passive Mode

Follow the steps below to activate the site survey passive mode and obtain current information about RF network traffic.

**Step 1** Select **Start > Programs > Cisco > Site Survey Tool**. The Site Survey - Passive screen appears (see **Figure E-1**), provided a client adapter is installed in the Windows CE device and is running.

**Note** This screen and the other screens in this chapter represent Windows CE devices with both a display width and a display height greater than 240 pixels, such as the HP Jornada 820 display of 640 x 480. On Windows CE devices with smaller displays, the site survey screens vary slightly from the screens shown here.

**Figure E-1 Site Survey - Passive Screen**

![Site Survey - Passive Screen](image)
Table E-1 interprets the information that is displayed on the Site Survey - Passive screen.

**Table E-1 Site Survey Passive Mode Statistics**

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first line of the Site Survey - Passive screen</td>
<td>Indicates the operational mode of your client adapter and the name or MAC address of any associated access point. Value: Associated, Not Associated, Authenticated, or Ad Hoc Mode</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal. The histogram below the bar graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest). Range: 0 to 100%</td>
</tr>
<tr>
<td>Signal Quality (Beacons Received is displayed instead if your firmware version is less than 4.05)</td>
<td>The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal. The histogram below the bar graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality). Range: 0 to 100%</td>
</tr>
<tr>
<td>Link Speed</td>
<td>The rate at which your client adapter is receiving echo packets from its associated access point. The Link Speed histogram provides a visual interpretation of the current rate at which your client adapter is receiving packets. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest). Value: 1, 2, 5.5, or 11 Mbps Note To examine real-time link speed for your client adapter, use the active mode. In passive mode, the link-speed indicator reports the speed of echo packets and does not indicate real-time link speed.</td>
</tr>
<tr>
<td>Overall Link Quality</td>
<td>The client adapter’s ability to communicate with the access point. Value: Not Associated, Poor, Fair, Good, Excellent</td>
</tr>
</tbody>
</table>

**Step 2** If you want to activate the site survey active mode, go to the “Using Active Mode” section on page E-5. Otherwise, click **OK** or **Cancel** to exit the site survey application.
Using Active Mode

Follow the steps below to activate the site survey active mode and obtain current information about your client adapter’s ability to transmit and receive RF packets.

**Step 1**
From the Site Survey - Passive screen (see Figure E-1), click the **Setup** button. The Active Mode Setup screen appears (see Figure E-2).

*Figure E-2  Active Mode Setup Screen*

![Active Mode Setup Screen]

Table E-2 lists and describes the parameters that affect how the site survey is performed. Follow the instructions in the table to set any parameters.
### Table E-2 Site Survey Active Mode Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination MAC Address          | The MAC address of the access point (in infrastructure mode) or other clients (in ad hoc mode) that will be used in the test.  
**Default:** The MAC address of the access point (in infrastructure mode) to which your client adapter is associated  
**Note:** During the test, the client adapter will not roam to other access points so that the size of a single cell can be determined. |
| Destination Is Another Cisco Aironet Device | Selecting this checkbox indicates that the device you named in the Destination MAC Address field is a Cisco Aironet access point (in infrastructure mode) or client (in ad hoc mode). In this case, packets sent to the client from the Cisco Aironet device contain additional information, such as lost to source, lost to target, and percent retries, and this information is displayed in the Site Survey - Active screen.  
If the device specified in the Destination MAC Address field is not a Cisco Aironet device, do not select this checkbox. In this case, the test sends out loopback packets, which originate from and return to the client adapter.  
**Default:** Selected |
| Number of Packets                | The number of packets that will be sent during the test.  
**Range:** 1 to 999  
**Default:** 100 |
| Data Rate                        | The bit rate at which packets will be transmitted. Rate shifting will not occur during the test because the echo test built into the radio firmware does not support it  
**Value:** 1, 2, 5.5, or 11 Mbps  
**Default:** 11 Mbps |
| Continuous Link Test             | Selecting this checkbox causes the test to run until you click OK or Stop. The test loops repeatedly for the number of packets specified in the Number of Packets field.  
**Default:** Deselected |
| Packet Size                      | The size of the packets that will be sent during the test. Select a size that will be typical during normal system use.  
**Range:** 30 to 1450  
**Default:** 512 |
| Delay Between Packets            | The delay (in milliseconds) between successive transmissions.  
**Range:** 1 to 2048 ms  
**Default:** 50 ms |
Table E-2  Site Survey Active Mode Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Percent Success Threshold  | The percentage of packets that are not lost.  
This parameter controls the red line on the Percent Successful histogram. Percentages greater than or equal to this value are displayed as green bars; percentages below this value are displayed as yellow bars.  
**Range:** 0 to 100%  
**Default:** 75 |
| Data Retries               | The number of times a transmission will be retried if an acknowledgment (Ack) is not returned by the destination device.  
**Default:** None |
| Retry Value                | Description                                                                                                                                 |
| None                       | No retries will occur.                                                                                                                       |
| Default Retries            | The firmware’s default value for retries (16) will be used.                                                                                   |
| Tx Type                    | The packet type that will be transmitted during the test.  
**Default:** Unicast |
| Packet Type                | Description                                                                                                                                 |
| Unicast                    | When unicast packets are used, the system expects to receive an acknowledgment from the destination, and retries can occur.                |
| Multicast                  | When multicast packets are used, no packet retries occur during the test.                                                                     |

**Step 2**  
After setting any parameters, click **OK** to save the settings. The Site Survey - Passive screen appears (see Figure E-1).

**Step 3**  
Click the **Start** button to run the site survey test. The Site Survey - Active screen appears (see Figure E-3).
**Figure E-3**  Site Survey - Active Screen

![Site Survey - Active Screen](image)

**Table E-3** Site Survey Active Mode Statistics

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first line of the Site Survey - Active screen</td>
<td>Indicates the operational mode of your client adapter and the name or MAC address of any associated access point. <strong>Value:</strong> Associated, Not Associated, Authenticated, or Ad Hoc Mode</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal. The histogram below the bar graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest). <strong>Range:</strong> 0 to 100%</td>
</tr>
</tbody>
</table>
### Table E-3 Site Survey Active Mode Statistics (continued)

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal Quality (Beacons Received is displayed instead if your firmware version is less than 4.05)</td>
<td>The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal. The histogram below the bar graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality). <strong>Range:</strong> 0 to 100%</td>
</tr>
<tr>
<td>Link Speed</td>
<td>The rate at which your client adapter is transmitting or receiving packets to or from its associated access point. The Link Speed histogram provides a visual interpretation of the current rate at which your client adapter is transmitting or receiving packets. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest). <strong>Value:</strong> 1, 2, 5.5, or 11 Mbps</td>
</tr>
<tr>
<td>Overall Link Quality</td>
<td>The client adapter’s ability to communicate with the access point. <strong>Value:</strong> Not Associated, Poor, Fair, Good, Excellent</td>
</tr>
<tr>
<td>Percent Complete</td>
<td>The percentage of packets that have been transmitted based on the number specified in the Number of Packets field.</td>
</tr>
<tr>
<td>Percent Successful</td>
<td>The percentage of packets that were transmitted successfully. The Percent Successful histogram provides a visual interpretation of the percentage of packets that are not lost. The value you set for the Percent Success Threshold is indicated by the red line. Percentages greater than or equal to this value are displayed as green bars; percentages below this value are displayed as yellow bars. <strong>Note</strong> Refer to the Percent Success Threshold parameter in Table E-2 for more information.</td>
</tr>
<tr>
<td>Lost To Target</td>
<td>The number of packets that were not transmitted successfully to the access point.</td>
</tr>
<tr>
<td>Lost To Source</td>
<td>The number of packets that were not received successfully from the access point.</td>
</tr>
<tr>
<td>Percent Retries</td>
<td>The percentage of packets that were retried for transmission. <strong>Note</strong> This value is calculated as follows: (number of retries x 100) / number of packets sent If a lot of packets get lost, the number of retries could be greater than the number of packets sent. Then this field would show a value greater than 100%.</td>
</tr>
</tbody>
</table>
Forcing the Client Adapter to Reassociate

A client adapter will attempt to maintain its association to an access point for as long as it can. Therefore if you are on a fringe area while conducting a site survey, you may want to try to force the adapter to disassociate from the access point to which it is currently associated in the hope that it will reassociate to another access point.

Follow the steps below to attempt to force the client adapter to disassociate from its current access point and reassociate to another during a site survey.

Step 1  While SST is open, double-click the Cisco ACU icon or select Start > Programs > Cisco > Aironet Client Utility to also open ACU.

Step 2  Click OK on the ACU screen. The first line of the Site Survey screen displays “Not Associated” while the client adapter disassociates from its current access point and then displays “Associated” once the adapter is reset and reassociated to an access point.

Step 4  When you click the Stop button or when the Percent Complete reaches 100%, the active mode changes back to the passive mode.

Step 5  Click OK or Cancel to exit the site survey application.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.11</strong></td>
<td>The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs.</td>
</tr>
<tr>
<td><strong>802.11b</strong></td>
<td>The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs.</td>
</tr>
</tbody>
</table>

**A**

- **Access Point**: A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- **ActiveSync**: A Microsoft program that enables desktop-to-Windows CE device connection in order to transfer files.
- **Ad Hoc Network**: A wireless network composed of stations without access points.
- **Alphanumeric**: A set of characters that contains both letters and numbers.
- **Associated**: A station is configured properly to allow it to wirelessly communicate with an access point.

**B**

- **Bandwidth**: Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant power loss.
- **BPSK**: A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 1 Mbps.
- **Broadcast key rotation**: A security feature for use with dynamic WEP keys. If your client adapter uses LEAP or EAP-TLS authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

**C**

- **Cabinet File**: A self-contained file with a .cab extension used for application installation and setup. In a cabinet file, multiple files are compressed into one file. Cabinet files are commonly found on software distribution disks.
- **CCK**: Complementary code keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
CeAppMgr  Windows CE Application Manager. The desktop Windows CE Services component that provides a desktop-to-device application management tool. It is responsible for adding and removing applications on the Windows CE device and for deleting the application files from the desktop computer. CeAppMgr is included with every installation of Windows CE Services.

Client  A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.

CSMA  Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

Cyclic Redundancy Check (CRC)  A method of checking for errors in a received packet.

Data Rates  The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi  A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and the more acute the angle of coverage.

DHCP  Dynamic Host Configuration Protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

Dipole  A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

Domain Name Server  A network server that translates text names to IP addresses.

Domain Name System (DNS)  Provides names for computers using alphanumeric characters instead of numbers like IP addresses use. Maintains a database of the host alphanumeric names and their corresponding IP addresses.

DSSS  Direct-sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

Duplicate Packets  Packets that were received twice because an acknowledgement got lost and the sender retransmitted the packet.

EAP  Extensible Authentication Protocol. EAP is the protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

Ethernet  The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 megabits per second (Mbps), depending on the physical layer used.
<table>
<thead>
<tr>
<th><strong>F</strong></th>
<th><strong>G</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Server</strong></td>
<td>A repository for files so that a local area network can share files, mail, and programs.</td>
</tr>
<tr>
<td><strong>Firmware</strong></td>
<td>Software that is programmed on a memory chip and kept in a computer’s semi-permanent memory.</td>
</tr>
<tr>
<td><strong>Fragmentation Threshold</strong></td>
<td>The size at which packets will be fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 64 to 2312 bytes.</td>
</tr>
<tr>
<td><strong>G</strong></td>
<td><strong>Gateway</strong></td>
</tr>
<tr>
<td></td>
<td>A device that connects two otherwise incompatible networks together.</td>
</tr>
<tr>
<td><strong>GHz</strong></td>
<td>Gigahertz. One billion cycles per second. A unit of measure for frequency.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>H</strong></th>
<th><strong>I</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hexadecimal</strong></td>
<td>A set of characters consisting of ten numbers and six letters (0-9, A-F, and a-f).</td>
</tr>
<tr>
<td><strong>HPC</strong></td>
<td>Handheld Personal Computer. One of the three defined types of Windows CE devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IEEE</strong></th>
<th><strong>Infrastructure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.</td>
<td></td>
</tr>
<tr>
<td><strong>Infrastructure Device</strong></td>
<td>The wired Ethernet network.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>A device that connects client adapters to a wired LAN, such as an access point, bridge, or base station.</td>
</tr>
<tr>
<td><strong>IP Subnet Mask</strong></td>
<td>The Internet Protocol (IP) address of a station.</td>
</tr>
<tr>
<td><strong>Isotropic</strong></td>
<td>The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.</td>
</tr>
<tr>
<td><strong>Isotropic</strong></td>
<td>An antenna that radiates its signal 360 degrees both vertically and horizontally in a perfect sphere.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>L</strong></th>
<th><strong>LEAP</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>LEAP, or <em>EAP-Cisco Wireless</em>, is the 802.1X authentication type that is available on Windows CE devices. Support for LEAP is provided in the client adapter’s firmware and the Cisco software that supports it, rather than in the operating system. With LEAP, a username and password are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.</td>
<td></td>
</tr>
</tbody>
</table>
### Glossary

#### M

**MAC Address**
The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.

**MIC**
Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter’s driver and firmware must support MIC functionality, and MIC must be enabled on the access point.

**Modulation**
Any of several techniques for combining user information with a transmitter’s carrier signal.

**Multicast Packets**
Packets transmitted to multiple stations.

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

#### O

**Overrun Packets**
Packets that were discarded because the access point had a temporary overload of packets to handle.

#### P

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

**PPC**
Pocket-sized Personal Computer. One of the three defined types of Windows CE devices.

#### Q

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

#### R

**Radio Channel**
The frequency at which a radio operates.

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

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

**RF**
Radio frequency. A generic term for radio-based technology.
Roaming
A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RTS Threshold
The packet size at which an access point will issue a request to send (RTS) before sending the packet.

S

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

SSID
Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

TKIP
Temporal Key Integrity Protocol. Also referred to as WEP key hashing. A security feature that defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.

Transmit Power
The power level of radio transmission.

U

Unicast Packets
Packets transmitted in point-to-point communication.

W

WCELoad
A Windows CE tool that unpacks a Windows CE .cab file to install an application on a device. It is included with most Windows CE devices.

WEP
Wired equivalent privacy. An optional security mechanism defined within the 802.11 standard designed to protect your data as it is transmitted through your wireless network by encrypting it through the use of encryption keys.

Workstation
A computing device with an installed client adapter.
Symbols

? button, function of  1-5

Numerics

802.1X  4-3

A

About button, function of  1-5
About screen  7-12
access points
in wireless infrastructure  1-7
problems associating to  8-3
problems authenticating to  8-4
role in wireless network  1-6
security settings  4-5
Active Mode Setup screen  E-5
ACU screen  3-5, 4-4, 4-9, 4-12, 5-2, 7-5, 7-9
ad hoc mode  5-3
ad hoc wireless LAN  1-6
advanced configuration  5-2 to 5-8
Aironet Client Utility (ACU)
described  1-5
using  5-2 to 5-8
antenna
described  1-3

gains  D-3 to D-4
placement  E-2
specifications  A-4
type  E-2

B

beacon packets, number received  6-4
broadcast key rotation
described  4-5
setting on client and access point  4-5
broadcast packets
number received  6-4
number transmitted  6-5
bytes
number received  6-4
number transmitted  6-5

C

CAM  5-4
Canadian compliance statement  C-3
Cancel button, function of  1-5
Card and Socket Services  2-4
cautions, defined  ix
CEM password, changing  4-10 to 4-11
CEM screen  4-7, 4-8, 4-9
Change Password screen  4-10
channels  D-2
Cisco.com, obtaining technical assistance  xii
Cisco Link Status (CLS)
described  1-5
using  6-2 to 6-3
Cisco Link Status screen  6-2
Client Encryption Manager (CEM)
- described 1-5
- entering password 4-6
- opening 4-6
- using 4-6 to 4-11

Client Name parameter 3-6, 5-3, 7-10

Client Statistics Utility (CSU)
- described 1-5
- using 6-3 to 6-7

Client utilities
- buttons described 1-5
- deleting icons 7-12
- described 1-4 to 1-5
- determining version of 7-12
- exiting 7-12
- installing 3-3 to 3-7
- installing on other Windows CE devices 3-8
- opening 7-12
- uninstalling 7-6 to 7-7
- upgrading 7-5 to 7-11

configuring client adapter 5-2 to 5-8

Continuous Link Test parameter E-6

conventions of document ix to x

CRC errors 6-4

D

Data Rate parameter E-6

data rates A-3, E-2

Data Rates parameter 3-7, 5-7, 7-11

Data Retries parameter E-7

declarations of conformity
- European community, Switzerland, Norway, Iceland, and Liechtenstein C-4 to C-5
- FCC C-2
- RF exposure C-5

Defaults button, function of 1-5

default values, setting 1-5

Delay Between Packets parameter E-6

Destination Is Another Cisco Aironet Device parameter E-6

Destination MAC Address parameter E-6
diagnostic utilities, overview 6-2
disassociating client adapter from access point 7-13
diversity antenna 1-3
document
- audience viii
- conventions ix to x
- organization viii
- purpose viii
documentation
- CD-ROM xi
- feedback xii
- obtaining xi to xii
- ordering xii
domain name, entering with LEAP username 4-13
driver
- described 1-4
- determining latest version 3-2
- determining version of 7-6
- installing 3-3 to 3-7
- installing on other Windows CE devices 3-8
- uninstalling version 1.4 for Windows CE 2.11 7-6 to 7-7
- uninstalling version 1.5 or later for Windows 2.11 or 3.0 7-7
- upgrading 7-5 to 7-11
- verifying installation 3-8
dynamic WEP keys with LEAP, overview 4-3

E

EIRP, maximum 1-3, D-3 to D-4

Enter Password screen 4-6

error messages 8-4 to 8-7

Extensible Authentication Protocol (EAP) 4-3
F

Fast PSP 5-4

FCC
deceleration of conformity statement C-2
safety compliance statement 2-2

firmware
described 1-4
determining version of 7-3
matching 802.1X draft standards 7-3
upgrading 7-3 to 7-5

frequencies D-2

H

hardware components of client adapter 1-3
help
on HPC devices 8-7
on PPC devices 8-7

I

infrastructure devices
defined 1-2
site requirements 2-5
Infrastructure Mode parameter 5-3
inserting client adapter into Windows CE device 7-2
interference 2-5
IP address
obtaining 7-9
problems obtaining 8-3
specifying 7-9

J

Japan, guidelines for operating client adapters C-6

L

LEAP
device-level 4-3
disabling 4-14
enabling 4-11, 4-12, 7-3
entering username and password 4-12 to 4-14
overview 4-3
parameter 5-5
procedures 4-11 to 4-14
setting on client and access point 4-5

LEDs
described 1-3
interpreting 8-2

link quality
in active site survey E-9
in passive site survey E-4

of client adapter 6-3

link speed
in active site survey E-9
in passive site survey E-4

LM card
antenna 1-3
described 1-2

Load New Firmware (LNF)
described 1-5
using 7-3 to 7-5

Load New Firmware screen 7-5

M

MAC CRC errors 6-5
Max PSP 5-4
message integrity check (MIC)
described 4-4
setting on client and access point 4-5
statistics 6-6 to 6-7

microcellular network 1-7
<table>
<thead>
<tr>
<th>MIC Statistics screen</th>
<th>E-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mixed Mode parameter</td>
<td>5-6</td>
</tr>
<tr>
<td>multicast packets</td>
<td></td>
</tr>
<tr>
<td>in active site survey</td>
<td>E-7</td>
</tr>
<tr>
<td>number received</td>
<td>6-4</td>
</tr>
<tr>
<td>number transmitted</td>
<td>6-5</td>
</tr>
</tbody>
</table>

**N**

network

configurations 1-6 to 1-7
problems connecting to 8-4
note, defined ix
Number of Packets parameter E-6

**O**

OK button, function of 1-5
open authentication 5-5
Open window 7-5
organization of document viii

**P**

package contents 2-3
packets

discarded due to MIC error 6-6 to 6-7
lost to source E-9
lost to target E-9
max retries 6-6
received with MIC 6-6
retry long 6-5
retry short 6-6
Packet Size parameter E-6
PC card

antenna 1-3
described 1-2
inserting into Windows CE device 7-2
removing from Windows CE device 7-2
peer-to-peer wireless LAN 1-6
percent complete, in active site survey E-9
percent successful, in active site survey E-9
Percent Successful histogram E-7, E-9
Percent Success Threshold parameter E-7
physical specifications A-2
PLCP CRC errors 6-4
power level

maximum D-3 to D-4
options A-3
Power Save Mode parameter 5-4
power specifications A-5
purpose of document viii

**R**

radio
described 1-3
specifications A-3 to A-4
RADIUS servers 4-3
range 3-7, 5-7, 7-11
reassociating client adapter E-10
receive statistics 6-4
Receive Statistics screen 6-4
regulatory
domains D-2
information C-2 to C-6
specifications A-5
related publications xi
removing client adapter from Windows CE device 7-2
restarting client adapter 7-13
RF obstructions 2-5, E-3
roaming 1-7
RTS packets, number retransmitted 6-6
S

safety
  information  2-2 to 2-3
  specifications  A-5

seamless roaming  1-7

security features
  overview  4-2 to 4-5
  synchronizing  4-5

sensitivity  A-3

shared key authentication  5-5

signal quality
  in active site survey  E-9
  in passive site survey  E-4
  of client adapter  6-3

signal strength
  in active site survey  E-8
  in passive site survey  E-4
  of client adapter  6-3

site requirements
  for client devices  2-5
  for infrastructure devices  2-5

site survey
  active mode  E-2, E-5 to E-10
  guidelines  E-2
  overview  E-2 to E-3
  passive mode  E-2, E-3 to E-4

Site Survey - Active screen  E-8
Site Survey - Passive screen  E-3

Site Survey Tool (SST)
  described  1-5
  using  E-3 to E-10

software, upgrading  7-3 to 7-11

software components of client adapter  1-4

specifications
  physical  A-2
  power  A-5
  radio  A-3 to A-4

regulatory compliance  A-5

safety  A-5

spread spectrum  1-3

SSID parameter  3-6, 5-3, 7-10

Start button, function of  1-5

static WEP
  disabling  4-11
  enabling  4-7 to 4-9
  procedures  4-6 to 4-11
  with open authentication, setting on client and access point  4-5
  with shared key authentication, setting on client and access point  4-5

static WEP keys
  entering  4-7 to 4-9
  guidelines for entering  4-8
  overview  4-2
  overwriting  4-9 to 4-10
  selecting transmit key  4-8
  size of  4-8
  viewing current settings  4-7

statistics of client adapter, viewing  6-3 to 6-7

status of client adapter, viewing  6-2 to 6-3

Stop button, function of  1-5

system requirements  2-4

T

technical assistance, obtaining  xii to xiv

Technical Assistance Center, contacting  xiii to xiv

Temporal Key Integrity Protocol (TKIP)  4-5

throughput  3-7, 5-4, 5-7, 7-11, 7-13

Transmit Power parameter  5-8

transmit statistics  6-5

Transmit Statistics screen  6-5

troubleshooting information  8-2 to 8-4
### U

**unicast packets**
- in active site survey [E-7]
- number received [6-4]
- number transmitted [6-5]

**unpacking the client adapter** [2-3]

**up time** [6-5, 6-6]

### W

**warning**
- defined [ix]
- dipole antenna [2-3, B-3]
- explosive device proximity [2-3, B-2]
- laptop users [2-3, B-4]

**WEP**
- enabling [5-4]
- parameter [5-4]

**WEP key hashing** [4-5]

**WEP keys**
- defined [4-2, 5]
- size of [4-2]

**Windows CE**
- determining version of [3-2]
- supported devices [2-4]

**wireless infrastructure** [1-7]

**Wireless Login Module (WLM)**
- described [1-5]
- using [4-12 to 4-14]

**Wireless Login Module screen** [4-13]

**workstation**
- defined [1-2]
- in wireless infrastructure [1-7]

**World Mode parameter** [5-6]

### X

**X button, function of** [1-5]