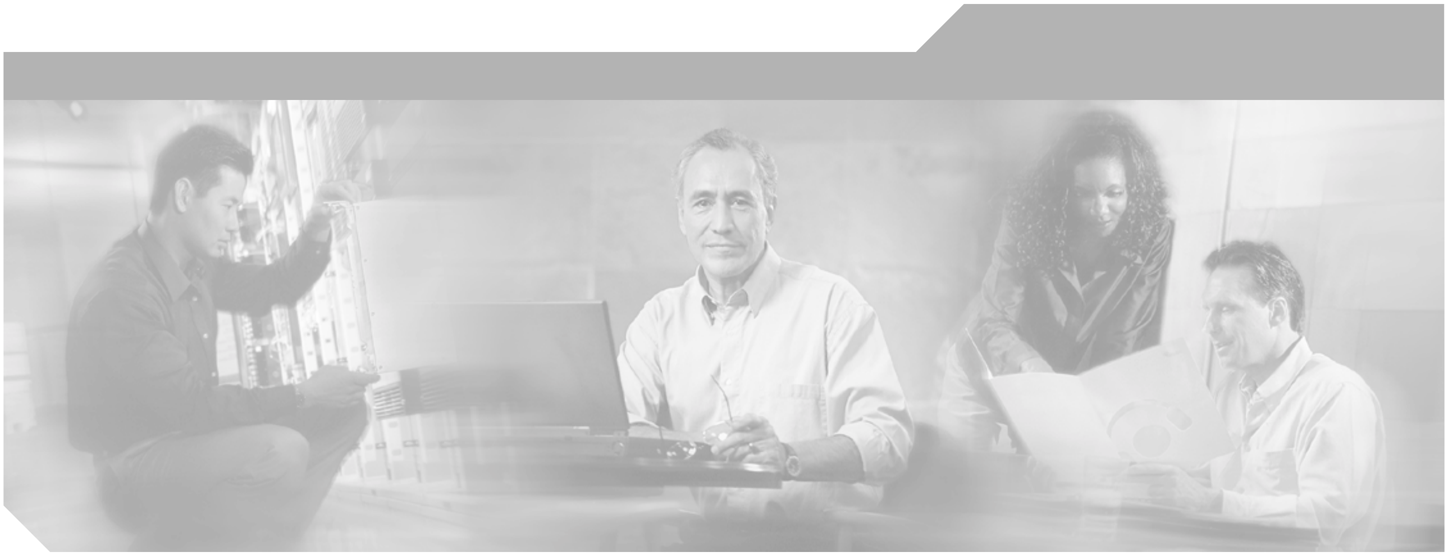
BETA DRAFT - CISCO CONFIDENTIAL



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

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-1394-03

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, GigaStack, 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)

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

CONTENTS

BETA DRAFT - CISCO CONFIDENTIAL

Preface

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

The following topics are covered in this section:

Audience

This publication is for the person responsible for installing, configuring, and maintaining a Cisco Aironet Wireless LAN Client Adapter on a computer running Windows 95, 98, NT, 2000, Me, or XP. This person should be familiar with computing devices and with network terms and concepts.

Purpose

This publication describes the Cisco Aironet client adapters and explains how to install, configure, and troubleshoot them.

Organization

This publication contains the following chapters:

- Chapter 1, "Product Overview," describes the types of client adapters and their hardware and software components 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 utility as well as setting basic configuration parameters.
- Chapter 4, "Using the Profile Manager," explains how to use the Aironet Client Utility (ACU) profile manager feature to create and manage profiles for your client adapter.
- Chapter 5, "Configuring the Client Adapter," explains how to change the configuration parameters for a specific profile.
- Chapter 6, "Using EAP Authentication," explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is selected for use.
- Chapter 7, "Performing Diagnostics," explains how to use ACU to perform user-level diagnostics.
- Chapter 8, "Routine Procedures," provides procedures for common tasks related to the client adapter, such as upgrading client software and restarting the adapter.
- Chapter 9, "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 adapters' safety warnings in nine languages.
- Appendix C, "Declarations of Conformity and Regulatory Information," provides declarations of conformity and regulatory information for the client adapters.
- Appendix D, "Channels, Power Levels, and Antenna Gains," lists the IEEE 802.11a and IEEE 802.11b channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per domain.

- Appendix E, "Configuring the Client Adapter through Windows XP," explains how to configure and use the client adapter with Windows XP.
- Appendix F, "Performing a Site Survey," shows people who are responsible for conducting a site survey how they can use ACU 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 aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

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

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

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

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

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

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

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

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

Related Publications

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

- *Release Notes for Cisco Aironet Client Utilities for Windows*
- *Release Notes for Cisco Aironet Client Adapter Drivers for Windows*
- *Release Notes for Cisco Aironet Client Adapter Firmware*
- *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE*
- *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*

For more information about related Cisco Aironet products, refer to the following publications:

- *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

These 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 this URL:

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped separately from the CD that was included 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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing 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 online 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 with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

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

Cisco TAC inquiries 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.

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

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service 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 this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

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

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

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). When you call the center, please have available your service agreement number and your product serial number.

CHAPTER 1

Product Overview

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

The following topics are covered in this chapter:

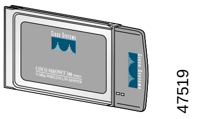
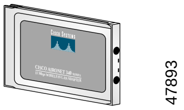
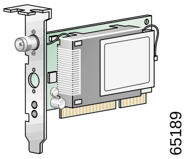
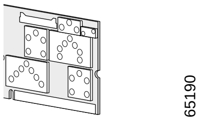
Introduction to the Client Adapters

The Cisco Aironet Wireless LAN Client Adapters are 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 the five client adapters described in Table 1-1.

Table 1-1 Client Adapter Types

Client Adapter	Model Number	Description	Illustration
PC card	AIR-PCM3*xx*	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz 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. The PC card is available in the 340 and 350 series.	
LM card	AIR-LMC3*xx*	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz PCMCIA card radio module that is usually preinstalled in a device equipped with an *internal* Type II or Type III PC card slot. Host devices usually include handheld or portable devices. The LM card is available in the 340 and 350 series.	
PCI card	AIR-PCI3*xx*	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot, such as a desktop personal computer. The PCI card is available in the 340 and 350 series.	
Mini PCI card	AIR-MPI350	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz client adapter card radio module that is preinstalled in a device equipped with an *internal* Type IIIA mini PCI card slot, such as a laptop computer. The mini PCI card is available only in the 350 series.	
PC-Cardbus card	AIR-CB20A	An IEEE 802.11a-compliant 54-Mbps 5-GHz client adapter card radio module with a Cardbus interface that can be inserted into any device equipped with an *external* Type II or Type III Cardbus slot. Host devices can include laptops, notebook computers, personal digital assistants, and handheld or portable devices.	

Note In the first three product model numbers, the first *x* represents the client adapter series (340 or 350), and 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. If the last two product model numbers contain K9, the card is 128-bit WEP capable.

Terminology

The following terms are used throughout this document:

- **client adapter** – Refers to all five types of adapters.
- **PC card**, **LM card**, **PCI card**, **mini PCI card**, or **PC-Cardbus card** – Refers to 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

Different radios are used for the 2.4-GHz and 5-GHz client adapters:

- The Cisco Aironet 340 and 350 series PC, LM, PCI, and mini PCI cards are IEEE 802.11b-compliant client adapters. They contain a direct-sequence spread spectrum (DSSS) radio that operates in the 2.4-GHz Industrial Scientific Medical (ISM) license-free band. The 340 series 30-milliwatt (mW) radio and the 350 series 100-mW radio transmit data over a half-duplex radio channel operating at up to 11 Mbps. These cards interoperate with other IEEE 802.11b-compliant client devices in ad hoc (or *peer-to-peer*) mode or with Cisco Aironet 340, 350, and 1200 Series Access Points (with a 2.4-GHz radio) and other IEEE 802.11b-compliant infrastructure devices in infrastructure mode. They are approved for indoor and outdoor use.

  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.
- The Cisco Aironet AIR-CB20A PC-Cardbus card is an IEEE 802.11a-compliant client adapter. It contains an orthogonal frequency division multiplexing (OFDM) radio that operates in the Unlicensed National Information Infrastructure (UNII) 1 and UNII 2 license-free bands located in the lower 5-GHz portion of the radio frequency spectrum. The 20-mW radio transmits data over a half-duplex radio channel operating at up to 54 Mbps. This card interoperates with other IEEE 802.11a-compliant client devices in ad hoc mode or with Cisco Aironet 1200 Series Access Points (with a 5-GHz radio) and other IEEE 802.11a-compliant infrastructure devices in infrastructure mode. It is approved for indoor use only, except in the United States which allows for outdoor use on channels 52 through 64.

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.
- PCI cards are shipped with a 2-dBi dipole antenna that attaches to the card's antenna connector. However, other types of antennas may be used. PCI cards can be operated through the primary (or right) antenna port only.
- Mini PCI cards are designed to be used with either one or two antennas, which connect to the card's two antenna connectors. If two antennas are used, the radio automatically selects the antenna that presents the best RF signal. If only one antenna is used, the radio finds and uses it regardless of which connector it is plugged into.
- PC-Cardbus cards have an integrated, permanently attached non-diversity antenna that contains two antenna ports, one for transmitting and one for receiving. The card cannot switch and sample between the ports. The antenna is housed within the section of the card that hangs out of the Cardbus slot when the card is installed.

Note Refer to the Antenna Mode (Transmit and Receive) parameters in Table 5-4 and Table 5-5 for information on setting the client adapter's antenna mode.

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-4.

LEDs

The client adapters have two LEDs that glow or blink to indicate the status of the adapter or to convey error messages. Refer to Chapter 9 for an interpretation of the LED codes.

Note Mini PCI cards do not have LEDs.

Software Components

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

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 8 provides instructions for determining the version of your client adapter's firmware and upgrading it if necessary.

Driver

The driver provides an interface between a computer running a Windows operating system and the client adapter, thereby enabling Windows and the applications it runs to communicate with the adapter. The driver is provided on the 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 Utility

The client utility, which is entitled Aironet Client Utility (ACU), is an optional application that interacts with the radio firmware to adjust client adapter settings and display information about the adapter. ACU is provided on the CD that shipped with the client adapter. If you plan to use ACU, it should be installed before the adapter is used. Chapter 3 provides instructions for installing ACU.

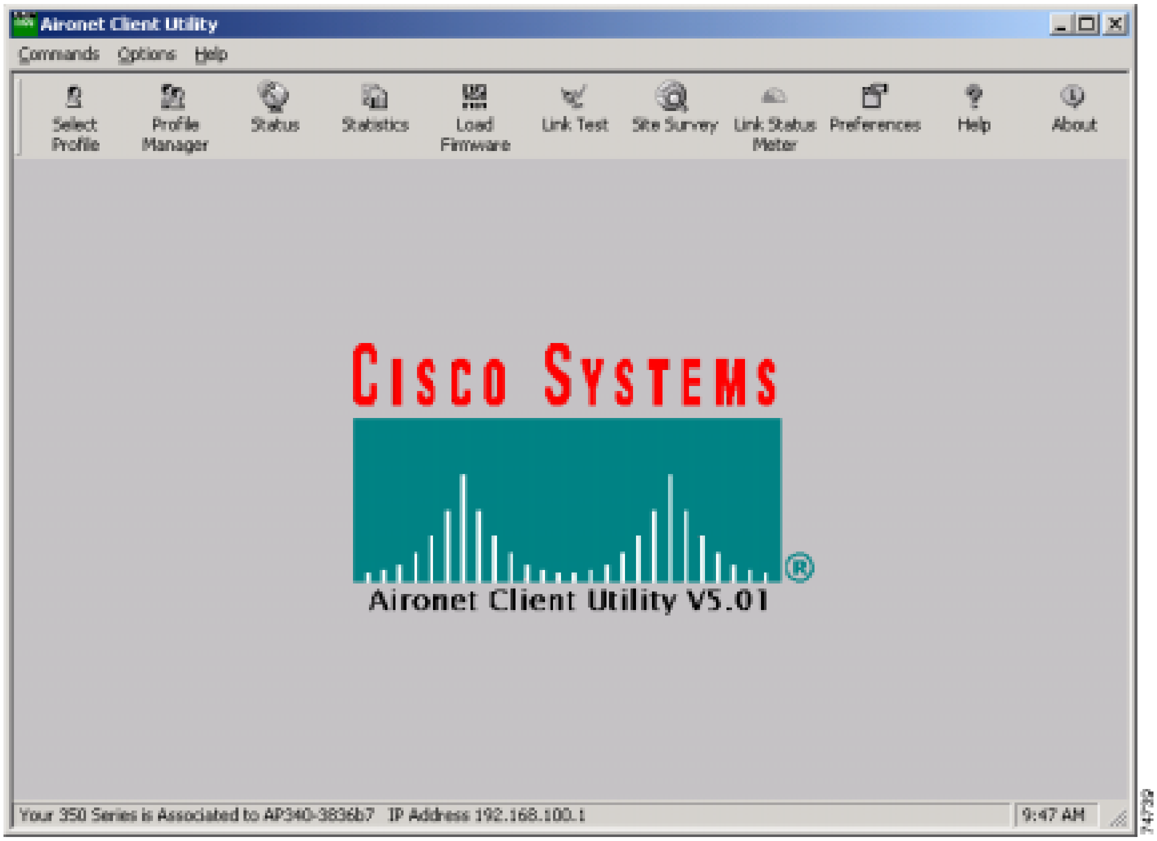
Note The CD has the latest version of ACU available at the time of pressing; however, a more recent version of ACU may be available from Cisco.com. Cisco recommends installing the most current version of ACU. Chapter 3 provides instructions for installing ACU from either location.

Note If your computer is running Windows XP, you can configure your client adapter through the Windows operating system instead of through ACU. Refer to Appendix E for information. However, ACU is recommended for configuring the client adapter.

Overview of ACU

The Aironet Client Utility screen (see Figure 1-1) is ACU’s primary screen.

Figure 1-1 Aironet Client Utility Screen



Your 350 Series is Associated to AP340-3836b7 IP Address 192.168.100.1

9:47 AM

The status bar at the bottom of the Aironet Client Utility screen reflects the current state of your client adapter. Possible states include Associated, Not Associated, Not Inserted, Being Flashed with New Firmware, and Unable To Read Status from the Card.

If your client adapter is associated to an access point, the status bar shows the name of the access point, provided it was configured with one. If shown, the access point name is limited to 16 characters by the client adapter’s radio firmware. The status bar also shows either the IP address or the MAC address of the access point to which the client adapter is associated. The information shown in the status bar is updated once per second.

The right side of the status bar shows the current time of day. If you set the clock to display seconds in the Aironet Client Utility Preferences screen, the time will include seconds in addition to hours and minutes.

Note To enable the clock to display seconds, open ACU, click the **Preferences** icon or select **Preferences** from the Options drop-down menu, select the **Display Seconds on Clock** checkbox, and click **OK**.

Buttons on the ACU Screens

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

Table 1-2 Buttons on the ACU Screens

Button	Description
Apply	Saves any changes without exiting the screen
Cancel	Exits the screen without saving any changes
Defaults	Displays the default value of each parameter
Help	Provides information on the screen and its parameters
OK	Saves any changes and exits the screen
Start	Initiates a test
Stop	Stops a test that is running

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

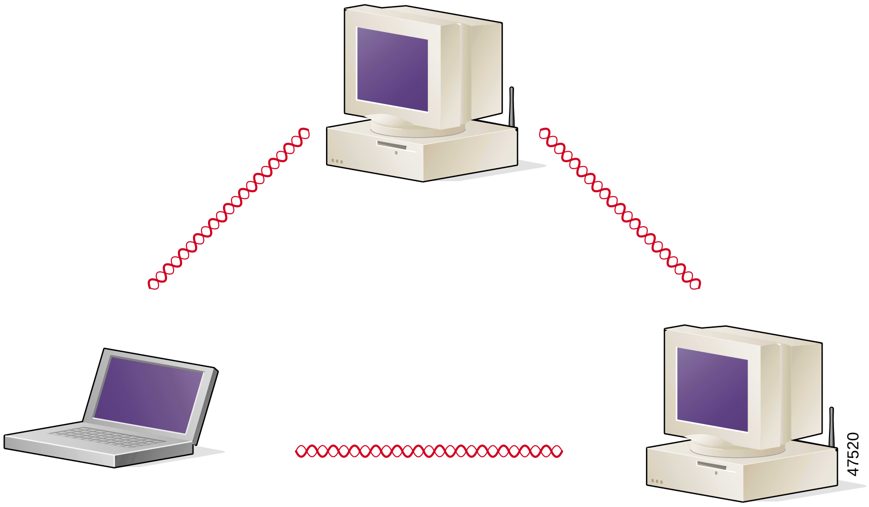
For examples of more complex network configurations involving client adapters and access points, refer to the *Cisco Aironet Access Point Hardware Installation Guide*.

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 1-2) 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 1-2 Ad Hoc Wireless LAN

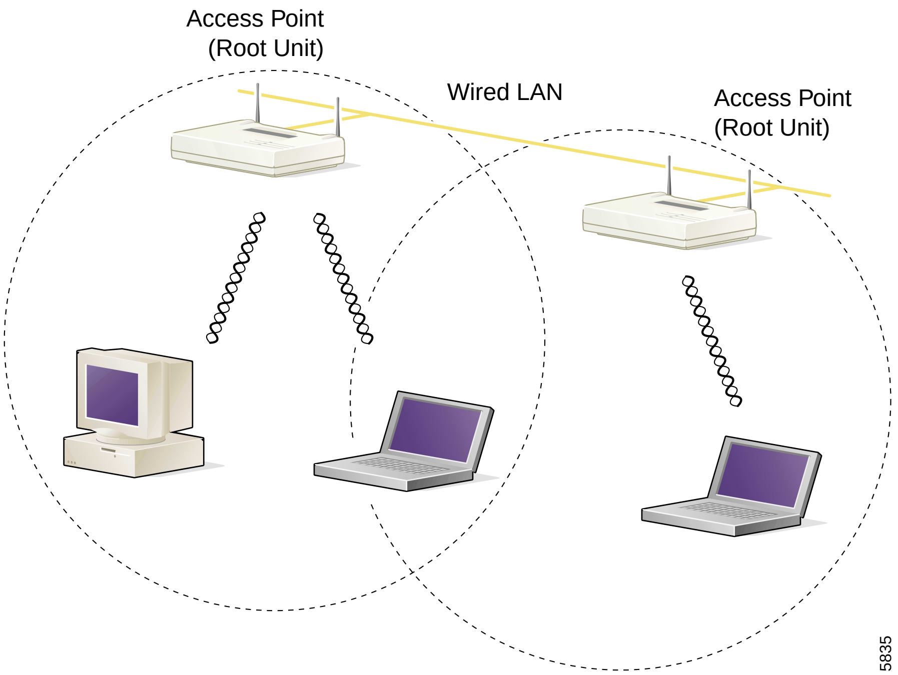


Wireless Infrastructure with Workstations Accessing a Wired LAN

A microcellular network can be created by placing two or more access points on a LAN. Figure 1-3 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 1-3 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

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:

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

Warning **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.**

Warning **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.**

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

Unpacking the Client Adapter

Follow these steps to unpack the client adapter:

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

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

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

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:

- Standard 2-dBi dipole antenna (PCI cards only)
- *Quick Start Guide: Cisco Aironet Wireless LAN Client Adapters*
- Cisco Aironet Wireless LAN Client Adapters CD (for 2.4-GHz client adapters) or Cisco Aironet 5-GHz 54-Mbps Wireless Adapter CD (for 5-GHz client adapters)
- 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 computing devices running Windows 95, 98, NT, 2000, Me, or XP:
  - Laptop, notebook, or portable or handheld device equipped with a Type II or Type III PC card slot or Cardbus slot
  - Desktop personal computer equipped with an empty PCI expansion slot
  - Handheld or portable device with an embedded LM card
  - Laptop or other computing device with an embedded mini PCI card

Note Cisco recommends using a display with a minimum resolution of 800 x 600.

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

- Windows NT Service Pack 3 or greater if your computer is running Windows NT
- A Phillips screwdriver (for PCI cards)
- The following information from your system administrator:
  - The logical name for your workstation (also referred to as *client name*)
  - The protocols necessary to bind to the client adapter
  - The case-sensitive service set identifier (SSID) for your RF network
  - If your computer is not connected to a DHCP server, the IP address, subnet mask, and default gateway address of your computer
  - 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 network account
  - The username and password for your RADIUS server account, if your wireless network uses LEAP or EAP-MD5 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 F, which is provided for people who are responsible for conducting a site survey, explains how ACU's site survey tool 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.

CHAPTER 3

Installing the Client Adapter

This chapter provides instructions for installing the client adapter driver and the client utility.

The following topics are covered in this chapter:

- Determining the Latest Versions of the Driver and ACU, page 3-2
- Installing the Driver, page 3-3
- Installing ACU, page 3-16
- Verifying Installation, page 3-19

Determining the Latest Versions of the Driver and ACU

The driver and the Aironet Client Utility (ACU) are provided on the CD that shipped with the client adapter; however, a more recent version of each may be available from Cisco.com. Cisco recommends installing the most current versions of the driver and ACU.

Note Although the client adapter is shipped with the firmware installed, you may want to check Cisco.com to see if a more recent version is available. Chapter 8 provides instructions for determining the version of your client adapter's firmware and upgrading it if necessary.

Note Mini PCI cards, along with their driver and ACU, are generally preinstalled inside of computers. Therefore, the mini PCI software is not provided on the CD, and you do not need to follow the instructions in this chapter to install the card's driver and ACU. However, if you want to upgrade the mini PCI card's driver and ACU, refer to the instructions provided in Chapter 8.

Follow the steps below to determine the most recent versions of the driver and ACU on your CD and Cisco.com.

Step 1 To determine the version of the driver and ACU on the 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" section on page 3-3.

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

a. Use your computer's web browser to access the following URL:
http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Locate the drivers for your specific operating system and client adapter type and find the one with the greatest release number. This is the latest available version on Cisco.com.

> **Note** The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

d. Locate the ACU files and find the one with the greatest release number. This is the latest available version on Cisco.com.

Step 3 Go to the "Installing the Driver" section on page 3-3. If the driver version on Cisco.com is greater than the version on the CD, follow the instructions for installing the driver from Cisco.com.

Step 4 After you install the driver, go to the "Installing ACU" section on page 3-16. If the ACU version on Cisco.com is greater than the version on the CD, follow the instructions for installing ACU from Cisco.com.

Installing the Driver

Note This procedure is meant to be used the first time the driver is installed on a computer running Windows 95, 98, NT, 2000, Me, or XP. If a Cisco Aironet client adapter driver is already installed on your computer, follow the instructions in Chapter 8 to upgrade to a new driver. However, if the 6.10 driver is installed on your Windows 95, 98, NT, or 2000 computer, you must remove this driver before you can install a more recent driver. Refer to the "Uninstalling the 6.10 Driver" section on page 8-13 for instructions.

The driver you use for your client adapter depends on which operating system your computer is running and your client adapter type. This section provides instructions for installing the correct driver for your operating system. Use Table 3-1 to quickly locate the installation instructions for your specific operating system.

Table 3-1 Locating Driver Installation Instructions

Operating System	Page Number
Windows 95	3-3
Windows 98	3-7
Windows NT	3-9
Windows 2000	3-10
Windows Millennium Edition (Me)	3-12
Windows XP	3-13

Note Before you begin the driver installation process, make sure you have the installation disks for your computer's operating system nearby. Some operating system files may be needed to complete the driver installation.

Installing the Driver for Windows 95

Note Windows 95 limits your computer's network connections to four. If you try to install a client adapter when four network devices (such as a PCMCIA Ethernet card, dial-up adapter, VPN adapter, docking station Ethernet card, etc.) are already connected to your computer, the new adapter cannot establish a network connection.

The driver installation instructions vary for Windows 95 Version A and Version B. You can determine which version your computer is running by double-clicking **My Computer**, **Control Panel**, **System**, and **General**. The version of your computer's operating system is located under the System heading. If you have Windows 95 Version B, the version number ends with the letter *B*.

- For Windows 95 Version A driver installation instructions, go to the "Windows 95 Version A" section on page 3-4.
- For Windows 95 Version B driver installation instructions, go to the "Windows 95 Version B" section on page 3-5.

Windows 95 Version A

If your computer's operating system is Windows 95 Version A, follow these steps.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows 95 and your client adapter type.

> **Note** The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 After you insert the client adapter into your computing device, Windows automatically detects it and opens the New Hardware Found window.

Step 4 Select **Driver from disk provided by hardware manufacturer** and click **OK**.

Step 5 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 6 In the Install From Disk window, enter the path to where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\Win95.

Step 7 Click **OK**.

Step 8 If you are prompted to insert the Windows 95 operating system disk, click **OK** and do one of the following:

- If the Windows 95 operating system files are installed on your computer, they are usually located in the C:\Windows\Options\Cabs folder. Type **C:\Windows\Options\Cabs** in the Copy files from dialog box. Click **OK** to copy the required files.
- If Windows 95 prompts for the Windows 95 operating system CD, insert this CD into your computer's CD-ROM drive. If your CD-ROM drive is drive D, the path in the dialog box should be D:\Win95. Click **OK** to copy the required files.

Step 9 After the files are copied, remove any disks from your computer.

Step 10 Double-click **My Computer**, **Control Panel**, and **Network**.

Step 11 Select the Cisco Systems wireless LAN adapter and click **Properties**.

Step 12 In the client adapter Properties window, click the **Advanced** tab.

Step 13 Select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 14 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 15 Click **OK**.

Step 16 If you are prompted to restart your computer, click **Yes**.

Step 17 If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK** twice. When prompted to restart your computer, click **Yes**.

Note On Windows 95, TCP/IP is not installed by default.

The driver installation is complete.

Windows 95 Version B

If your computer's operating system is Windows 95 Version B, follow these steps.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL:
http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows 95 and your client adapter type.

Note The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 After you insert the client adapter into your computing device, Windows automatically detects it and briefly opens the New Hardware Found window.

Step 4 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 5 The Update Device Driver Wizard dialog box opens and indicates that Windows will complete the installation of the client adapter. Click **Next**.

Step 6 If the Update Device Driver Wizard indicates that Windows was unable to locate a driver for the client adapter, click **Other Locations**.

Step 7 In the Select Other Location window, enter the path to where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\Win95.

Step 8 Click **OK**.

Step 9 When the Update Device Driver Wizard indicates that it has found the driver, click **Finish**.

Step 10 When the Insert Disk window appears prompting you to insert the Aironet Wireless LAN Adapter Installation Disk, click **OK**.

Step 11 If a window appears indicating that the pcx50*.sys file could not be found, enter the same path that you entered in Step 7 and click **OK**.

Step 12 If you are prompted to insert the Windows 95 operating system disk, click **OK** and do one of the following:

- If the Windows 95 operating system files are installed on your computer, they are usually located in the C:\Windows\Options\Cabs folder. Type **C:\Windows\Options\Cabs** in the Copy files from dialog box. Click **OK** to copy the required files.
- If Windows 95 prompts for the Windows 95 operating system CD, insert this CD into your computer's CD-ROM drive. If your CD-ROM drive is drive D, the path in the dialog box should be D:\Win95. Click **OK** to copy the required files.

Step 13 When prompted to restart your computer, remove any disks and click **Yes**.

Step 14 When the computer restarts, double-click **My Computer**, **Control Panel**, and **Network**.

Step 15 Select the Cisco Systems wireless LAN adapter and click **Properties**.

Step 16 In the client adapter Properties window, click the **Advanced** tab.

Step 17 Select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 18 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 19 Click **OK**.

Step 20 If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.

Note On Windows 95, TCP/IP is not installed by default.

Step 21 In the Network window, click **OK**.

Step 22 When prompted to restart your computer, click **Yes**.

The driver installation is complete.

Installing the Driver for Windows 98

Note Windows 98 limits your computer's network connections to eight. If you try to install a client adapter when eight network devices (such as a PCMCIA Ethernet card, dial-up adapter, VPN adapter, docking station Ethernet card, etc.) are already connected to your computer, the new adapter cannot establish a network connection.

If your computer's operating system is Windows 98, follow these steps.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows 98 and your client adapter type.

Note The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 After you insert the client adapter into your computing device, Windows automatically detects it, briefly opens the New Hardware Found window, and starts collecting information for a driver information database.

The Add New Hardware Wizard dialog box opens and indicates that Windows is searching for new drivers.

Step 4 Click **Next**. Another dialog box opens and asks what you want Windows to do.

Step 5 Select **Display a list of all the drivers in a specific location, so you can select the driver you want** and click **Next**.

Step 6 Select **Network adapters** from the drop-down list of devices and click **Next**.

Step 7 Click **Have Disk**.

Step 8 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 9 Enter or browse to the path where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\Win98.

Step 10 Click **OK**.

Step 11 Make sure the Cisco Systems wireless LAN adapter is selected in the Select Device screen and click **OK**. The wizard finds the installation files and displays the search results.

Step 12 When the client adapter driver is displayed, click **Next** to copy the required files.

Step 13 During driver installation, you may be prompted to enter a path to the Windows 98 operating system files. If so, do one of the following:

- If the Windows 98 operating system files are installed on your computer, they are usually located in the C:\Windows\Options\Cabs folder. Type **C:\Windows\Options\Cabs** in the Copy files from dialog box. Click **OK** to copy the required files.
- If Windows 98 prompts for the Windows 98 operating system CD, insert this CD into your computer's CD-ROM drive. If your CD-ROM drive is drive D, the path in the dialog box should be D:\Win98. Click **OK** to copy the required files.

Step 14 The Add New Hardware Wizard window opens and indicates that the installation is complete. Click **Finish**.

Step 15 When prompted to restart your computer, remove the CD or floppy disk (if installed) and click **Yes**.

Step 16 When the computer restarts, double-click **My Computer**, **Control Panel**, and **Network**.

Step 17 Select the Cisco Systems wireless LAN adapter and click **Properties**.

Step 18 In the client adapter Properties window, click the **Advanced** tab.

Step 19 Select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 20 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 21 Click **OK**.

Step 22 If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.

Step 23 In the Network window, click **OK**.

Step 24 When prompted to restart your computer, click **Yes**.

The driver installation is complete.

Installing the Driver for Windows NT

Note This procedure requires that your computer has Windows NT Service Pack 3 or greater.

If your computer's operating system is Windows NT, follow these steps.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL:
http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows NT and your client adapter type.

Note The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 After you insert the client adapter into your computer, an error message may appear indicating that at least one service or driver failed during system setup. If this message appears, click **OK**.

Step 4 Follow the steps below to obtain an available interrupt request (IRQ):

a. Select **Start** > **Programs** > **Administrative Tools** > **Windows NT Diagnostics**.

b. Click the **Resources** tab.

c. The used IRQs are listed in numerical order along the left side of the Resources window. Write down the number of an IRQ that is not being used. You will need this IRQ for Step 15.

Step 5 On your computer desktop, double-click **My Computer**, **Control Panel**, and **Devices**. Scroll down and select **Pcmcia**. Click **Startup**, select **Automatic**, and click **OK**.

Note For PC cards and PC-Cardbus cards, also ensure that the Cardbus service is deselected.

Step 6 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 7 Double-click **My Computer**, **Control Panel**, and **Network**.

Step 8 Click the **Adapters** tab and select **Add**.

Step 9 In the Select Network Adapter window, click **Have Disk**.

Step 10 In the Insert Disk window, enter the path to where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\WinNT4.

Step 11 Click **OK**.

Step 12 In the Select OEM Option box, select the Cisco Systems wireless LAN adapter and click **OK**.

Step 13 In the Adapter Setup window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 14 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 15 Enter an available IRQ number, which you obtained in Step 4.

Step 16 Click **OK** and **Close**.

Step 17 The Microsoft TCP/IP Properties window should open. If it does not open, double-click **My Computer**, **Control Panel**, and **Network**. Click **Protocols**, **TCP/IP**, and **Properties**.

Step 18 Perform one of the following:

- If your computer is connected to a DHCP server, select **Obtain an IP address from a DHCP server**. When asked if you want to enable DHCP, click **Yes** and **OK**.
- If your computer is not connected to a DHCP server, select **Specify an IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.

Step 19 When prompted to restart your computer, remove the CD or floppy disk (if installed) and click **Yes**.

The driver installation is complete.

Installing the Driver for Windows 2000

If your computer's operating system is Windows 2000, follow these steps.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows 2000 (Win2K) and your client adapter type.

Note The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 After you insert the client adapter into your computer, Windows 2000 automatically detects it and briefly opens the Found New Hardware window.

The Found New Hardware Wizard window opens and indicates that the wizard will help you to install the driver.

Step 4 Click **Next**. Another window opens and asks what you want the wizard to do.

Step 5 Select **Display a list of the known drivers for this device so that I can choose a specific driver** and click **Next**.

Step 6 Click **Have Disk**.

Step 7 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 8 Enter or browse to the path where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\Win2000.

Step 9 Click **OK**. The wizard finds the installation files and displays the search results.

Step 10 When the client adapter driver is displayed, click **Next** to copy the required files.

Step 11 When you receive a message indicating that Windows has finished the installation, click **Finish**.

Step 12 Remove the CD or floppy disk (if installed).

Step 13 Double-click **My Computer**, **Control Panel**, and **System**.

Step 14 In the System Properties window, click the **Hardware** tab.

Step 15 Click **Device Manager**.

Step 16 In the Device Manager window, double-click **Network Adapters**.

Step 17 Right-click the Cisco Systems wireless LAN adapter.

Step 18 Click **Properties**.

Step 19 In the client adapter Properties window, click the **Advanced** tab.

Step 20 In the Advanced window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 21 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 22 Click **OK**.

Step 23 If your computer is not connected to a DHCP server and you plan to use TCP/IP, follow these steps:

a. Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.

b. Right-click **Local Area Connection**.

c. Click **Properties**, **Internet Protocol (TCP/IP)**, and **Properties**.

d. Click **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.

e. In the Local Area Connection Properties window, click **OK**.

Step 24 If you are prompted to restart your computer, click **Yes**.

The driver installation is complete.

Installing the Driver for Windows Millennium Edition (Me)

The first release of Windows Me comes with driver version 6.15, which is installed automatically the first time you insert a client adapter. To upgrade to the driver on the CD that shipped with your client adapter or on Cisco.com, follow these steps.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped wih your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows Me and your client adapter type.

Note The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 4 Double-click **My Computer**, **Control Panel**, and **System**.

Step 5 Click the **Device Manager** tab.

Step 6 Double-click **Network Adapters**.

Step 7 Select the Cisco Aironet wireless LAN adapter. Click **Properties**.

Step 8 In the client adapter Properties window, click the **Driver** tab.

Step 9 Click **Update Driver**. The Update Device Driver Wizard window appears.

Step 10 Select **Specify the location of the driver (Advanced)** and click **Next**.

Step 11 Select **Search for a better driver than the one your device is using now (Recommended)**.

Step 12 Make sure the **Removable Media** checkbox is deselected.

Step 13 Select the **Specify a location** checkbox and click **Browse**.

Step 14 Find the location of the driver (on your CD, floppy disk, or computer's hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\WinME.

Step 15 Click **Next**.

Step 16 When asked what you would like to install, select **The updated driver (recommended)** and click **Next**.

Step 17 When a screen appears indicating the driver that will be installed and its location, click **Next**.

Step 18 If Windows cannot find the pcx50*.sys file, enter the same path that you browsed to in Step 14 and click **OK**.

Step 19 When you are notified that the installation is complete, click **Finish**.

Step 20 When you are prompted to restart your computer, remove the CD or floppy disk (if installed) and click **No**.

Step 21 Double-click **My Computer**, **Control Panel**, and **Network**.

Step 22 Select the Cisco Systems wireless LAN adapter. Click **Properties**.

Step 23 In the client adapter Properties window, click the **Advanced** tab.

Step 24 In the Advanced window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 25 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 26 Click **OK**.

Step 27 If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.

Step 28 In the Network window, click **OK**.

Step 29 When prompted to restart your computer, click **Yes**.

The driver installation is complete.

Installing the Driver for Windows XP

The first release of Windows XP comes with driver version 7.29, which is installed automatically the first time you insert a client adapter. To upgrade to the driver on the CD that shipped with your client adapter or on Cisco.com, follow these steps.

Note If you do not upgrade from the 7.29 driver, you cannot specify an SSID through Windows XP's driver Advanced tab.

Note These instructions assume you are using Windows XP's classic view rather than its category view.

Step 1 If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to Step 2.

a. Use the computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml

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

c. Click the link for individual Windows files.

d. Select the latest driver file for Windows XP and your client adapter type.

Note The drivers for PC, LM, and PCI cards are labeled *PCM-LMC-PCI*; the drivers for mini PCI cards and PC-Cardbus cards are labeled *MPI-CB*.

e. Read and accept the terms and conditions of the Software License Agreement.

f. Select the driver file to download it.

g. Save the file to a floppy disk or to your computer's hard drive.

h. Locate the file using Windows Explorer, double-click it, and extract its files to a folder.

i. Go to Step 2.

Step 2 Follow the instructions in Chapter 8 to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.

Step 3 Double-click **My Computer**, **Control Panel**, and **System**.

Step 4 Click the **Hardware** tab and **Device Manager**.

Step 5 Double-click **Network Adapters** and **Cisco Systems 3x0 Series Wireless LAN Adapter**.

Step 6 Click the **Driver** tab.

Step 7 Click **Update Driver**. The Welcome to the Hardware Update Wizard screen appears.

Step 8 Select the **Install from a list or specific location (Advanced)** option and click **Next**.

Step 9 When prompted to choose your search and installation options, select **Don't search. I will choose the driver to install** and click **Next**.

Step 10 When prompted to select a network adapter to install, click **Have Disk**. The Install From Disk screen appears.

Step 11 Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

Step 12 Click **Browse**; then find the location of the driver (on your CD, floppy disk, or computer's hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\WinXP.

Step 13 Click **Open**. The installation wizard finds the driver file (netx500.inf).

Step 14 Click **OK** on the Install From Disk screen.

Step 15 The Select Network Adapter screen reappears. Select the Cisco Systems Wireless LAN Adapter and click **Next**.

Step 16 The installation wizard copies the driver files from the CD, floppy disk, or computer's hard drive. When the installation is complete, click **Finish**.

Step 17 Click **Close** on the Cisco Aironet Wireless LAN Adapter Properties screen and exit the Control Panel.

> **Note** You must exit the Control Panel before opening it again in Step 18. Otherwise, the SSID property option will not be available when you get to Step 22.

Step 18 Double-click **Control Panel** and **Network Connections**.

Step 19 Right-click **Wireless Network Connection**.

Step 20 Click **Properties**, **Configure**, and the **Advanced** tab.

Step 21 In the Advanced window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.

Step 22 Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.

Step 23 Click **OK**.

Step 24 If your computer is not connected to a DHCP server and you plan to use TCP/IP, right-click **Wireless Network Connection** and click **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Select **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.

Step 25 The driver installation is complete. Now you must decide whether to configure your client adapter through Windows XP or ACU. To help you with your decision, Table 3-2 compares the Windows XP and ACU client adapter features.

Table 3-2 Comparison of Windows XP and ACU Client Adapter Features

Feature	Windows XP	ACU
Configuration parameters	Limited	Extensive
Capabilities		
Create profiles	No	Yes
Upgrade radio firmware	No	Yes
Restart client adapter without rebooting or ejecting card	No	Yes
Turn radio on or off	No	Yes
Security		
Static WEP	Yes	Yes
LEAP authentication with dynamic WEP	No	Yes
Host-based EAP authentication with static or dynamic WEP	Yes	Yes

Table 3-2 Comparison of Windows XP and ACU Client Adapter Features (continued)

Feature	Windows XP	ACU
Diagnostics		
Status screen	Limited	Extensive
Statistics screen (transmit & receive)	No	Yes
Site survey tool	No	Yes
RF link test tool	No	Yes
Link status meter (graphical display)	No	Yes

Step 26 Perform one of the following:

- If you are planning to configure your client adapter through ACU instead of through Windows XP, follow the steps below:
  - **a.** Double-click **My Computer**, **Control Panel**, and **Network Connections**.
  - **b.** Right-click **Wireless Network Connection** and click **Properties**.
  - **c.** Select the **Wireless Networks** tab.
  - **d.** Deselect the **Use Windows to configure my wireless network settings** checkbox.
  - **e.** Follow the instructions in the "Installing ACU" section on page 3-16 to install ACU.
- If you are planning to configure your client adapter through Windows XP instead of through ACU, go to Appendix E and follow the instructions there.
- If you are planning to configure your client adapter through Windows XP but you want to use ACU's diagnostic tools, go to Appendix E to configure the adapter through Windows XP; then install ACU but do not create any profiles.

Installing ACU

After you have installed the appropriate driver for your computer's operating system and your client adapter type, follow the steps below to install the Aironet Client Utility (ACU).

Note Follow the procedure below if ACU has never been installed on your computer or if ACU version 4.13 or greater is currently installed. If a version of ACU prior to 4.13 is installed on your computer, follow the instructions in Chapter 8 to uninstall it; then follow the steps below to install the latest version. Cisco does not recommend uninstalling ACU version 4.13 or greater before installing the latest version of ACU.

Note ACU version 5.02.005 or greater must be used with PCM/LMC/PCI card driver version 8.2 or greater and PCM/LMC/PCI card firmware version 4.25.30 or greater or mini PCI card driver version 3.4 or greater and mini PCI card firmware version 5.00.03 or greater. ACU version 5.02.006 or greater must be used with PC-Cardbus card driver version 3.4 or greater and PC-Cardbus card firmware version 4.99 or greater.

Step 1 Close any Windows programs that are running.

Step 2 Perform one of the following:

- If you are installing ACU from the CD that shipped with your client adapter, follow the steps below:
  - **a.** Insert the CD into your computer's CD-ROM drive.
  - **b.** Select **Start** > **Run**, enter the following path (where *D* is the letter of your CD-ROM drive): **D:\Aironet Client Utility\Setup.exe**, and click **OK**. The Aironet Client Utility Setup screen and the InstallShield Wizard appear.
  - **c.** Go to Step 3.
- If you are installing ACU from Cisco.com, follow the steps below:
  - **a.** Use the computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml
  - **b.** Locate the section for client adapter drivers and utilities.
  - **c.** Click the link for individual Windows files.
  - **d.** Select the latest ACU file.
  - **e.** Read and accept the terms and conditions of the Software License Agreement.
  - **f.** Select the ACU file to download it.
  - **g.** Save the file to your computer's hard drive.
  - **h.** Locate the file using Windows Explorer, double-click it, and extract its files to a folder.
  - **i.** Select **Start** > **Run**, enter or browse to the path where you extracted the files (for example, C:\temp\setup.exe), and click **OK**. The Aironet Client Utility Setup screen and the InstallShield Wizard appear.
  - **j.** Go to Step 3.

Step 3 When the Welcome screen appears, click **Next**.

Step 4 In the Select Options screen, select as many of the following options as desired and click **Next**:

Option	Description
LEAP	Enables you to create a profile in ACU that uses LEAP authentication. If this option is not selected now and you later want to use LEAP, you must run this installation again, select **Modify**, and select this option. **Default:** Selected **Note** Refer to Chapter 5 for information on enabling LEAP. **Note** If you select LEAP on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are installed during ACU installation to fix two problems related to the use of LEAP. Refer to Chapter 9 for more information on the hot fixes. **Note** If you select LEAP on a Windows XP device, you cannot use Windows XP's fast user switching feature.

Allow Saved LEAP User Name and Password	Enables you to create a profile in ACU that uses a saved (rather than temporary) username and password for LEAP authentication. When such a profile is used, the saved username and password are used to start the LEAP authentication process, and you are not prompted to enter them. **Default:** Selected **Note** This option is available only if the LEAP option is selected.
Create ACU Icon on your Desktop	Causes the installation program to add an ACU icon to your computer's desktop to provide quick access to the utility. **Default:** Deselected
Allow Non-Administrator Users to use ACU to modify profiles	Enables users without administrative rights to modify profiles in ACU on computers running Windows NT, 2000, or XP. **Default:** Selected **Note** This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.

Step 5 In the Choose Destination Location screen, perform one of the following:

- If you want the ACU program files to be installed in the default location (C:\Program Files, provided C:\Program Files is the default Windows program file folder), click **Next**.
- If you want to specify a different destination location for the ACU program files, click **Browse**, select a location, and click **Next**.

Step 6 In the Select Program Folder screen, specify a program folder name for ACU by selecting from the list of existing folders (the default name is Cisco Aironet) or entering a new folder name; then click **Next**.

A status screen displays the progress of the installation. Then one of two Setup Complete screens displays, depending on whether Windows needs to be restarted to complete the installation.

Step 7 Perform one of the following:

- If your computer does not need to be rebooted, select either of the following options and click **Finish**:

Option	Description
View the README.TXT file	Opens a read-me file containing information about ACU.
Launch the Aironet Client Utility	Opens ACU so you can configure your client adapter.

- If your computer needs to be rebooted, select **Yes, I want to restart my computer now** or **No, I will restart my computer later**, remove the CD (if installed), and click **Finish**.

Note If you are prompted to reboot your computer, Cisco recommends that you select the **Yes, I want to restart my computer now** option.

Step 8 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 below to determine if the installation was successful. After you verify installation, go to Chapter 4 if you want to create profiles for your client adapter.

Verifying Installation

To verify that you have properly installed the driver and ACU 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 9 for troubleshooting information.

Go to Chapter 4 if you want to create profiles for your client adapter.

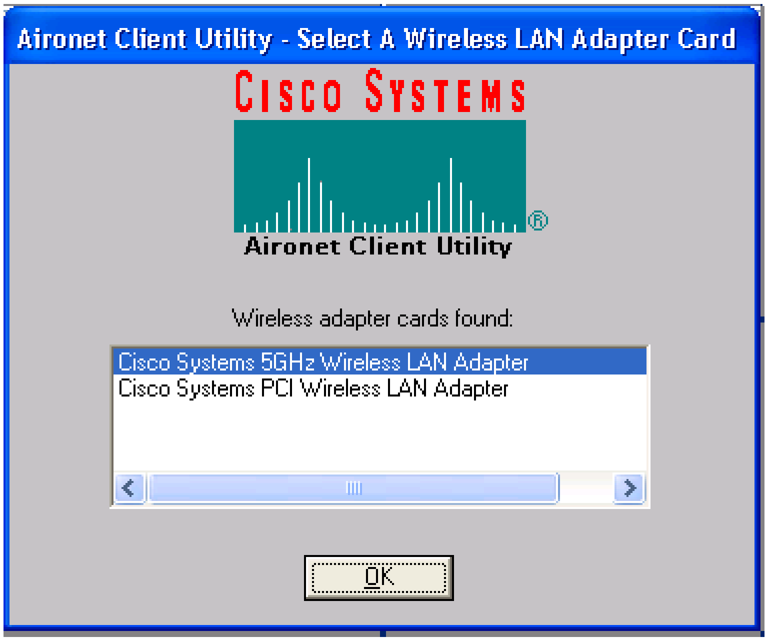
Note If two client adapters (e.g., a PCI card and a PC-Cardbus card) are installed in your computer, you must specify the one for which you currently wish to set up profiles in ACU. Go to the "Selecting Between Two Installed Client Adapters" section for instructions.

Selecting Between Two Installed Client Adapters

If two client adapters are installed in your computer, follow the instructions below to specify the one for which you want to set up profiles in ACU.

Step 1 Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU. The Select A Wireless LAN Adapter Card screen displays (see Figure 3-1).

Figure 3-1 Select A Wireless LAN Adapter Card Screen



Wireless adapter cards found:

Cisco Systems 5GHz Wireless LAN Adapter
Cisco Systems PCI Wireless LAN Adapter

Step 2 Select the card you wish to configure from the list of available cards and click **OK**.

Step 3 Go to Chapter 4 to create profiles for this card.

Using the Profile Manager

This chapter explains how to use ACU's profile manager feature to create and manage profiles for your client adapter.

The following topics are covered in this chapter:

Overview of Profile Manager

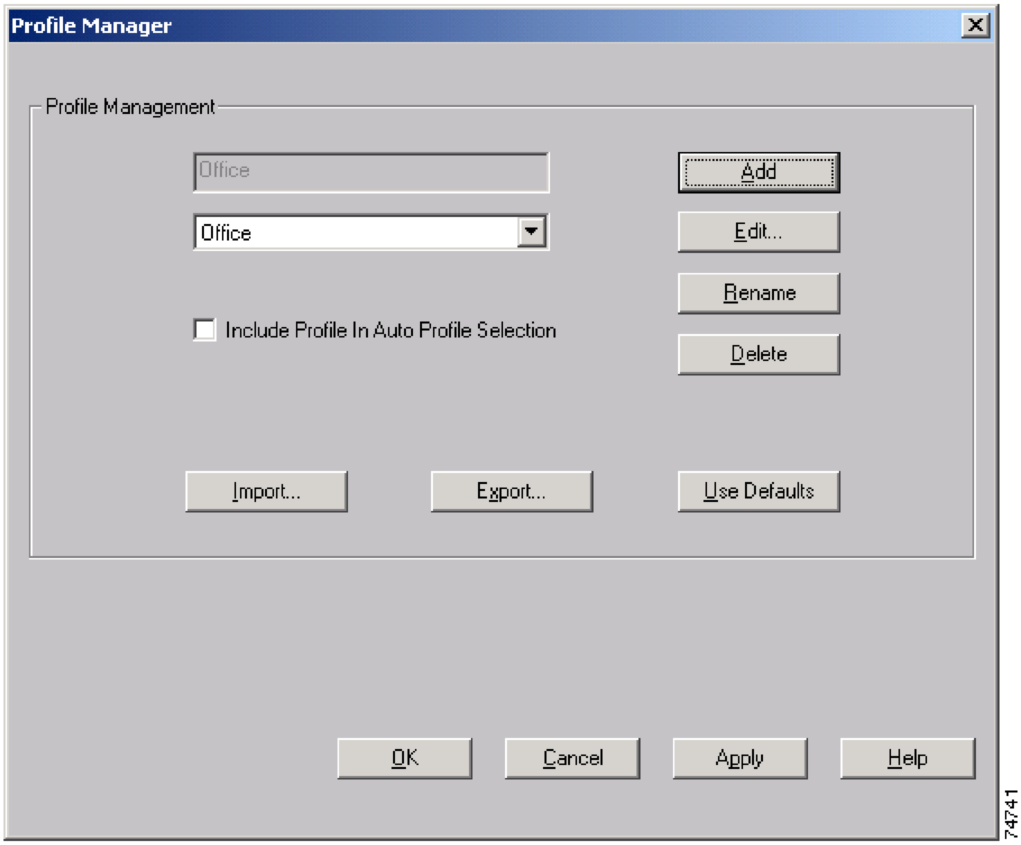
ACU's profile manager feature allows you to create and manage up to 16 *profiles* (or saved configurations) for your client adapter. These profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for using your client adapter at the office, at home, and in public areas such as airports. Once the profiles are created, you can easily switch between them without having to reconfigure your client adapter each time you enter a new location.

Profiles are stored in the part of the registry reserved for the client adapter driver and, therefore, are tied to radio type. Consequently, if you set up profiles for a 340 series PC card and later upgrade to a 350 series PC card, all of the profiles will be lost. Similarly, all profiles are lost if you uninstall the client adapter's driver. To prevent your profiles from being lost, Cisco recommends that you back up your profiles using the profile manager's import/export capability. See the "Importing and Exporting Profiles" section on page 4-6 for details.

Opening Profile Manager

To open ACU's profile manager, double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen displays (see Figure 4-1).

Figure 4-1 Profile Manager Screen



Office

Office

□ Include Profile In Auto Profile Selection

Profile manager allows you to perform the following tasks related to the management of profiles:

- Create a new profile, see below
- Select the active profile, see page 4-4
- Edit a profile, see page 4-5
- Set a profile to default values, see page 4-6
- Rename a profile, see page 4-6
- Delete a profile, see page 4-6
- Import a profile, see page 4-7
- Export a profile, see page 4-7

Follow the instructions on the page indicated for the task you want to perform.

Creating a New Profile

Follow the steps below to create a new profile.

Step 1 Click **Add**. A cursor appears in the Profile Management edit box.

Step 2 Enter the name for your new profile (for example, Office, Home, etc.).

Step 3 Press **Enter**. The Properties screens appear with the name of your new profile in parentheses.

Step 4 Perform one of the following:

- If you want this profile to use the default values, click **OK**. The profile is added to the list of profiles on the Profile Manager screen.
- If you want to change any of the configuration parameter settings, follow the instructions in Chapter 5. The profile is added to the list of profiles on the Profile Manager screen.

Step 5 If you want this profile to be included in auto profile selection, select the **Include Profile in Auto Profile Selection** checkbox on the Profile Manager screen.

Note If your profile is configured to use LEAP, it can be included in auto profile selection *only* if it has a saved LEAP username and password. For more information on auto profile selection, see the "Selecting the Active Profile" section on page 4-4.

Step 6 Click **OK** or **Apply** to save your profile.

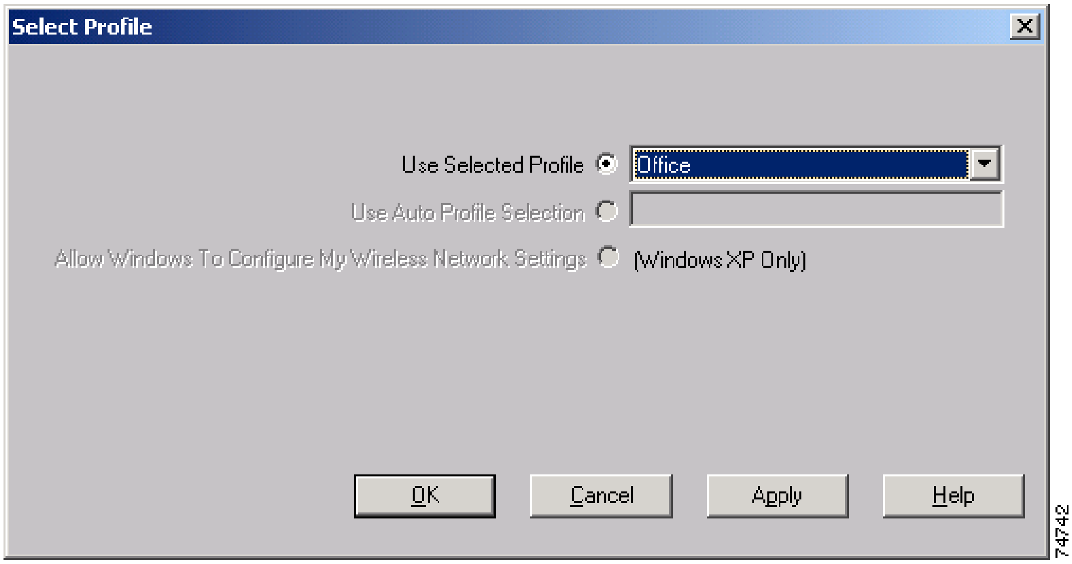
Selecting the Active Profile

Follow the steps below to specify the profile that the client adapter is to use.

Note If this is the first time that you are using profile manager and no profiles have been set previously, the Use Selected Profile drop-down box is disabled but displays "Driver Advanced Tab Settings," which indicates that the driver is using any settings that were set through the Control Panel.

Step 1 Open ACU; then click the **Select Profile** icon or select **Select Profile** from the Commands drop-down menu. The Select Profile screen displays (see Figure 4-2).

Figure 4-2 Select Profile Screen



Select Profile

Use Selected Profile ● Office

Use Auto Profile Selection ○

Allow Windows To Configure My Wireless Network Settings ○ (Windows XP Only)

Step 2 Select one of the following options:

- **Use Selected Profile** – This option allows you to select one profile for the client adapter to use. If you choose this option, you also must select the desired profile from the drop-down box.

  If the client adapter cannot associate to an access point or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To associate, you must select a different profile or select Use Auto Profile Selection.

- **Use Auto Profile Selection** – This option causes the client adapter's driver to automatically select a profile from the list of profiles that were set up to be included in auto profile selection. The name of the profile that is being used appears in the box to the right of the Use Auto Profile Selection option.

  If the client adapter loses association for more than 10 seconds (or for more than the time specified by the LEAP authentication timeout value on the LEAP Settings screen if LEAP is enabled), the driver switches automatically to another profile that is included in auto profile selection. The adapter will not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value). To force the client adapter to associate to a different access point, you must disable auto profile selection and select a new profile.

Note This option is available only if two or more profiles are included in auto profile selection and if the client adapter is using PCM/LMC/PCI card driver version 8.01 or greater (or mini PCI/PC-Cardbus card driver version 2.20 or greater).

Note Login scripts are not reliable if you use auto profile selection with LEAP. If you LEAP authenticate and achieve full network connectivity before or at the same time as you log into the computer, the login scripts will run. However, if you LEAP authenticate and achieve full network connectivity after you log into the computer, the login scripts will not run.

- **Allow Windows To Configure My Wireless Network Settings** – This option, which is available only on Windows XP, allows Windows to configure the client adapter and disregard any ACU profiles. You must select this option if you are configuring your card through Windows XP but want to use ACU's diagnostic tools. Refer to Appendix E for information on configuring your client adapter through Windows XP.

Step 3 Click **OK** or **Apply** to save your selection. The client adapter starts using a profile based on the option selected above.

Modifying a Profile

This section provides instructions for modifying an existing profile. Follow the steps in the corresponding section below to edit, set to default values, rename, or delete a profile.

Editing a Profile

Step 1 Open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu.

Step 2 From the Profile Management drop-down box, select the profile that you want to edit.

Step 3 Click **Edit**. The Properties screens appear with the name of the profile in parentheses.

Step 4 Follow the instructions in Chapter 5 to change any of the configuration parameters for this profile.

Step 5 If you want this profile to be included in auto profile selection, make sure the **Include Profile in Auto Profile Selection** checkbox on the Profile Manager screen is selected.

Note If your profile is configured to use LEAP, it can be included in auto profile selection only if it has a saved LEAP username and password.

Step 6 Click **OK** or **Apply** to save your configuration changes.

Setting a Profile to Default Values

Step 1 Open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu.

Step 2 From the Profile Management drop-down box, select the profile that you want to set to default values.

Step 3 Click **Use Defaults**.

Step 4 When prompted, click **Yes** to confirm your decision.

Step 5 Click **OK** or **Apply** to save your change. The profile is saved with default values.

Renaming a Profile

Step 1 Open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu.

Step 2 From the Profile Management drop-down box, select the profile that you want to rename.

Step 3 Click **Rename**. The Profile Management edit box becomes enabled.

Step 4 Enter a new name for the profile.

Step 5 Click **OK** or **Apply** to save your change. The profile is renamed and added to the list of profiles.

Deleting a Profile

Step 1 Open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu.

Step 2 From the Profile Management drop-down box, select the profile that you want to delete.

Step 3 Click **Delete**.

Step 4 When prompted, click **Yes** to confirm your decision.

Step 5 Click **OK** or **Apply** to save your change. The profile is deleted.

Importing and Exporting Profiles

This section provides instructions for importing and exporting profiles. You may want to use the import/export feature for the following reasons:

- To back up profiles before uninstalling the client adapter driver or changing radio types
- To set up your computer with a profile from another computer
- To export one of your profiles and use it to set up additional computers

Follow the steps in the corresponding section below to import or export profiles.

Importing a Profile

Step 1 If the profile that you want to import is on a floppy disk, insert the disk into your computer's floppy drive.

Step 2 Open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu.

Step 3 Click **Import**. The Import Profile screen appears.

Step 4 Find the directory where the profile is located.

Step 5 Click the profile so it appears in the File name box at the bottom of the Import Profile screen.

Step 6 Click **Open**. The imported profile appears in the list of profiles on the Profile Manager screen.

Exporting a Profile

Step 1 Insert a blank floppy disk into your computer's floppy drive, if you wish to export a profile to a floppy disk.

Step 2 Open ACU; then click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu.

Step 3 From the Profile Management drop-down box, select the profile that you want to export.

Step 4 Click **Export**. The Save Profile As screen appears. The default filename is *ProfileName*.pro, where *ProfileName* is the name of the selected profile, and the default directory is the directory in which ACU was installed.

Step 5 If you want to change the profile name, enter a new name in the File name edit box.

Step 6 Select a different directory (for example, your computer's floppy disk drive or a location on the network) from the Save in drop-down box.

Step 7 Click **Save**. The profile is exported to the specified location.

Step 8 Follow the instructions in the "Importing a Profile" section to import the profile on another computer.

Denying Access to Non-Administrative Users

By default, ACU allows regular-class users to modify and save profiles to the registry. However, if you have administrative rights, you can prevent regular-class users from saving profiles on computers running Windows NT, 2000, or XP. (This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.)

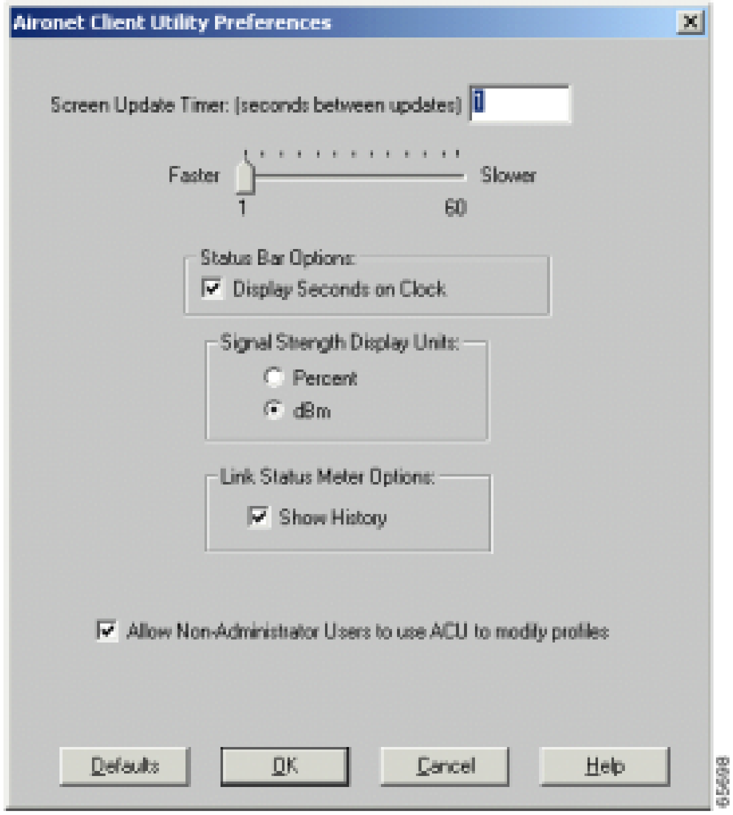
Note You were able to grant or deny access to non-administrative users during ACU installation. If you chose to deny access then, you can follow the steps below to change your decision.

Follow the steps below if you wish to prevent users without administrative rights from modifying and saving profiles (or to allow regular-class users to save profiles if permission was denied previously).

Step 1 Open ACU by double-clicking the **Aironet Client Utility (ACU)** icon on your desktop.

Step 2 Click the **Preferences** icon or select **Preferences** from the Options drop-down menu. The Aironet Client Utility Preferences screen appears (see Figure 4-3).

Figure 4-3 Aironet Client Utility Preferences Screen



Aironet Client Utility Preferences

Screen Update Timer: (seconds between updates) 1

Status Bar Options:
☑ Display Seconds on Clock

Signal Strength Display Units:
○ Percent
● dBm

Link Status Meter Options:
☑ Show History

☑ Allow Non-Administrator Users to use ACU to modify profiles

Step 3 Deselect the **Allow Non-Administrator Users to use ACU to modify profiles** checkbox (or select this checkbox if you wish to allow regular-class users to save profiles).

Step 4 Click **OK** to save your changes.

Configuring the Client Adapter

This chapter explains how to change the configuration parameters for a specific profile.

The following topics are covered in this chapter:

Overview

When you choose to create a new profile or edit an existing profile on the Profile Manager screen, the Properties screens appear with the name of your profile in parentheses. These screens enable you to set the configuration parameters for that profile.

Note If you do not change any of the configuration parameters, the default values are used.

Note If you are planning to set parameters on more than one of the Properties screens, wait until you are finished with all of the screens before clicking OK. When you click OK, you are returned to the Profile Manager screen.

Each of the Properties screens (listed below) contains parameters that affect a specific aspect of the client adapter:

- **System Parameters** – Prepares the client adapter for use in a wireless network
- **RF Network** – Controls how the client adapter transmits and receives data
- **Advanced (Infrastructure)** – Controls how the client adapter operates within an infrastructure network
- **Advanced (Ad Hoc)** – Controls how the client adapter operates within an ad hoc (peer-to-peer) network
- **Network Security** – Controls how a client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data

Table 5-1 enables you to quickly locate the instructions for setting each Properties screen's parameters.

Table 5-1 Locating Configuration Instructions

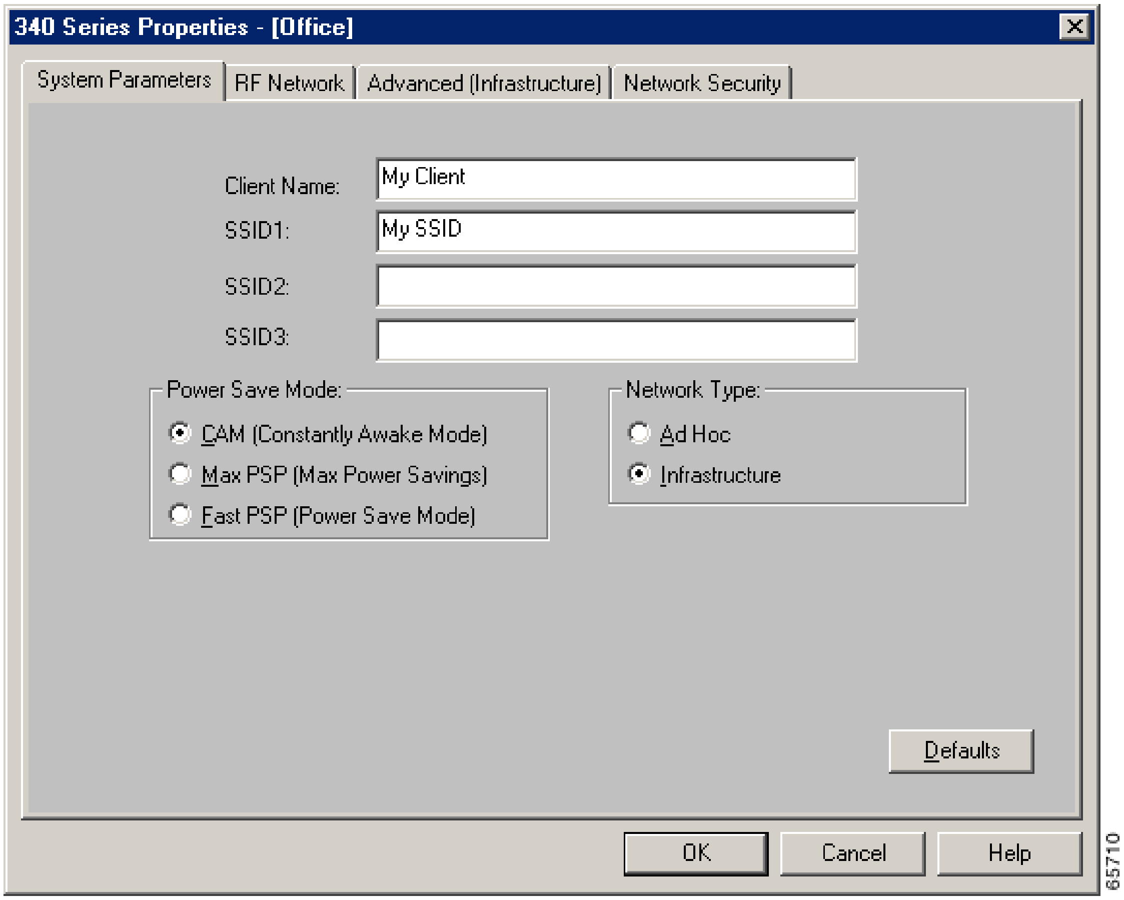
Parameter Category	Page Number
System	5-3
RF network	5-6
Advanced infrastructure	5-13
Advanced ad hoc	5-17
Network security	5-20

Note If your system administrator used an auto-installer to deactivate certain parameters in ACU, these parameters are grayed out on the ACU Properties screens and cannot be selected.

Setting System Parameters

The System Parameters screen (see Figure 5-1) enables you to set parameters that prepare the client adapter for use in a wireless network. This screen appears after you create and save a new profile or click Edit on the Profile Manager screen.

Figure 5-1 System Parameters Screen



Client Name: My Client

SSID1: My SSID

SSID2:

SSID3:

Power Save Mode:
- ● CAM (Constantly Awake Mode)
- ○ Max PSP (Max Power Savings)
- ○ Fast PSP (Power Save Mode)

Network Type:
- ○ Ad Hoc
- ● Infrastructure

Table 5-2 lists and describes the client adapter’s system parameters. Follow the instructions in the table to change any parameters.

Table 5-2 System Parameters

Parameter	Description
Client Name	A logical name for your workstation. 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:** You can key in up to 16 ASCII characters **Default:** A blank field **Note** Each computer on the network should have a unique client name.
SSID1	The service set identifier (SSID) identifies the specific wireless network that you want to access. **Range:** You can key in up to 32 ASCII characters (case sensitive) Default: A blank field **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 is unable to access the network.
SSID2	An optional SSID that identifies a second distinct network and enables you to roam to that network without having to reconfigure your client adapter. **Range:** You can key in up to 32 ASCII characters (case sensitive) **Default:** A blank field
SSID3	An optional SSID that identifies a third distinct network and enables you to roam to that network without having to reconfigure your client adapter. **Range:** You can key in up to 32 ASCII characters (case sensitive) **Default:** A blank field

Table 5-2 System Parameters (continued)

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td rowspan="5">Power Save Mode</td><td colspan="2">Sets your client adapter to its optimum power consumption setting.
Options: CAM, Max PSP, or Fast PSP
Default: CAM (Constantly Awake Mode)</td></tr>
<tr><th>Power Save Mode</th><th>Description</th></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>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).
Note When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode will be temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</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>
</table>

Table 5-2 System Parameters (continued)

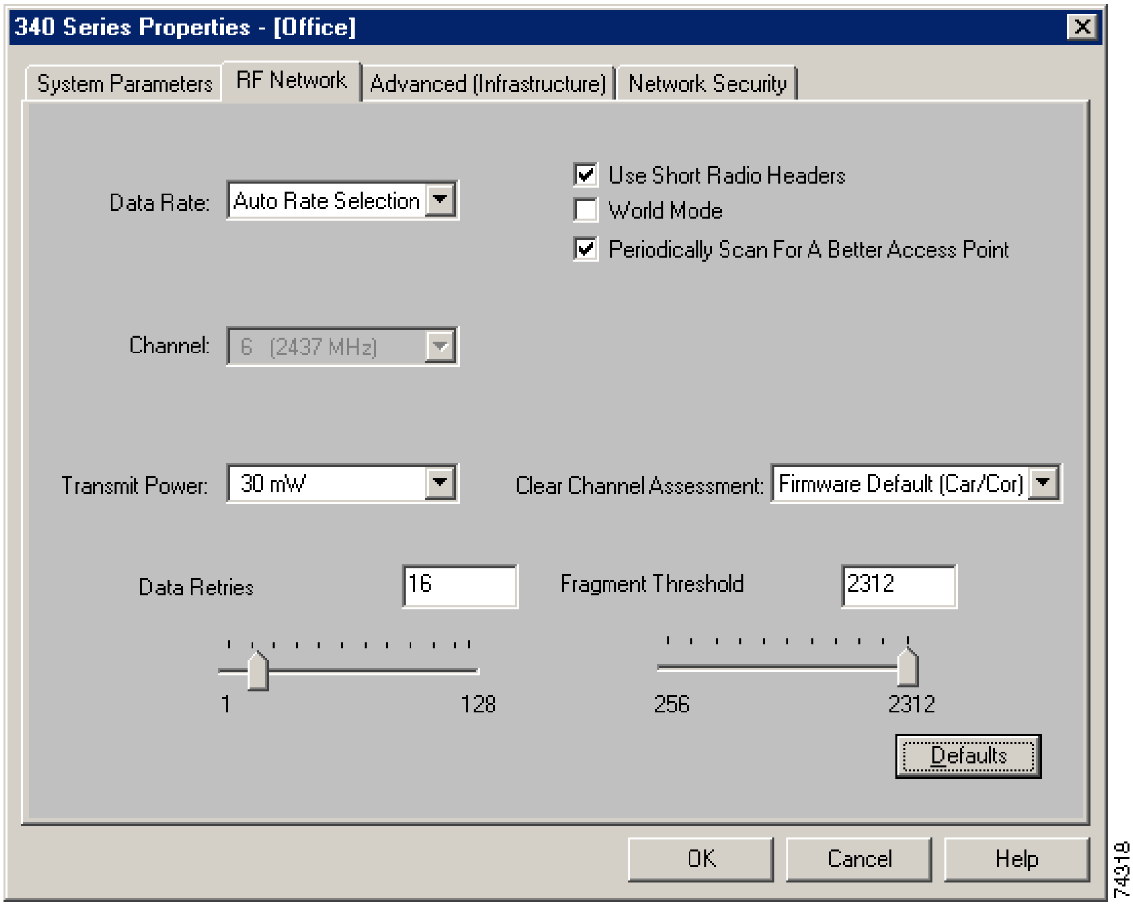
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Network Type</td><td>Specifies the type of network in which your client adapter is installed.
<b>Options:</b> Ad Hoc or Infrastructure
<b>Default:</b> Infrastructure
<table>
<tr><th>Network Type</th><th>Description</th></tr>
<tr><td>Ad Hoc</td><td>Often referred to as <i>peer to peer</i>. Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so users can share information in a meeting.</td></tr>
<tr><td>Infrastructure</td><td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td></tr>
</table>
</td></tr>
</table>

Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

Setting RF Network Parameters

The RF Network screen (see Figure 5-2) enables you to set parameters that control how and when the client adapter transmits and receives data. To access this screen, select the **RF Network** tab from the Properties screens.

Figure 5-2 RF Network Screen



340 Series Properties - [Office]

Data Rate: Auto Rate Selection

☑ Use Short Radio Headers
☐ World Mode
☑ Periodically Scan For A Better Access Point

Channel: 6 (2437 MHz)

Transmit Power: 30 mW

Clear Channel Assessment: Firmware Default (Car/Cor)

Data Retries 16

Fragment Threshold 2312

Table 5-3 lists and describes the client adapter’s RF network parameters. Follow the instructions in the table to change any parameters.

Table 5-3 RF Network Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Data Rate</td><td>
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 Rate Selection is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.
<b>Options:</b> Auto Rate Selection, 1 Mbps Only, 2 Mbps Only, 5.5 Mbps Only, or 11 Mbps Only (2.4-GHz client adapters);
Auto Rate Selection, 6 Mbps Only, 9 Mbps Only, 12 Mbps Only, 18 Mbps Only, 24 Mbps Only, 36 Mbps Only, 48 Mbps Only, or 54 Mbps Only (5-GHz client adapters)
<b>Default:</b> Auto Rate Selection
<table>
<tr><th colspan="2">Data Rate</th><th rowspan="2">Description</th></tr>
<tr><th>2.4-GHz Client Adapters</th><th>5-GHz Client Adapters</th></tr>
<tr><td>Auto Rate Selection</td><td>Auto Rate Selection</td><td>Uses the 11-Mbps (for 2.4-GHz client adapters) or 54-Mbps (for 5-GHz client adapters) data rate when possible but drops to lower rates when necessary.</td></tr>
<tr><td>1 Mbps Only</td><td>6 Mbps Only</td><td>Offers the greatest range but the lowest throughput.</td></tr>
<tr><td>2 Mbps Only and 5.5 Mbps Only</td><td>9 Mbps Only to 48 Mbps Only</td><td>Progressively offers less range but greater throughput than the 1 Mbps Only (for 2.4-GHz client adapters) or 6 Mbps Only (for 5-GHz client adapters) option.</td></tr>
<tr><td>11 Mbps Only</td><td>54 Mbps Only</td><td>Offers the greatest throughput but the lowest range.</td></tr>
</table>
<b>Note</b> Your client adapter’s data rate must be set to Auto Rate Selection 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.
</td></tr>
</table>

Table 5-3 RF Network Parameters (continued)

Parameter	Description
Use Short Radio Headers	Selecting this checkbox sets your client adapter to use short radio headers. However, the adapter can use short radio headers only if the access point is also configured to support them and is using them. If any clients associated to an access point are using long headers, then *all* clients in that cell must also use long headers, even if both this client and the access point have short radio headers enabled. Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers. **Default:** Selected **Note** This parameter is available only for 2.4-GHz client adapters. **Note** This parameter is referred to as *Preambles* on the access point screens.
World Mode	Selecting this checkbox 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. **Default:** Deselected **Note** This parameter is available only for 2.4-GHz client adapters. **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.
Periodically Scan For A Better Access Point	Selecting this checkbox causes the client to look for a better access point if its signal strength becomes low and to switch associations if it finds one. **Default:** Selected **Note** This parameter is available only if your client adapter is using PCM/LMC/PCI card firmware version 4.25.30 or greater, mini PCI card firmware version 5.00.03 or greater, or PC-Cardbus card firmware version 4.99 or greater.

Table 5-3 RF Network Parameters (continued)

Parameter	Description
Channel	Specifies which frequency your client adapter will use as the channel for communications. These channels conform to the IEEE 802.11 Standard for your regulatory domain. • In infrastructure mode, this parameter is set automatically and cannot be changed. The client adapter listens to the entire spectrum, selects the best access point to associate to, and uses the same frequency as that access point. • In ad hoc mode, the channel of the client adapter must be set to match the channel used by the other clients in the wireless network. **Range:** Dependent on client adapter radio and regulatory domain **Example for 2.4-GHz client adapters:** 1 to 11 (2412 to 2462 MHz) in North America **Example for 5-GHz client adapters:** 36, 40, 44, 48, 52, 56, 60, and 64 (5180, 5200, 5220, 5240, 5260, 5280, 5300, and 5320 MHz) in North America **Default:** Dependent on client adapter radio and regulatory domain **Example for 2.4-GHz client adapters:** 6 (2437 MHz) in North America **Example for 5-GHz client adapters:** 36 (5180 MHz) in North America **Note** Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

Table 5-3 RF Network Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<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.).
<b>Options:</b> Dependent on the power table programmed into the client adapter; see the table below
<b>Default:</b> The maximum level programmed into the client adapter and allowed by your country's regulatory agency
<table>
<tr><th>Possible Power Levels</th><th>Client Adapter Type</th></tr>
<tr><td>100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW</td><td>350 series client adapters</td></tr>
<tr><td>30 mW or 1 mW</td><td>340 series PC cards</td></tr>
<tr><td>30 mW, 15 mW, 5 mW, or 1 mW</td><td>340 series PCI cards and LM cards</td></tr>
<tr><td>20 mW, 10 mW, or 5 mW</td><td>PC-Cardbus card</td></tr>
</table>
<b>Note</b> Reducing the transmit power level conserves battery power but decreases radio range.
<b>Note</b> 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.
<b>Note</b> 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.</td></tr>
</table>

Table 5-3 RF Network Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Clear Channel Assessment</td><td>Specifies the method that determines whether the channel on which your client adapter will operate is clear prior to the transmission of data.
<b>Options:</b> Firmware Default (<i>XXX</i>), Carrier/Correlation (Car/Cor), Energy Detect (ED), or ED or Car/Cor
<b>Default:</b> Firmware Default (<i>XXX</i>)
<table>
<tr><th>Method</th><th>Description</th></tr>
<tr><td>Firmware Default (<i>XXX</i>)</td><td>The Clear Channel Assessment (CCA) mechanism will report that the channel is busy based on the default value of the client adapter’s firmware. The firmware’s CCA default value is shown in parentheses.
<b>Note</b> The CCA default value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.</td></tr>
<tr><td>Carrier/Correlation (Car/Cor)</td><td>The CCA mechanism will report that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.</td></tr>
<tr><td>Energy Detect (ED)</td><td>The CCA mechanism will report that the channel is busy upon detection of any energy above the ED threshold.</td></tr>
<tr><td>ED or Car/Cor</td><td>The CCA mechanism will report that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.</td></tr>
</table>
<b>Note</b> This parameter is available only for 2.4-GHz client adapters using PCM/LMC/PCI card firmware version 4.25.30 or greater (or mini PCI card firmware version 5.00.03 or greater).</td></tr>
</table>

Table 5-3 RF Network Parameters (continued)

Parameter	Description
Data Retries	Defines the number of times a packet will be resent if the initial transmission is unsuccessful. Range: 1 to 128 **Default:** 16 **Note** If your network protocol performs its own retries, set this to a smaller value than the default. This way notification of a “bad” packet is sent up the protocol stack quickly so the application can retransmit the packet if necessary.
Fragment Threshold	Defines the threshold above which an RF data packet will be split up or fragmented. If one of those fragmented packets experiences interference during transmission, only that specific packet would need to be resent. Throughput is generally lower for fragmented packets because the fixed packet overhead consumes a higher portion of the RF bandwidth. **Range:** 256 to 2312 **Default:** 2312

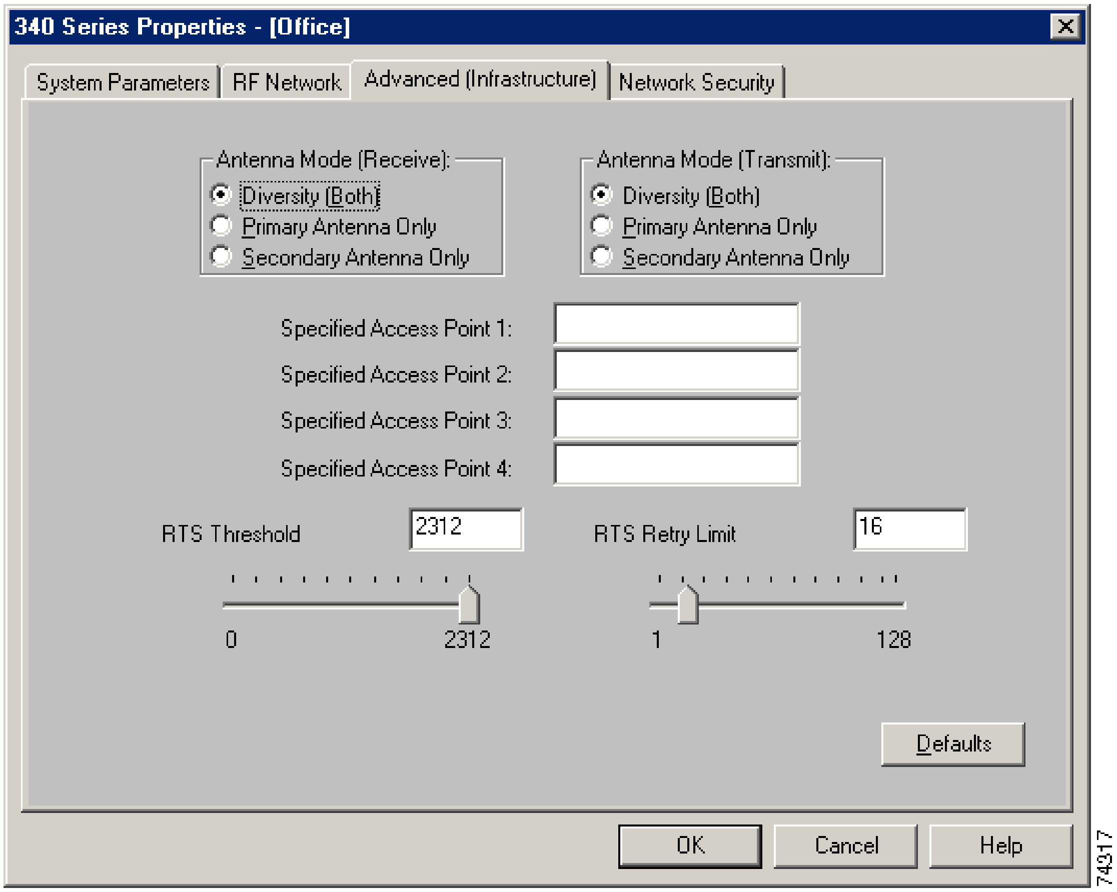
Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

Setting Advanced Infrastructure Parameters

Note You can set advanced infrastructure parameters only if your client adapter has been set to operate in an infrastructure network. See the Network Type parameter in Table 5-2.

The Advanced (Infrastructure) screen (see Figure 5-3) enables you to set parameters that control how the client adapter operates within an infrastructure network. To access this screen, select the **Advanced (Infrastructure)** tab from the Properties screens.

Figure 5-3 Advanced (Infrastructure) Screen



340 Series Properties - [Office]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Antenna Mode (Receive):
● Diversity (Both)
○ Primary Antenna Only
○ Secondary Antenna Only

Antenna Mode (Transmit):
● Diversity (Both)
○ Primary Antenna Only
○ Secondary Antenna Only

Specified Access Point 1:
Specified Access Point 2:
Specified Access Point 3:
Specified Access Point 4:

RTS Threshold: 2312
RTS Retry Limit: 16

Table 5-4 lists and describes the client adapter's advanced infrastructure parameters. Follow the instructions in the table to change any parameters.

Table 5-4 Advanced (Infrastructure) Parameters

Parameter	Description
Antenna Mode (Receive)	Specifies the antenna that your client adapter uses to receive data. • PC card – The PC card's integrated, permanently attached antenna operates best when used in diversity mode. Diversity mode allows the card to use the better signal from its two antenna ports. **Options:** Diversity (Both), Primary Antenna Only, Secondary Antenna Only **Default:** Diversity (Both) • LM card – The LM card is shipped without an antenna; however, an antenna can be connected through the card's external connector. If a snap-on antenna is used, diversity mode is recommended. Otherwise, select the mode that corresponds to the antenna port to which the antenna is connected. **Options:** Diversity (Both), Primary Antenna Only, Secondary Antenna Only **Default:** Diversity (Both) • PCI client adapter – The PCI client adapter must use the Primary Antenna Only option. **Default:** Primary Antenna Only • Mini PCI card – The mini PCI card, which can be used with one or two antennas, operates best in diversity mode. Diversity mode allows the card to use the better signal from its two antenna connectors. **Options:** Diversity (Both), Primary Antenna Only, Secondary Antenna Only **Default:** Diversity (Both) **Note** This parameter is available only for 2.4-GHz client adapters. **Note** The Primary Antenna Only and Secondary Antenna Only options were formerly named Right Antenna Only and Left Antenna Only, respectively.
Antenna Mode (Transmit)	Specifies the antenna that your client adapter uses to transmit data. See the Antenna Mode (Receive) parameter above for information on the options available for your client adapter. **Note** This parameter is available only for 2.4-GHz client adapters.

Table 5-4 Advanced (Infrastructure) Parameters (continued)

Parameter	Description
Specified Access Point 1- 4	Specifies the MAC addresses of up to four preferred access points with which the client adapter can associate. If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point. You can enter the MAC addresses of the access points in the edit boxes or choose not to specify access points by leaving the boxes blank. **Default:** Blank fields **Note** This parameter should be used only for access points that are in repeater mode. For normal operation, leave these fields blank because specifying an access point slows down the roaming process.
RTS Threshold	Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet. Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced, but the system is able to recover faster from interference or collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces. Range: 0 to 2312 **Default:** 2312 **Note** Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.
RTS Retry Limit	Specifies the number of times the client adapter will resend a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet. Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered but makes the system more immune to interference and collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces. Range: 1 to 128 **Default:** 16 **Note** Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.

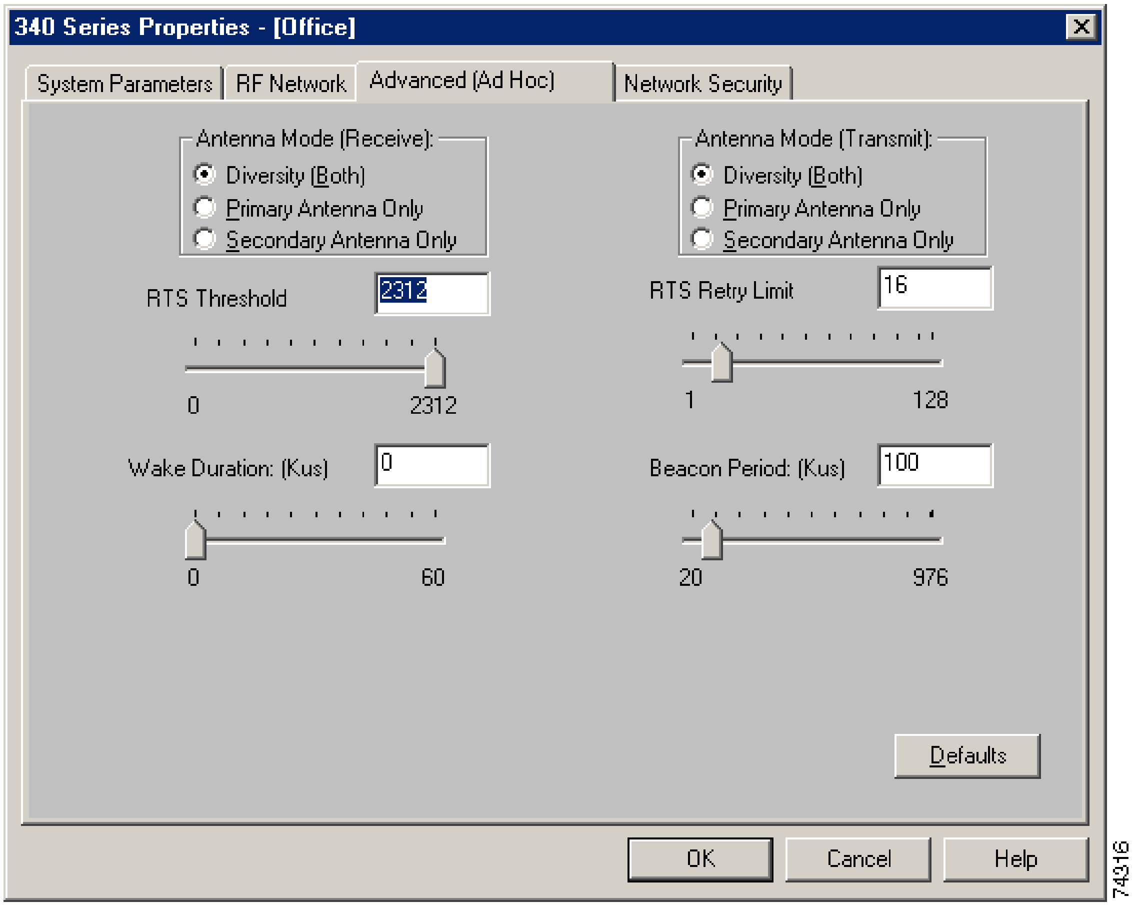
Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

Setting Advanced Ad Hoc Parameters

Note You can set advanced ad hoc parameters only if your client adapter has been set to operate in an ad hoc network. See the Network Type parameter in Table 5-2.

The Advanced (Ad Hoc) screen (see Figure 5-4) enables you to set parameters that control how the client adapter operates within an ad hoc network. To access this screen, select the **Advanced (Ad Hoc)** tab from the Properties screens.

Figure 5-4 Advanced (Ad Hoc) Screen



Antenna Mode (Receive):
● Diversity (Both)
○ Primary Antenna Only
○ Secondary Antenna Only

Antenna Mode (Transmit):
● Diversity (Both)
○ Primary Antenna Only
○ Secondary Antenna Only

RTS Threshold 2312 (0 – 2312)

RTS Retry Limit 16 (1 – 128)

Wake Duration: (Kus) 0 (0 – 60)

Beacon Period: (Kus) 100 (20 – 976)

Table 5-5 lists and describes the client adapter's advanced ad hoc parameters. Follow the instructions in the table to change any parameters.

Table 5-5 Advanced (Ad Hoc) Parameters

Parameter	Description
Antenna Mode (Receive)	Specifies the antenna that your client adapter uses to receive data. • PC card – The PC card's integrated, permanently attached antenna operates best when used in diversity mode. Diversity mode allows the card to use the better signal from its two antenna ports. **Options:** Diversity (Both), Primary Antenna Only, Secondary Antenna Only **Default:** Diversity (Both) • LM card – The LM card is shipped without an antenna; however, an antenna can be connected through the card's external connector. If a snap-on antenna is used, diversity mode is recommended. Otherwise, select the mode that corresponds to the antenna port to which the antenna is connected. **Options:** Diversity (Both), Primary Antenna Only, Secondary Antenna Only **Default:** Diversity (Both) • PCI client adapter – The PCI client adapter must use the Primary Antenna Only option. **Default:** Primary Antenna Only • Mini PCI card – The mini PCI card, which can be used with one or two antennas, operates best in diversity mode. Diversity mode allows the card to use the better signal from its two antenna connectors. **Options:** Diversity (Both), Primary Antenna Only, Secondary Antenna Only **Default:** Diversity (Both) **Note** This parameter is available only for 2.4-GHz client adapters. **Note** The Primary Antenna Only and Secondary Antenna Only options were formerly named Right Antenna Only and Left Antenna Only, respectively.
Antenna Mode (Transmit)	Specifies the antenna that your client adapter uses to transmit data. See the Antenna Mode (Receive) parameter above for information on the options available for your client adapter. **Note** This parameter is available only for 2.4-GHz client adapters.

Table 5-5 Advanced (Ad Hoc) Parameters (continued)

Parameter	Description
RTS Threshold	Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet. Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced, but the system is able to recover faster from interference or collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces. **Range:** 0 to 2312 **Default:** 2312 **Note** Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.
RTS Retry Limit	Specifies the number of times the client adapter will resend a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet. Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered but makes the system more immune to interference and collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces. Range: 1 to 128 **Default:** 16 **Note** Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.
Wake Duration (Kμs)	Specifies the amount of time following a beacon that the client adapter stays awake to receive announcement traffic indication message (ATIM) packets, which are sent to the adapter to keep it awake until the next beacon. Refer to the Power Save Mode parameter in Table 5-2. **Range:** 0 Kμs (in CAM mode); 5 to 60 Kμs (in Max PSP or Fast PSP mode) **Default:** 5 Kμs **Note** If your client adapter is set to CAM mode, you must set the wake duration to 0 Kμs. If your client adapter is set to Max PSP or Fast PSP mode, you must set the wake duration to a minimum of 5 Kμs. **Note** Kμs is a unit of measurement in software terms. K = 1024, μ = 10^{-6}, and s = seconds, so Kμs = .001024 seconds, 1.024 milliseconds, or 1024 microseconds.

Table 5-5 Advanced (Ad Hoc) Parameters (continued)

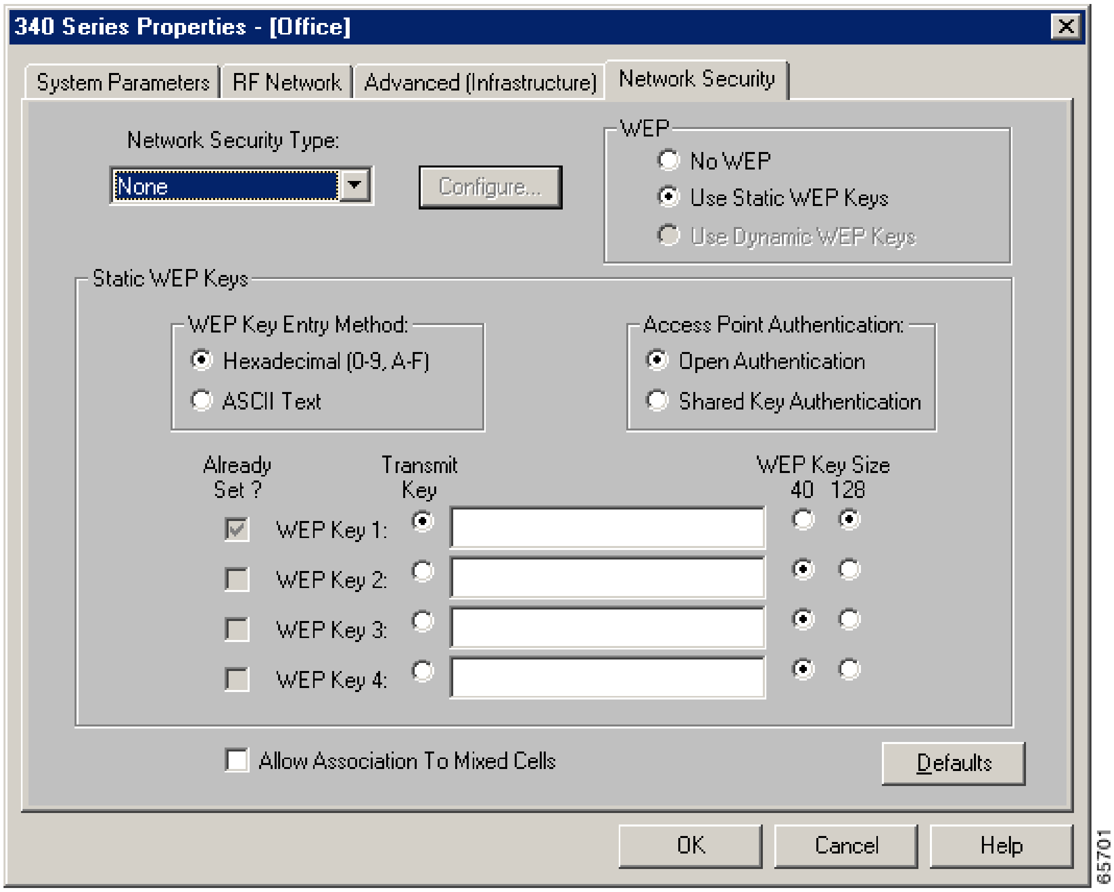
Parameter	Description
Beacon Period (Kµs)	Specifies the duration between beacon packets, which are used to help clients find each other in ad hoc mode. Range: 20 to 976 Kµs **Default:** 100 Kµs

Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

Setting Network Security Parameters

The Network Security screen (see Figure 5-5) enables you to set parameters that control how the client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data. To access this screen, select the **Network Security** tab from the Properties screens.

Figure 5-5 Network Security Screen



Network Security Type: None

WEP
○ No WEP
● Use Static WEP Keys
○ Use Dynamic WEP Keys

Static WEP Keys

WEP Key Entry Method:
● Hexadecimal (0-9, A-F)
○ ASCII Text

Access Point Authentication:
● Open Authentication
○ Shared Key Authentication

Already Set ?		Transmit Key		WEP Key Size 40	128
☑	WEP Key 1:	●		○	●
□	WEP Key 2:	○		●	○
□	WEP Key 3:	○		●	○
□	WEP Key 4:	○		●	○

□ Allow Association To Mixed Cells

This screen is different from the other Properties screens in that it presents several security features, each of which involves a number of steps. In addition, the security features themselves are complex and need to be understood before they are implemented. Therefore, this section provides an overview of the security features as well as procedures for using them.

However, before you determine the appropriate security settings for your client adapter, you must decide how to set the **Allow Association To Mixed Cells** parameter, which appears at the bottom of the Network Security screen and is not associated to any of the security features. See the "Setting the Allow Association To Mixed Cells Parameter" section below.

Setting the Allow Association To Mixed Cells Parameter

The Allow Association To Mixed Cells parameter indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations. Follow the steps below to set this parameter.

Step 1 Perform one of the following:

- Select the **Allow Association To Mixed Cells** checkbox if the access point with which the client adapter is to associate has WEP set to Optional (regardless of whether WEP is enabled on the adapter). Otherwise, the client adapter is unable to establish a connection with the access point.
- Deselect the **Allow Association To Mixed Cells** checkbox if the access point with which the client adapter is to associate does not have WEP set to Optional. This is the default setting.

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.

Step 2 Perform one of the following:

- If you do not want to change any other parameters on the Network Security screen, click **OK** to return to the Profile Manager screen; then click **OK** or **Apply** to save your changes
- If you want to change some of the other parameters on the Network Security screen, go to the next section.

Overview of Security Features

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 EAP authentication process. The information in the "Static WEP Keys" and "EAP (with Static or Dynamic WEP Keys)" sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with EAP 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 offer a greater level of security than 40-bit WEP keys.

Note Refer to the "Additional WEP Key Security Features" section on page 5-24 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

Each device (or profile) 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 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 device is rebooted. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows 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.

The Network Security screen 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 as well as to enable or disable static WEP. Refer to the "Using Static WEP" section on page 5-26 for instructions.

EAP (with Static or Dynamic WEP Keys)

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.

Two 802.1X authentication types can be selected in ACU for use with Windows operating systems:

- **EAP-Cisco Wireless** (or **LEAP**) – This authentication type is available for Windows 95, 98, NT, 2000, Me, and XP, as well as non-Windows systems. Support for LEAP is provided not in the Windows 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 Software's Steel-Belted RADIUS version 3.0 and greater.

  LEAP is enabled or disabled for a specific profile through ACU, provided LEAP was selected during ACU installation. Once enabled, a variety of configuration options are available, including how and when a username and password are entered to begin the authentication process.

  The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The 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 If LEAP was not selected during installation, the LEAP option is unavailable in ACU. If you want to be able to enable and disable LEAP, you must run the installation program again and select **Modify** and **LEAP**.

- **Host Based EAP –** Selecting this option enables you to use any 802.1X authentication type for which your operating system has built-in support. For example, Windows XP has built-in support for both EAP-TLS and EAP-MD5.
  - **EAP-TLS** – EAP-TLS is enabled or disabled through the operating system and uses a dynamic, session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. Once enabled, a few configuration parameters must be set within the operating system.

    RADIUS servers that support EAP-TLS include Cisco Secure ACS version 3.0 and greater and Cisco Access Registrar version 1.8 and greater.

    Note EAP-TLS requires the use of a certificate. Refer to Microsoft’s documentation for information on downloading and installing the certificate.

  - **EAP-MD5** – EAP-MD5 is enabled or disabled through the operating system and uses static WEP to encrypt data. EAP-MD5 requires you to enter a separate EAP username and password (in addition to your standard Windows network login) in order to start the EAP authentication process and gain access to the network.

    RADIUS servers that support EAP-MD5 include Cisco Secure ACS version 3.0 and greater and Cisco Access Registrar version 1.8 and greater.

    Note If you want to authenticate without encrypting the data that is transmitted over your network, you can use EAP-MD5 without static WEP.

Note Although EAP-TLS and EAP-MD5 are enabled in the operating system, you can set up profiles in ACU to use these authentication types. To do so, follow the instructions in the “Enabling Host-Based EAP” section on page 5-31.

When you enable Network-EAP on your access point and configure your client adapter for LEAP, EAP-TLS, or EAP-MD5 using ACU or enable Require EAP on your access point and configure your client adapter for EAP-TLS or EAP-MD5 using Windows XP, authentication to the network occurs in the following sequence:

1. The client 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 (or certificate for EAP-TLS) being the shared secret for authentication. The password (or certificate) is never transmitted during the process.

Note The authentication process is now complete for EAP-MD5. For LEAP or EAP-TLS, the process continues.

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 "Enabling LEAP" section on page 5-28 for instructions on enabling LEAP or to the "Enabling Host-Based EAP" section on page 5-31 for instructions on enabling EAP-TLS or EAP-MD5.

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

The three security features discussed in this section (MIC, TKIP, and broadcast key rotation) are designed to prevent sophisticated attacks on your wireless network's WEP keys. These features are supported in the following client adapter software releases:

- PCM/LMC/PCI card firmware version 4.25.23 or greater and PCM/LMC/PCI card driver version 8.01 or greater
- Mini PCI card firmware version 5.0 or greater and mini PCI card driver version 2.20 or greater
- PC-Cardbus card firmware version 4.99 or greater and PC-Cardbus driver 3.4.9 or greater

These features do not need to be enabled on the client adapter; they are supported automatically in the firmware and driver 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 Status screen indicates if MIC is being used, and the Statistics screen provides MIC statistics.

Note If you enable MIC on the access point, your client adapter's driver must support these features; 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 these features; 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 5-6 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 5-6 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP
EAP-TLS authentication		
If using ACU to configure card	Enable Host Based EAP in ACU and enable Smart Card or Other Certificate in Windows XP	Set up and enable WEP and enable Network-EAP
If using Windows XP to configure card	Enable Smart Card or other Certificate	Set up and enable WEP and enable Require EAP and Open Authentication

Table 5-6 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-MD5 authentication		
If using ACU to configure card	Enable Host Based EAP in ACU and enable MD5-Challenge in Windows XP	Set up and enable WEP and enable Network-EAP
If using Windows XP to configure card	Enable MD5-Challenge	Set up and enable WEP and enable Require EAP and Open Authentication
MIC	Use PCM/LMC/PCI card driver version 8.01 or greater, mini PCI card driver version 2.20 or greater, or PC-Cardbus card driver version 3.4.9 or greater	Set up and enable WEP with full encryption, set MIC to MMH, and set Use Aironet Extensions to Yes
TKIP	Use PCM/LMC/PCI card firmware version 4.25.23 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater	Set up and enable WEP, set TKIP to Cisco, and set Use Aironet Extensions to Yes
Broadcast key rotation	Use PCM/LMC/PCI card firmware version 4.25.23 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater and enable LEAP	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

Using Static WEP

This section provides instructions for entering new static WEP keys or overwriting existing static WEP keys.

Entering a New Static WEP Key

Follow the steps below to enter a new static WEP key for this profile.

Step 1 Select **None** from the Network Security Type drop-down box on the Network Security screen.

Step 2 Select **Use Static WEP Keys** under WEP.

Step 3 Select one of the following WEP key entry methods:

- **Hexadecimal (0-9, A-F)** – Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text** – Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.

Step 4 Select one of the following access point authentication options, which defines how your client adapter will attempt to authenticate to an access point:

- **Open Authentication** – Allows your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. Open Authentication is the default setting.
- **Shared Key Authentication** – Allows your client adapter to communicate only with access points that have the same WEP key. This option is available only if **Use Static WEP Keys** is selected.

  In shared key authentication, 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. If the packet is successfully encrypted/decrypted, the user is considered to be authenticated.

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

Step 5 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 6 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 must contain the following number of characters:
  - 10 hexadecimal characters or 5 ASCII text characters for 40-bit keys

    Example: 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
  - 26 hexadecimal characters or 13 ASCII text characters for 128-bit keys

    Example: 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)
- 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 7 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 8 Click **OK** to return to the Profile Manager screen; then click **OK** or **Apply** to save your changes.

Overwriting an Existing Static WEP Key

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

Note You can overwrite existing WEP keys, but you cannot edit or delete them.

Step 1 Look at the current WEP key settings in the middle of the Network Security 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 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 6 of the "Entering a New Static WEP Key" section on page 5-26.

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 return to the Profile Manager screen; then click **OK** or **Apply** to save your changes

Disabling Static WEP

If you ever need to disable static WEP for a particular profile, select **No WEP** under WEP on the Network Security screen, click **OK**, and click **OK** or **Apply** on the Profile Manager screen.

Note Selecting **LEAP** from the Network Security Type drop-down box on the Network Security screen disables static WEP automatically.

Enabling LEAP

Note LEAP authentication is supported only on client adapters that support WEP and use PCM/LMC/PCI card firmware version 4.13 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus firmware version 4.99 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). Mini PCI firmware and PC-Cardbus card firmware were first released at draft 10.

Follow the steps below to enable LEAP authentication for this profile.

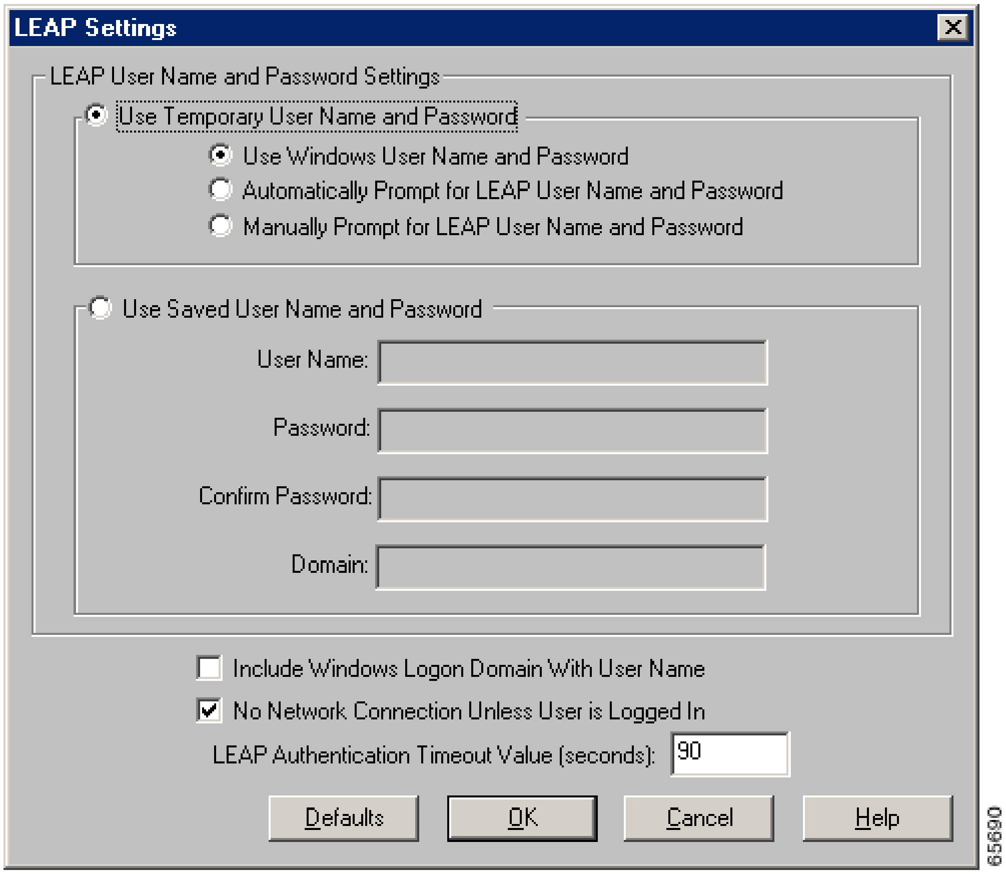
Step 1 Select **LEAP** from the Network Security Type drop-down box on the bottom of the Network Security screen.

> **Note** When you select this option, dynamic WEP is set automatically.

> **Note** The LEAP option is available only if you selected LEAP during the ACU installation process and the firmware supports it.

Step 2 Click **Configure** to the right of the Network Security Type drop-down box. The LEAP Settings screen appears (see Figure 5-6).

Figure 5-6 LEAP Settings Screen



LEAP Settings

LEAP User Name and Password Settings

● Use Temporary User Name and Password

● Use Windows User Name and Password
○ Automatically Prompt for LEAP User Name and Password
○ Manually Prompt for LEAP User Name and Password

○ Use Saved User Name and Password

User Name:
Password:
Confirm Password:
Domain:

□ Include Windows Logon Domain With User Name
☑ No Network Connection Unless User is Logged In
LEAP Authentication Timeout Value (seconds): 90

Step 3 Select one of the following LEAP username and password setting options:

- **Use Temporary User Name and Password** – Requires you to enter the LEAP username and password each time the computer reboots in order to authenticate and gain access to the network.
- **Use Saved User Name and Password** – Does not require you to enter a LEAP username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

Note The Use Saved User Name and Password option is available only if the Allow Saved LEAP User Name and Password checkbox was selected during installation.

Note If a profile is using LEAP, it can be included in auto profile selection only if it has a saved user name and password. The Include Profile In Auto Profile Selection checkbox on the Profile Manager screen is grayed out and cannot be selected for profiles that are using LEAP without a saved user name and password.

Step 4 Perform one of the following:

- If you selected Use Temporary User Name and Password in Step 3, select one of the following options:
  - **Use Windows User Name and Password** – Causes your Windows username and password to also serve as your LEAP username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for LEAP User Name and Password** – Requires you to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for LEAP User Name and Password** – Requires you to manually invoke the LEAP authentication process as needed using the Manual LEAP Login option from the Commands drop-down menu. You are not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a SoftToken one-time password system or other systems that require additional software that is not available at login.
- If you selected Use Saved User Name and Password in Step 3, follow the steps below:

a. Enter a username and password in the appropriate fields.

Note Usernames and passwords are limited to 32 ASCII characters each. However, if a domain name is entered in the Domain field, the sum of the username and domain name is limited to 31 ASCII characters.

b. Re-enter the password in the Confirm Password field.

c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.

Step 5 If you work in an environment with multiple domains and, therefore, want your Windows login domain to be passed to the RADIUS server along with your username, select the **Include Windows Login Domain With User Name** checkbox. The default setting is selected.

Note If you selected to use a saved username and password but do not select the Include Windows Login Domain With User Name checkbox, the Domain field becomes unavailable, and a domain name is not passed to the RADIUS server.

Step 6 If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, select the **No Network Connection Unless User is Logged In** checkbox. The default setting is selected.

Step 7 In the LEAP Authentication Timeout Value field, enter the amount of time (in seconds) before a LEAP authentication is considered to be failed and an error message appears.

Range: 10 to 300 seconds

Default: 90 seconds

Step 8 Click **OK** to exit the LEAP Settings screen.

Step 9 Click **OK** to exit the Network Security screen and return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes

Note Chapter 6 describes the sequence of events that occurs when a profile that is set for LEAP authentication is selected for use.

Enabling Host-Based EAP

Note Host-based EAP authentication is supported only on client adapters that support WEP and use PCM/LMC/PCI card firmware version 4.13 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater.

Note In order to use EAP-TLS or EAP-MD5 authentication, your client adapter and access point must use 802.1X draft standard 10 firmware.

Follow the steps below to enable host-based EAP authentication (such as EAP-TLS or EAP-MD5) for this profile.

Step 1 Select **Host Based EAP** from the Network Security Type drop-down box on the Network Security screen.

Note The Host Based EAP option is available only if your computer's operating system has built-in EAP support, such as Windows XP.

Step 2 Perform one of the following:

- If you are planning to use EAP-TLS authentication, select **Use Dynamic WEP Keys** under WEP.
- If you are planning to use EAP-MD5 authentication with static WEP, select **Use Static WEP Keys** under WEP.
- If you are planning to use EAP-MD5 authentication without WEP, select **No WEP** under WEP.

Step 3 If you are planning to use EAP-MD5 authentication with static WEP, follow Step 3 through Step 7 in the "Entering a New Static WEP Key" section to create a new static WEP key or follow the steps in the "Overwriting an Existing Static WEP Key" section to overwrite an existing static WEP key.

Step 4 Click **OK** to return to the Profile Manager screen.

Step 5 Click **OK** or **Apply** on the Profile Manager screen to save your changes.

Step 6 On your computer desktop, double-click **My Computer**, **Control Panel**, and **Network Connections**.

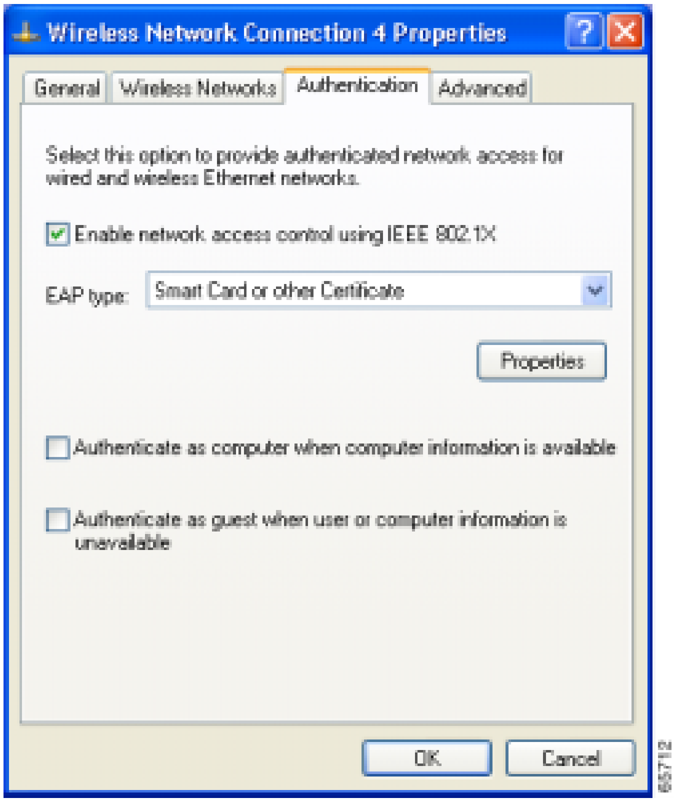
Note These instructions assume you are using Windows XP's classic view rather than its category view.

Step 7 Right-click **Wireless Network Connection**.

Step 8 Click **Properties**. The Wireless Network Connection Properties screen appears.

Step 9 Click the **Authentication** tab. The following screen appears (see Figure 5-7).

Figure 5-7 Wireless Network Connection Properties Screen (Authentication Tab)


Wireless Network Connection 4 Properties

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: Smart Card or other Certificate

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

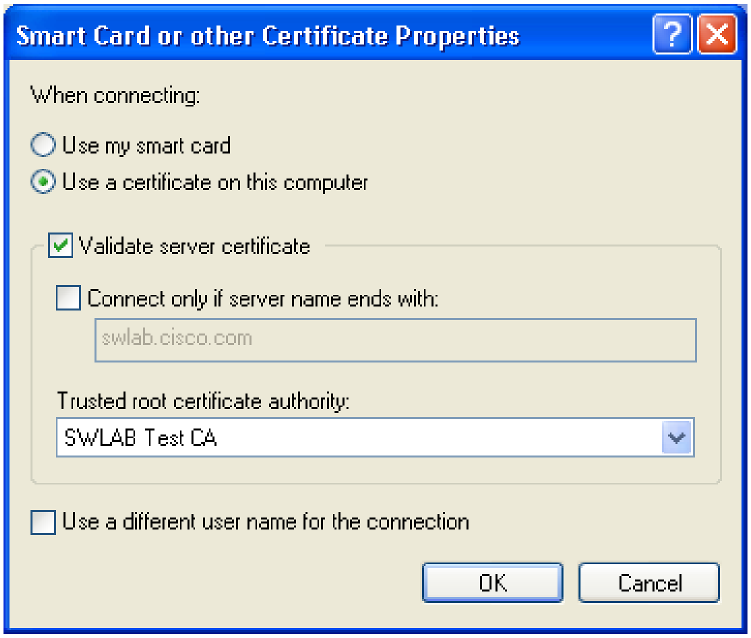
Step 10 Select the **Enable network access control using IEEE 802.1X** checkbox.

Step 11 Perform one of the following:

- If you are planning to use EAP-TLS, select **Smart Card or other Certificate** for EAP type; then go to Step 12.
- If you are planning to use EAP-MD5, select **MD5-Challenge** for EAP type; then go to Step 16.

Step 12 Click **Properties**. The Smart Card or other Certificate Properties screen appears (see Figure 5-8).

Figure 5-8 Smart Card or other Certificate Properties Screen



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Validate server certificate

□ Connect only if server name ends with:

swlab.cisco.com

Trusted root certificate authority:

SWLAB Test CA

□ Use a different user name for the connection

Step 13 Select the **Use a certificate on this computer** option.

Step 14 Select the **Validate server certificate** checkbox.

Step 15 Make sure that the name of the certificate authority from which the EAP-TLS certificate was downloaded appears in the Trusted root certificate authority field.

Step 16 Click **OK** to save your settings. The configuration is complete.

Note Chapter 6 describes the sequence of events that occurs when a profile that is set for EAP authentication is selected for use.

Disabling LEAP or Host-Based EAP

If you ever need to disable LEAP or host-based EAP for a particular profile, follow the instructions below for your EAP authentication type.

Disabling LEAP

To disable LEAP for a particular profile, select **None** from the Network Security Type drop-down box on the Network Security screen in ACU, click **OK**, and click **OK** or **Apply** on the Profile Manager screen.

Disabling Host-Based EAP

To disable host-based EAP (EAP-TLS or EAP-MD5) for a particular profile, follow the steps below:

Step 1 Select **None** from the Network Security Type drop-down box on the Network Security screen in ACU and click **OK**.

Step 2 Click **OK** or **Apply** on the Profile Manager screen.

Step 3 On your computer desktop, double-click **My Computer**, **Control Panel**, and **Network Connections**.

Step 4 Right-click **Wireless Network Connection**.

Step 5 Click **Properties**. The Wireless Network Connection Properties screen appears.

Step 6 Click the **Authentication** tab.

Step 7 Deselect the **Enable network access control using IEEE 802.1X** checkbox.

Step 8 Click **OK**.

Using EAP Authentication

This chapter explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is selected for use.

The following topics are covered in this chapter:

Overview

This chapter explains the sequence of events that occurs as soon as you or ACU's auto profile selection feature selects a profile that uses EAP authentication as well as after you eject and reinsert the client adapter, reboot the computer, log off while this profile is selected, or are informed that your username and password have expired. The chapter contains five sections based on the profile's authentication type and its username and password settings: LEAP (with the Windows username and password, with an automatically prompted login, with a manually prompted login, or with a saved username and password) or host-based EAP.

When LEAP authentication begins, the "LEAP Authentication in progress" message appears. This message provides information about the status of authentication. Table 6-1 lists and explains the stages of LEAP authentication.

Table 6-1 Stages of LEAP Authentication

Status Message	Explanation
Starting LEAP Authentication	The client adapter associates to an access point, and the LEAP authentication process begins.
Checking Link Status	The client adapter is LEAP authenticated, and the network connection is verified.
Renewing IP Address	If DHCP is enabled, the IP address is released and renewed.
Finding Domain Controller	If you are logging into a domain and the active profile specifies that the domain name be included, an attempt is made to find the domain controller to make sure subsequent access to the domain is successful.

Follow the instructions for your profile's authentication type and credential settings to successfully authenticate.

Using LEAP with the Windows Username and Password

After Profile Selection/Card Insertion

After you (or auto profile selection) select a profile that uses LEAP authentication and specifies that your Windows username and password also serve as your LEAP username and password or you eject and reinsert the client adapter while this profile is selected, the following events occur:

1. The "LEAP Authentication in progress" message appears.
2. If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows "LEAP Authenticated."

   If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the "Error Messages" section in Chapter 9 for the necessary action to take.

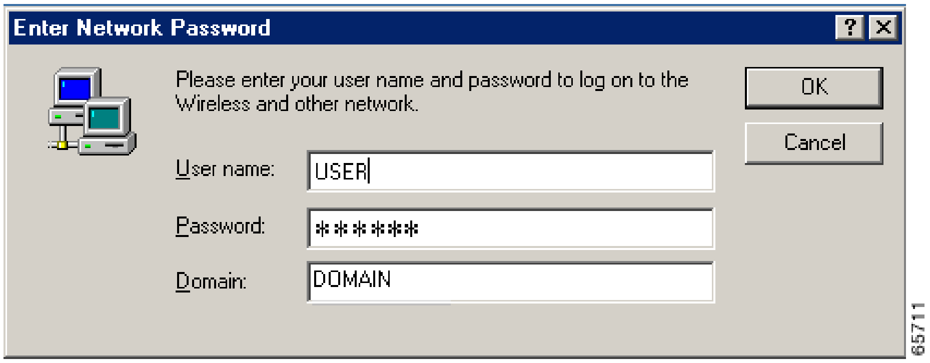
After a Reboot/Logoff

After your computer reboots or you log off, follow the steps below to LEAP authenticate.

Step 1 When the Windows login screen appears (see Figure 6-1 and Figure 6-2), enter your Windows username and password and click **OK**. The domain name is optional.

Note If your computer is running Windows NT, 2000, or XP and has Novell Client 32 software installed, a separate LEAP login screen appears before the Novell login screen. If this occurs, enter your Windows and Novell username and password in the login screens and click **OK**.

Figure 6-1 Windows Login Screen (Windows 95, 98, and Me)



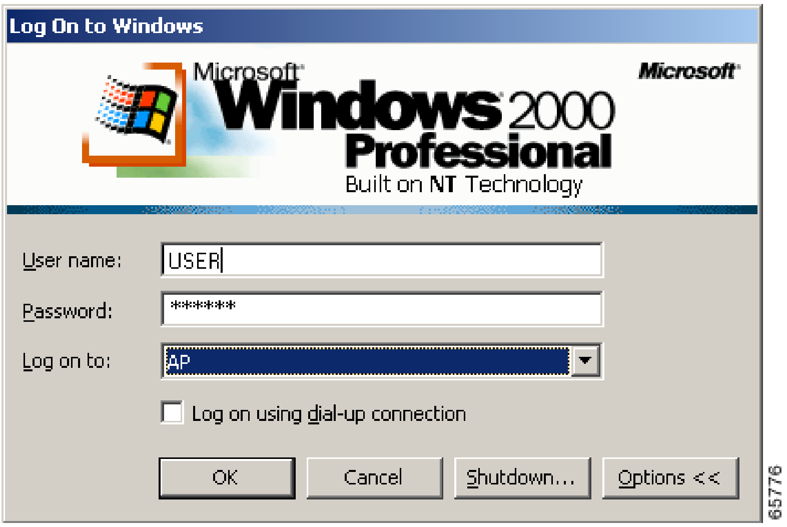
Please enter your user name and password to log on to the Wireless and other network.

User name: USER

Password: ******

Domain: DOMAIN

Figure 6-2 Windows Login Screen (Windows 2000)



User name: USER

Password: *******

Log on to: AP

□ Log on using dial-up connection

Note The Windows login screens shown above appear on computers running Windows 95, 98, and Me (Figure 6-1) and Windows 2000 (Figure 6-2), respectively. The login screen looks slightly different on computers running Windows NT and XP.

The "LEAP Authentication in progress" message appears.

Step 2 If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows "LEAP Authenticated."

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the "Error Messages" section in Chapter 9 for the necessary action to take.

Step 3 Windows continues to log you onto the system.

After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

Note If your computer is running Windows NT, 2000, or XP and you change your Windows password using the standard Windows Change Password function, the client will update the LEAP password automatically and maintain its connection to the access point if the current profile uses the Windows username and password. If your computer is running Windows 95, 98, or Me and you change your Windows password, the client will lose association from the access point, and you will be prompted to enter your new credentials.

Step 1 Click **OK** when the following message appears: "The user name and password entered for profile '*xxx*' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password."

Step 2 When the Windows login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.

Note If you click Cancel rather than OK on the Windows login screen, the following message appears: "The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?" If you click No, the Windows login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being "Disabled."

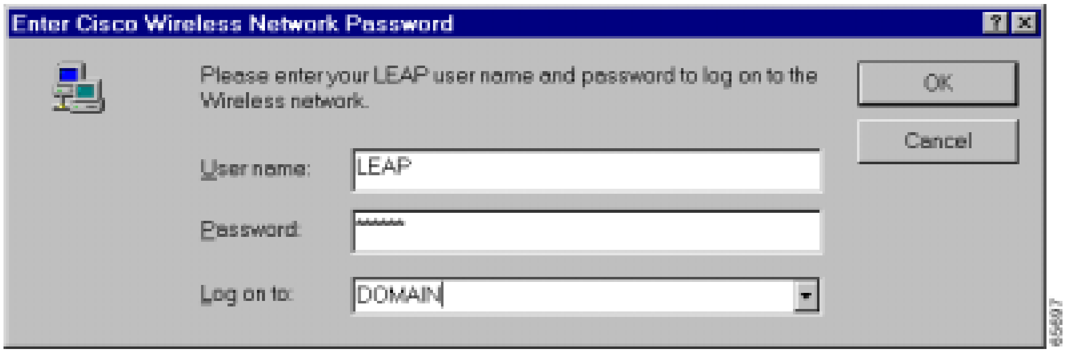
Using LEAP with an Automatically Prompted Login

After Profile Selection/Card Insertion

After you (or auto profile selection) select a profile that uses LEAP authentication but specifies that you be automatically prompted to enter a separate LEAP username and password or you eject and reinsert the client adapter while this profile is selected, follow the steps below to LEAP authenticate.

Step 1 When the LEAP login screen appears (see Figure 6-3), enter your LEAP username and password and click **OK**. The domain name is optional.

Figure 6-3 LEAP Login Screen



Enter Cisco Wireless Network Password

Please enter your LEAP user name and password to log on to the Wireless network.

User name: LEAP

Password: ******

Log on to: DOMAIN

Note The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

Step 2 If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

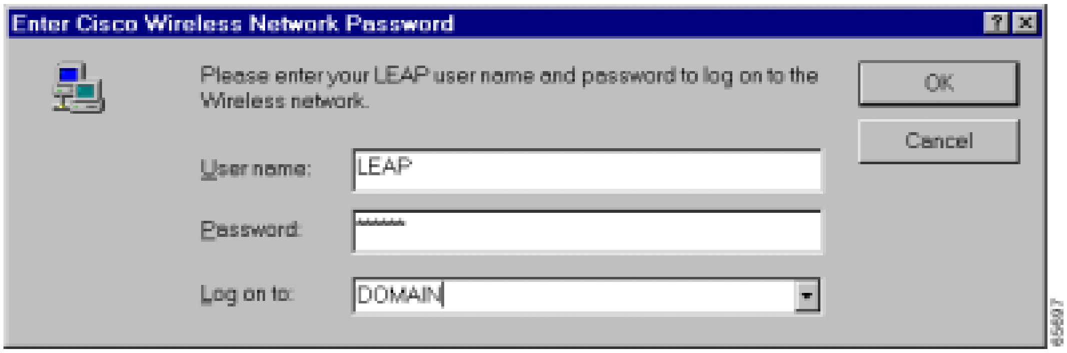
If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in Chapter 9 for the necessary action to take.

After a Reboot/Logoff

After your computer reboots or you log off, follow the steps below to LEAP authenticate.

Step 1 When the LEAP login screen appears (see Figure 6-4), enter your LEAP username and password and click **OK**. The domain name is optional.

Figure 6-4 LEAP Login Screen


Enter Cisco Wireless Network Password

Please enter your LEAP user name and password to log on to the Wireless network.

User name: LEAP

Password: ******

Log on to: DOMAIN

Note The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

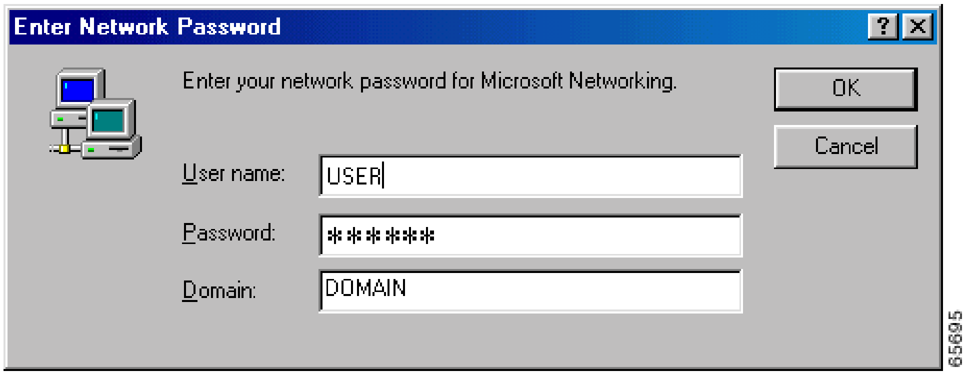
Step 2 If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in Chapter 9 for the necessary action to take.

Step 3 When the network login screen appears (see Figure 6-5 and Figure 6-6), enter your network username and password and click **OK**.

Note Figure 6-5 shows an example network login screen that may appear on computers running Windows 95, 98, and Me. Your screen may look different. Figure 6-6 shows the network login screen that appears on Windows 2000 systems. The login screen looks slightly different on computers running Windows NT and XP.

Figure 6-5 Network Login Screen (Windows 95, 98, and Me)


Enter Network Password

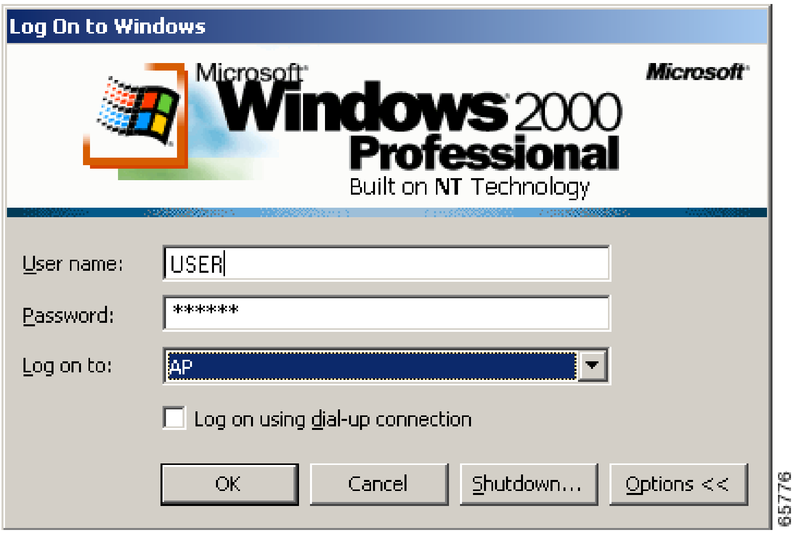
Enter your network password for Microsoft Networking.

User name: USER

Password: *******

Domain: DOMAIN

Figure 6-6 Network Login Screen (Windows 2000)


Log On to Windows

User name: USER

Password: *******

Log on to: AP

After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

Step 1 Click **OK** when the following message appears: “The user name and password entered for profile '*xxx*' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password.”

Step 2 When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.

Note If you click Cancel rather than OK on the LEAP login screen, the following message appears: “The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?” If you click No, the LEAP login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being “Disabled.”

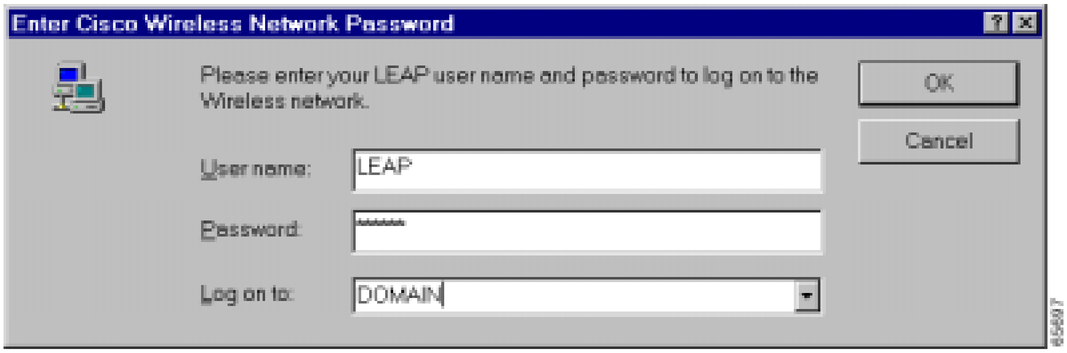
Using LEAP with a Manually Prompted Login

After Profile Selection

After you (or auto profile selection) select a profile that uses LEAP authentication but specifies that the process be manually invoked, follow the steps below to LEAP authenticate.

Step 1 When the LEAP login screen appears (see Figure 6-7), enter your LEAP username and password and click **OK**. The domain name is optional.

Figure 6-7 LEAP Login Screen



Enter Cisco Wireless Network Password

Please enter your LEAP user name and password to log on to the Wireless network.

User name: LEAP

Password: ******

Log on to: DOMAIN

Note The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

Step 2 If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in Chapter 9 for the necessary action to take.

After a Reboot/Logoff/Card Insertion

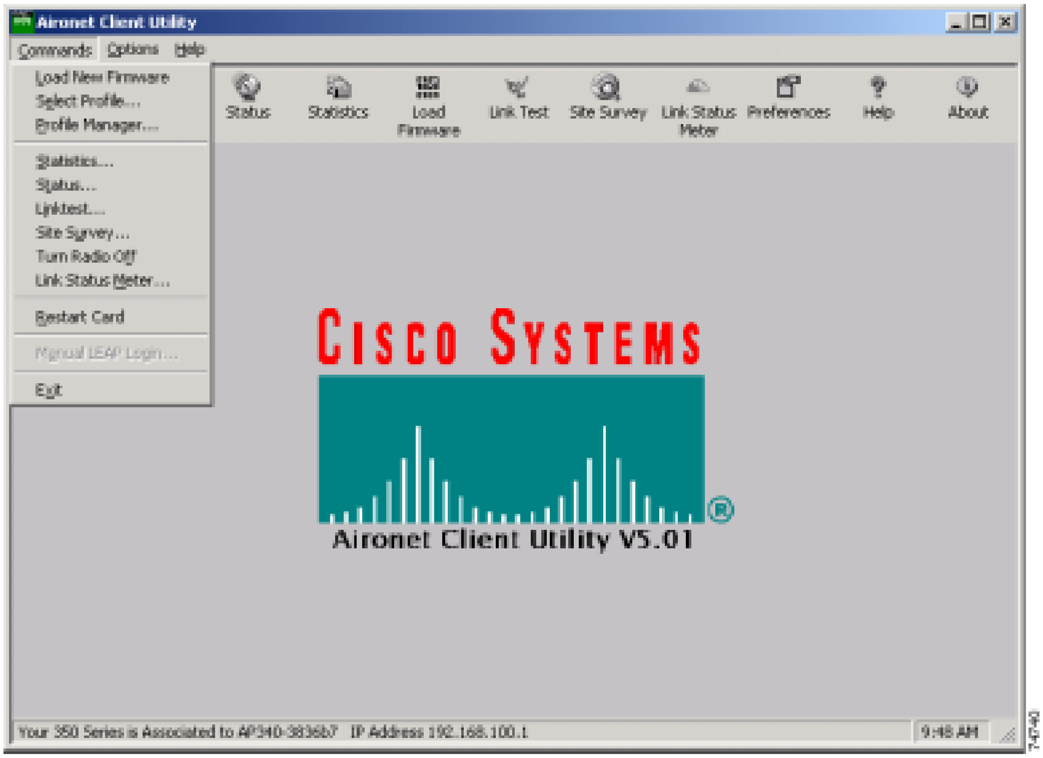
After your computer reboots, you log off, or you eject and reinsert the client adapter, the adapter does not automatically attempt to authenticate. You must manually invoke the authentication process. To do so, follow the steps below.

Step 1 If you rebooted your computer or logged off, complete your standard Windows login.

Step 2 Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU.

Step 3 Select the **Manual LEAP Login** option from the Commands drop-down menu (see Figure 6-8).

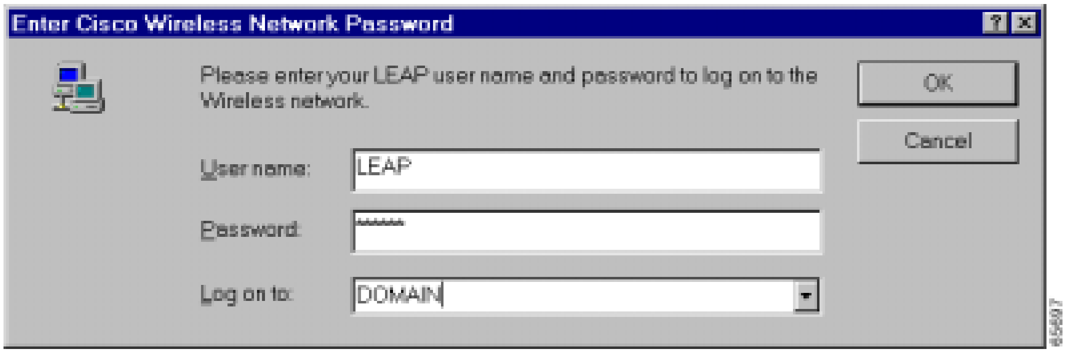
Figure 6-8 Commands Drop-Down Menu



Your 350 Series is Associated to AP340-3836b7 IP Address 192.168.100.1

Step 4 When the LEAP login screen appears (see Figure 6-9), enter your LEAP username and password and click **OK**. The domain name is optional.

Figure 6-9 LEAP Login Screen



Please enter your LEAP user name and password to log on to the Wireless network.

User name: LEAP

Password: ******

Log on to: DOMAIN

Note The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The "LEAP Authentication in progress" message appears.

Step 5 If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows "LEAP Authenticated."

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the "Error Messages" section in Chapter 9 for the necessary action to take.

After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

Step 1 Click **OK** when the following message appears: "The user name and password entered for profile '*xxx*' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password."

Step 2 When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.

Note If you click Cancel rather than OK on the LEAP login screen, the following message appears: "The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?" If you click No, the LEAP login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being "Disabled."

Using LEAP with a Saved Username and Password

After Profile Selection/Card Insertion

After you (or auto profile selection) select a profile that uses LEAP authentication with a saved LEAP username and password or you eject and reinsert the client adapter while this profile is selected, the following events occur:

1. The "LEAP Authentication in progress" message appears.
2. If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows "LEAP Authenticated."

   If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the "Error Messages" section in Chapter 9 for the necessary action to take.

After a Reboot/Logoff

After your computer reboots or you log off, the following events occur:

1. After you enter your Windows username and password, the LEAP authentication process begins automatically using your saved LEAP username and password.
2. If your client adapter authenticates, the “LEAP Authentication in progress” message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

   If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in Chapter 9 for the necessary action to take.
3. Windows continues to log you onto the system.

After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

Step 1 Click **OK** when the following message appears: “The user name and password entered for saved profile '*xxx*' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password. Please also remember to change them permanently in the saved profile using the ACU Profile Manager.”

Step 2 When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.

Note If you click Cancel rather than OK on the LEAP login screen, the following message appears: “The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?” If you click No, the LEAP login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being “Disabled.”

Step 3 Edit the profile in ACU by changing the saved username and password on the LEAP Settings screen.

Step 4 Save the changes to your profile.

Using Host-Based EAP

After Profile Selection/Card Insertion

After you (or auto profile selection) select a profile that uses host-based EAP authentication or you eject and reinsert the client adapter while this profile is selected, follow the steps below for either EAP-TLS or EAP-MD5 to EAP authenticate.

EAP-TLS

Step 1 If a pop-up message appears above the Windows system tray informing you that you need to accept a certificate to begin the EAP authentication process, click the message and follow the instructions provided to accept the certificate.

Note You should not have to accept a certificate for future authentication attempts. The same certificate, which is tied to your standard Windows network login, will be used.

Step 2 The client adapter should now EAP authenticate. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, “Authentication succeeded.” The status line also indicates if the authentication attempt fails.

EAP-MD5

Step 1 When a pop-up message appears above the Windows system tray informing you that you need to enter your credentials to access the network, click the message. The Wireless Network Connection screen appears.

Step 2 Enter your EAP-MD5 authentication username, password, and optional domain name (which are registered with the RADIUS server) and click **OK**.

Step 3 The client adapter should now EAP authenticate. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, “Authentication succeeded.” The status line also indicates if the authentication attempt fails.

After a Reboot/Logoff

EAP-TLS

After your computer reboots or you log off and you enter your Windows username and password, the EAP authentication process begins automatically and the client adapter should EAP authenticate.

To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status is displayed to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, “Authentication succeeded.” The status line also indicates if the authentication attempt fails.

EAP-MD5

After your computer reboots or you log off and you enter your Windows username and password, follow the steps below to EAP authenticate.

Step 1 When a pop-up message appears above the Windows system tray informing you that you need to enter your credentials to access the network, click the message. The Wireless Network Connection screen appears.

Step 2 Enter your EAP-MD5 authentication username, password, and optional domain name (which are registered with the RADIUS server) and click **OK**.

Step 3 The client adapter should now EAP authenticate. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, “Authentication succeeded.” The status line also indicates if the authentication attempt fails.

Performing Diagnostics

This chapter explains how to use ACU to perform user-level diagnostics.

The following topics are covered in this chapter:

Overview of ACU Diagnostic Tools

In addition to enabling you to configure your client adapter for use in various types of networks, ACU provides tools that enable you to assess the performance of the client adapter and other devices on the wireless network. ACU diagnostic tools perform the following functions:

- Display your client adapter's current status and configured settings
- Display statistics pertaining to your client adapter's transmission and reception of data
- Display a graphical image of your client adapter's RF link
- Run an RF link test to assess the performance of the RF link between your client adapter and its associated access point

Table 7-1 enables you to quickly locate the instructions for using each of the diagnostic tools.

Table 7-1 Locating Diagnostic Instructions

Diagnostic Tool	Page Number
Status	7-4
Statistics	7-12
Link status meter	7-16
RF link test	7-18

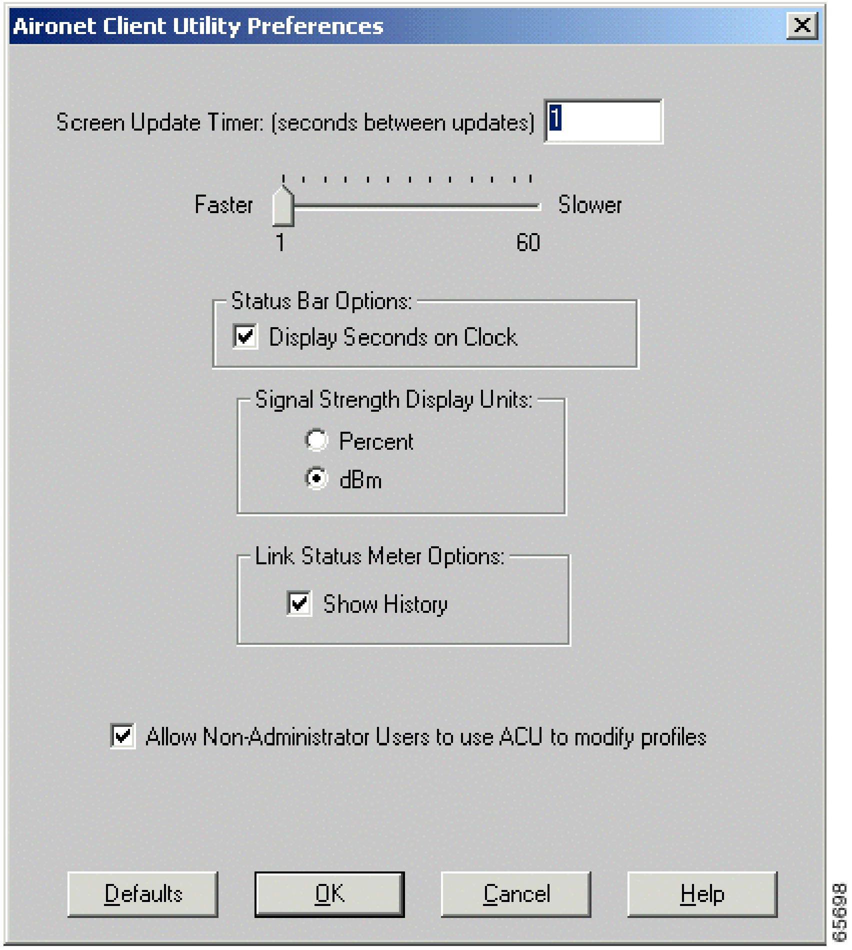
Setting Parameters that Affect ACU Diagnostic Tools

Several parameters affect the operation of ACU diagnostic tools. Follow the steps below to set these parameters.

Step 1 Double-click the **Aironet Client Utility** (**ACU)** icon on your desktop to open ACU.

Step 2 Click the **Preferences** icon or select **Preferences** from the Options drop-down menu. The Aironet Client Utility Preferences screen appears (see Figure 7-1).

Figure 7-1 Aironet Client Utility Preferences Screen



Aironet Client Utility Preferences

Screen Update Timer: (seconds between updates) 1

Faster 1 — 60 Slower

Status Bar Options:
☑ Display Seconds on Clock

Signal Strength Display Units:
○ Percent
● dBm

Link Status Meter Options:
☑ Show History

☑ Allow Non-Administrator Users to use ACU to modify profiles

Step 3 Table 7-2 lists and describes the parameters that affect the operation of ACU diagnostic tools. Follow the instructions in the table to change any parameters.

Table 7-2 Parameters Affecting ACU Diagnostic Tools

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Screen Update Timer (seconds between updates)</td><td>Specifies how often the Status and Statistics screens are updated. You can type a number in the edit box or use the slider to change this value.
<b>Range:</b> 1 to 60 seconds between updates (in 1-second increments)
<b>Default:</b> 1 second between updates</td></tr>
<tr><td>Signal Strength Display Units</td><td>Specifies the units used to display signal strength on the Status, Linktest, and Site Survey screens.
<b>Default:</b> Percent
<table>
<tr><th>Units</th><th>Description</th></tr>
<tr><td>Percent</td><td>Displays the signal strength as a percentage.</td></tr>
<tr><td>dBm</td><td>Displays the signal strength in decibels with respect to milliwatts.</td></tr>
</table>
<b>Note</b> dBm can be selected only if your client adapter is using PCM/LMC/PCI card firmware version 3.92 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater.</td></tr>
<tr><td>Show History</td><td>Selecting this checkbox causes the Link Status Meter graphical display to show a recent history of the RF performance between your client adapter and its associated access point. Black dots on the graphical display show the performance of the last 50 signals.
<b>Default:</b> Selected</td></tr>
</table>

Step 4 Click **OK** to save your changes.

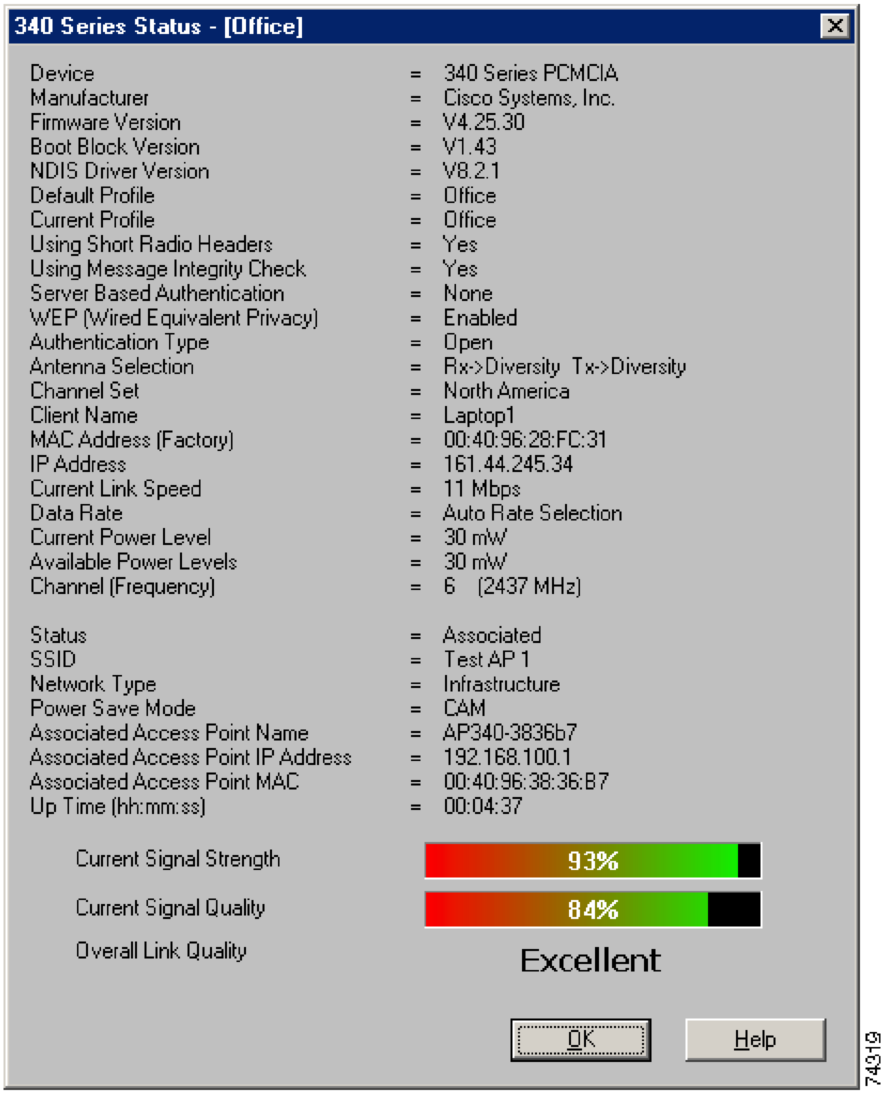
Viewing the Current Status of Your Client Adapter

ACU enables you to view the current status of your client adapter as well as many of the settings that have been configured for the adapter.

To view your client adapter's status and settings, open ACU; then click the **Status** icon or select **Status** from the Commands drop-down menu. The Status screen appears. Figure 7-2 shows the Status screen with the signal strength values displayed as percentages, and Figure 7-3 shows the bottom of the same screen with the signal strength values displayed in decibels with respect to milliwatts (dBm).

Note The name of the current profile appears in parentheses at the top of the screen.

Figure 7-2 Status Screen (with Signal Strength as a Percentage)



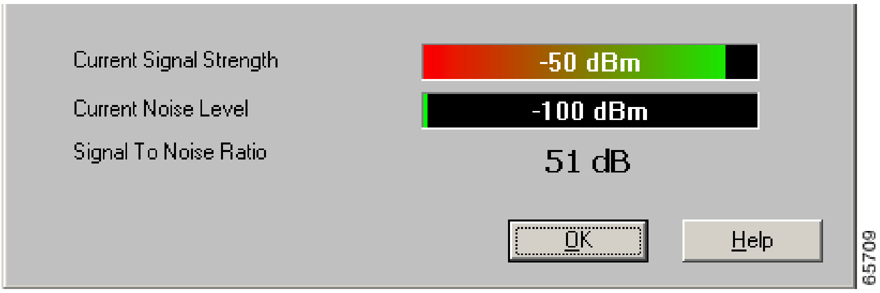
340 Series Status - [Office]

Device = 340 Series PCMCIA
Manufacturer = Cisco Systems, Inc.
Firmware Version = V4.25.30
Boot Block Version = V1.43
NDIS Driver Version = V8.2.1
Default Profile = Office
Current Profile = Office
Using Short Radio Headers = Yes
Using Message Integrity Check = Yes
Server Based Authentication = None
WEP (Wired Equivalent Privacy) = Enabled
Authentication Type = Open
Antenna Selection = Rx->Diversity Tx->Diversity
Channel Set = North America
Client Name = Laptop1
MAC Address (Factory) = 00:40:96:28:FC:31
IP Address = 161.44.245.34
Current Link Speed = 11 Mbps
Data Rate = Auto Rate Selection
Current Power Level = 30 mW
Available Power Levels = 30 mW
Channel (Frequency) = 6 (2437 MHz)

Status = Associated
SSID = Test AP 1
Network Type = Infrastructure
Power Save Mode = CAM
Associated Access Point Name = AP340-3836b7
Associated Access Point IP Address = 192.168.100.1
Associated Access Point MAC = 00:40:96:38:36:B7
Up Time (hh:mm:ss) = 00:04:37

Current Signal Strength 93%
Current Signal Quality 84%
Overall Link Quality Excellent

Figure 7-3 Bottom of Status Screen (with Signal Strength in dBm)



Current Signal Strength -50 dBm
Current Noise Level -100 dBm
Signal To Noise Ratio 51 dB

Table 7-3 interprets each element of the Status screen.

Table 7-3 Client Adapter Status

Status	Description
Device	A description of your client adapter.
Manufacturer	The manufacturer of your client adapter.
Firmware Version	The version of the firmware that is currently running on your client adapter.
Boot Block Version	The version of the boot block firmware that is currently in your client adapter. The boot block firmware contains identification information for the client adapter and functions to start up the radio and pass control to the main firmware, which (unlike the boot block) can be modified and upgraded by the user.
NDIS Driver Version	The version of the NDIS device driver that is currently installed on your computer.
Default Profile	The network configuration (or profile) shown in the Use Selected Profile drop-down box on the Profile Manager screen, if your driver supports auto profile selection. This is the profile that you have selected as the active profile. **Note** The current profile may be different than the default profile if you are using auto profile selection. The client adapter will not switch profiles as long as it remains associated to the access point or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value if LEAP is enabled). Refer to Chapter 4 for information on creating and using profiles. **Note** Auto profile selection is supported in PCM/LMC/PCI card driver version 8.01 and greater (or mini PCI/PC-Cardbus card driver version 2.20 and greater).
Current Profile	The network configuration (or profile) your client adapter is currently using, if your driver supports auto profile selection. **Note** The current profile may be different than the default profile if you are using auto profile selection. The client adapter does not switch profiles as long as it remains associated to the access point or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value if LEAP is enabled). Refer to Chapter 4 for information on creating and using profiles. **Note** If your current profile becomes disabled due to an invalid LEAP username and password, this field lists the profile as (Disabled). **Note** Auto profile selection is supported in PCM/LMC/PCI card driver version 8.01 and greater (or mini PCI/PC-Cardbus card driver version 2.20 and greater).

Table 7-3 Client Adapter Status (continued)

<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>Using Short Radio Headers</td><td>Indicates whether your client adapter is actually using short radio headers.
<b>Value:</b> Yes or No
<b>Note</b> This setting appears only for 2.4-GHz client adapters.
<b>Note</b> Refer to the Use Short Radio Headers parameter in Table 5-3 for information on using short radio headers.</td></tr>
<tr><td>Using Message Integrity Check</td><td>Indicates whether your client adapter is using message integrity check (MIC) to protect packets sent to and received from the access point.
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. Client adapters using PCM/LMC/PCI card driver version 8.01 or greater and PCM/LMC/PCI card firmware version 4.25.23 or greater (or mini PCI/PC-Cardbus card driver version 2.20 or greater and mini PCI/PC-Cardbus card firmware version 5.0 or greater) support MIC; however, MIC can be used only if it is also enabled on the access point.
<b>Note</b> If the access point is using MIC, your client adapter's driver must support MIC; otherwise, the client will not be able to associate.
<b>Value:</b> Yes or No</td></tr>
<tr><td>Server Based Authentication</td><td>Indicates the configuration of the access point to which your client adapter is associated.
<b>Value:</b> None, WEP Key In Use, Cell Is Secure, or LEAP Authenticated
<table>
<tr><th>Server Based Authentication</th><th>Description</th></tr>
<tr><td>None</td><td>The access point is configured for No Encryption.</td></tr>
<tr><td>WEP Key In Use</td><td>The access point is configured for Optional encryption.</td></tr>
<tr><td>Cell Is Secure</td><td>The access point is configured for Full Encryption.
<b>Note</b> If the client's current profile does not have Allow Association To Mixed Cells enabled, the client can associate only to access points that use full encryption.</td></tr>
<tr><td>LEAP Authenticated</td><td>The client is using LEAP and is authenticated to an access point that has WEP and Network-EAP enabled.</td></tr>
</table></td></tr>
</table>

Table 7-3 Client Adapter Status (continued)

Status	Description
WEP (Wired Equivalent Privacy)	Your client adapter's current WEP status. **Value:** Enabled, Not Enabled, or Need Firmware Upgrade **Note** Refer to the "Setting Network Security Parameters" section on page 5-20 for information on enabling WEP.
Authentication Type	Indicates whether the client adapter must share the same WEP keys as the access point in order to communicate or can communicate with the access point regardless of its WEP settings. **Value:** Open or Shared Key **Note** Refer to the "Setting Network Security Parameters" section on page 5-20 for information on setting the authentication type.
Antenna Selection	The antenna mode that your client adapter is currently using. **Value:** Diversity, Primary Only, Secondary Only (Primary Only is the only option available for PCI client adapters) **Note** This setting appears only for 2.4-GHz client adapters. **Note** The Primary Only and Secondary Only values were formerly named Right Only and Left Only, respectively. Refer to the Antenna Mode (Receive) and Antenna Mode (Transmit) parameters in Table 5-4 and Table 5-5 for information on setting the antenna mode.
Channel Set	The regulatory domain for which your client adapter is currently configured, such as Americas. (For the Japan channel set, the Call ID is also displayed.) This value is not user selectable. **Note** Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.
Client Name	The name your client adapter uses when it associates to an access point. **Note** Refer to the Client Name parameter in Table 5-2 for information on setting the client name.
MAC Address	The MAC address assigned to your client adapter at the factory.
IP Address	The IP address of your client adapter.
Current Link Speed	The rate at which your client adapter is currently transmitting data packets. **Value:** 1, 2, 5.5, or 11 Mbps (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)

Table 7-3 Client Adapter Status (continued)

Status	Description
Data Rate	The rate at which your client adapter has been configured to transmit or receive data packets. **Value:** 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, or Auto Rate Selection (2.4-GHz client adapters); 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, or Auto Rate Selection (5-GHz client adapters) **Note** Refer to the Data Rate parameter in Table 5-3 for information on setting the client adapter's data rate.
Current Power Level	The power level at which your client adapter is currently transmitting. The maximum level is dependent upon the radio installed in your client adapter and your country's regulatory agency. **Value:** 1, 5, 20, 30, 50, or 100 mW (350 series client adapters); 1, 5, 15, or 30 mW (340 series client adapters); 5, 10, or 20 mW (5-GHz client adapters) **Note** Refer to the Transmit Power parameter in Table 5-3 for information on setting the client adapter's power level.
Available Power Levels	The power levels at which your client adapter is capable of transmitting. The maximum level is dependent upon the radio installed in your client adapter and your country's regulatory agency. **Value:** 1, 5, 15, 20, 30, 50, or 100 mW (350 series client adapters); 1, 5, 15, or 30 mW (340 series client adapters); 5, 10, or 20 mW (5-GHz client adapters) **Note** Refer to the Transmit Power parameter in Table 5-3 for information on the client adapter's available power levels.
Channel (Frequency)	The frequency that your client adapter is currently using as the channel for communications. **Value:** Dependent on client adapter radio and regulatory domain **Note** Refer to the Channel parameter in Table 5-3 for information on selecting the frequency for your client adapter.
Status	The operational mode of your client adapter. **Value:** Error, Configured, Associated, Not Associated, or Ad Hoc Mode
SSID	The SSID that your client adapter is currently using. **Note** Refer to the SSID1 parameter in Table 5-2 for information on the client adapter's SSID.
Network Type	The type of network in which your client adapter is being used. **Value:** Infrastructure or Ad Hoc **Note** Refer to the Network Type parameter in Table 5-2 for information on setting the network type.

Table 7-3 Client Adapter Status (continued)

Status	Description
Power Save Mode	The client adapter's current power consumption setting. **Value:** CAM, Max PSP, or Fast PSP **Note** Refer to the Power Save Mode parameter in Table 5-2 for information on setting the client adapter's power save mode.
Associated Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the access point was configured with a name and the client adapter is in infrastructure mode.
Associated Access Point IP Address	The IP address of the access point to which your client adapter is associated. It is shown only if the access point was configured with an IP address and the client adapter is in infrastructure mode.
Associated Access Point MAC Address	The MAC address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode.
Beacon Period	Specifies the duration between beacon packets, which are used to help clients find each other in ad hoc mode. **Range:** Approximately 20 to 999 milliseconds (ms) **Note** The beacon period is shown only if your client adapter is in ad hoc mode.
Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) that the client adapter has been receiving power. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
Current 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. **Range:** 0 to 100% or –95 to –45 dBm
Current Signal Quality (2.4-GHz client adapters)	The signal quality for all received packets. The higher the value and the more green the bar graph is, the better the quality of the signal. **Range:** 0 to 100% **Note** This setting appears only for 2.4-GHz client adapters and only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.

Table 7-3 Client Adapter Status (continued)

Status	Description
Current Beacons Received (5-GHz client adapters)	The percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph is, the clearer the signal. **Example:** The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%. **Range:** 0 to 100% **Note** This setting appears only for 5-GHz client adapters (or for 2.4-GHz client adapters using firmware version less than 4.05) and only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.
Current Noise Level	The level of background radio frequency energy in the 2.4- or 5-GHz band. The lower the value and the more green the bar graph is, the less background noise present. **Range:** –100 to –45 dBm **Note** This setting appears only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in Table 7-2 for information.
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 **Note** This setting appears only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.
Signal To Noise Ratio	The difference between the signal strength and the current noise level. The higher the value, the better the client adapter's ability to communicate with the access point. **Range:** 0 to 90 dB **Note** This setting appears only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in Table 7-2 for information.

Viewing Statistics for Your Client Adapter

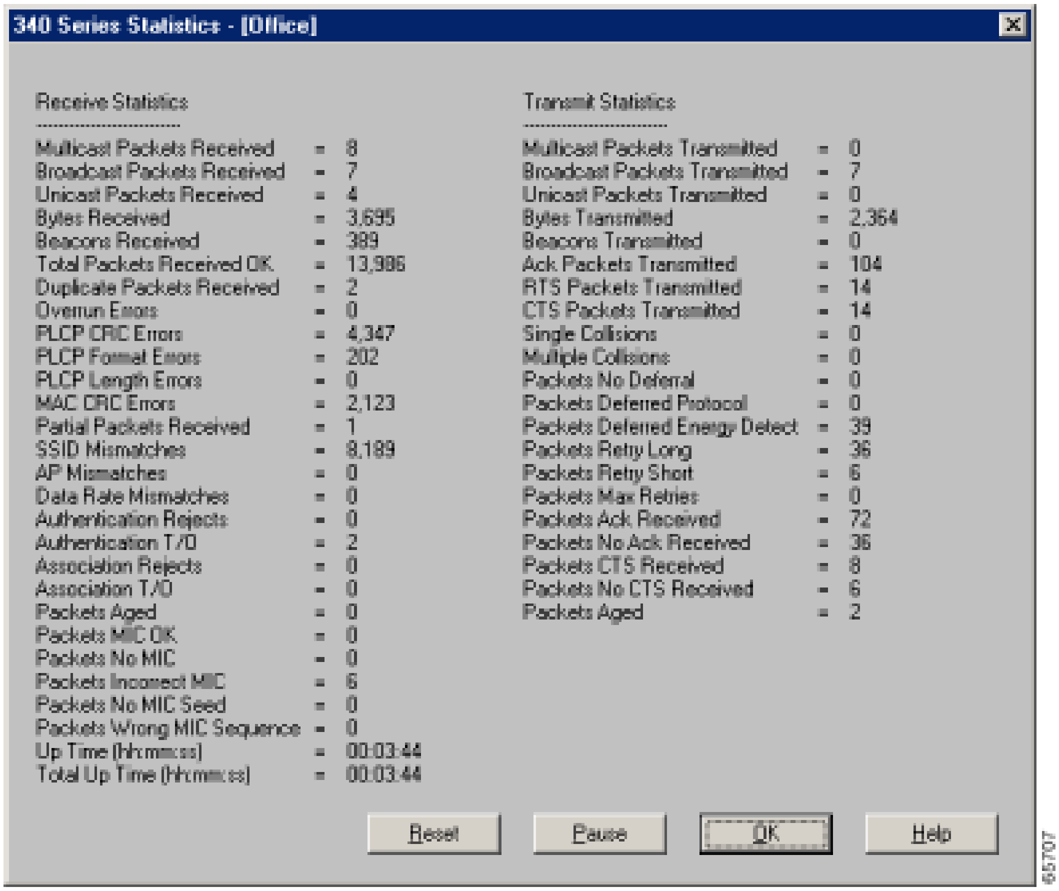
ACU enables you to view statistics that indicate how data is being received and transmitted by your client adapter.

To view your client adapter's statistics, open ACU; then click the **Statistics** icon or select **Statistics** from the Commands drop-down menu. The Statistics screen appears (see Figure 7-4).

Note The name of the current profile appears in parentheses at the top of the screen.

Note The receive and transmit statistics are host statistics. That is, they show packets and errors received or sent by the Windows device. Link status tests from the access point or site survey tool are performed at the firmware level; therefore, they have no effect on the statistics shown in the Statistics screen.

Figure 7-4 Statistics Screen



```
Receive Statistics                            Transmit Statistics
-------------------------                     -------------------------
Multicast Packets Received    =  8            Multicast Packets Transmitted    =  0
Broadcast Packets Received    =  7            Broadcast Packets Transmitted    =  7
Unicast Packets Received      =  4            Unicast Packets Transmitted      =  0
Bytes Received                =  3,695        Bytes Transmitted                =  2,364
Beacons Received              =  389          Beacons Transmitted              =  0
Total Packets Received OK     =  13,986       Ack Packets Transmitted          =  104
Duplicate Packets Received    =  2            RTS Packets Transmitted          =  14
Overrun Errors                =  0            CTS Packets Transmitted          =  14
PLCP CRC Errors               =  4,347        Single Collisions                =  0
PLCP Format Errors            =  202          Multiple Collisions              =  0
PLCP Length Errors            =  0            Packets No Deferral              =  0
MAC CRC Errors                =  2,123        Packets Deferred Protocol        =  0
Partial Packets Received      =  1            Packets Deferred Energy Detect   =  39
SSID Mismatches               =  8,189        Packets Retry Long               =  36
AP Mismatches                 =  0            Packets Retry Short              =  6
Data Rate Mismatches          =  0            Packets Max Retries              =  0
Authentication Rejects        =  0            Packets Ack Received             =  72
Authentication T/O            =  2            Packets No Ack Received          =  36
Association Rejects           =  0            Packets CTS Received             =  8
Association T/O               =  0            Packets No CTS Received          =  6
Packets Aged                  =  0            Packets Aged                     =  2
Packets MIC OK                =  0
Packets No MIC                =  0
Packets Incorrect MIC         =  6
Packets No MIC Seed           =  0
Packets Wrong MIC Sequence    =  0
Up Time (hh:mm:ss)            =  00:03:44
Total Up Time (hh:mm:ss)      =  00:03:44
```

The statistics are calculated as soon as your client adapter is started or the Reset button is selected and are continually updated at the rate specified by the Screen Update Timer. Instructions for changing the Screen Update Timer setting are provided in Table 7-2.

Table 7-4 describes each statistic that is displayed for your client adapter.

Table 7-4 Client Adapter Statistics

Statistic	Description
Receive Statistics	
Multicast Packets Received	The number of multicast packets that were received successfully.
Broadcast Packets Received	The number of broadcast packets that were received successfully.
Unicast Packets Received	The number of unicast packets that were received successfully.
Bytes Received	The number of bytes of data that were received successfully.
Beacons Received	The number of beacon packets that were received successfully.
Total Packets Received OK	The number of all packets that were received successfully.
Duplicate Packets Received	The number of duplicate packets that were received successfully.
Overrun Errors	The number of packets received when no receive buffers were available. These errors usually occur when the host does not read the received packets from the client adapter fast enough.
PLCP CRC Errors	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. **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.
PLCP Format Errors	The number of times an 802.11 PLCP header was received with a valid CRC but the rest of the packet was ignored due to an unknown value in the header.
PLCP Length Errors	The number of times an 802.11 PLCP header was received but the rest of the packet was ignored due to an illegal header length.
MAC CRC Errors	The number of packets that had a valid 802.11 PLCP header but contained a CRC error in the data portion of the packet. **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.
Partial Packets Received	The number of fragments that were discarded because the entire packet was not received successfully.
SSID Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the adapter's SSID was not the same as the access point's.

Table 7-4 Client Adapter Statistics (continued)

Statistic	Description
AP Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the access point was not the adapter's specified access point. **Note** Refer to the Specified Access Point 1- 4 parameter in Table 5-4 for information on specifying access points.
Data Rate Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the adapter's data rate was not supported by the access point. **Note** Refer to the Data Rate parameter in Table 5-3 for information on supported data rates.
Authentication Rejects	The number of times the client adapter tried to authenticate to an access point but was rejected.
Authentication T/O	The number of times the client adapter tried to authenticate to an access point but was unable to because the access point did not respond fast enough (timed out).
Association Rejects	The number of times the client adapter tried to associate to an access point but was rejected.
Association T/O	The number of times the client adapter tried to associate to an access point but was unable to because the access point did not respond fast enough (timed out).
Packets Aged	The number of packets received successfully but discarded by the client adapter because either all fragments were not received within 10 seconds or the host did not read the packet from the adapter within 10 seconds.
Packets MIC OK	The number of packets that were received successfully with a valid message integrity check (MIC). **Note** This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Packets No MIC	The number of packets that were discarded due to no MIC being found. **Note** This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Packets Incorrect MIC	The number of packets that were discarded due to an incorrect MIC value. **Note** This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.

Table 7-4 Client Adapter Statistics (continued)

Statistic	Description
Packets No MIC Seed	The number of packets that were discarded due to no MIC seed being received. **Note** This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Packets Wrong MIC Sequence	The number of packets that were discarded due to the MIC sequence number being wrong. **Note** This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) since the Reset button was selected. If the client adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
Total Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) that the client adapter has been receiving power. The total up time continues to increment even if the Reset button is selected. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
Transmit Statistics	
Multicast Packets Transmitted	The number of multicast packets that were transmitted successfully.
Broadcast Packets Transmitted	The number of broadcast packets that were transmitted successfully.
Unicast Packets Transmitted	The number of unicast packets that were transmitted successfully.
Bytes Transmitted	The number of bytes of data that were transmitted successfully.
Beacons Transmitted	The number of beacon packets that were transmitted successfully (in ad hoc mode only).
Ack Packets Transmitted	The number of acknowledgment (Ack) packets that were transmitted in response to successfully received unicast packets.
RTS Packets Transmitted	The number of request-to-send (RTS) packets that were transmitted successfully.
CTS Packets Transmitted	The number of clear-to-send (CTS) packets that were transmitted in response to a successfully received RTS packet.
Single Collisions	The number of packets that had to be retransmitted once due to a collision.
Multiple Collisions	The number of packets that had to be retransmitted more than once due to additional collisions.
Packets No Deferral	The number of packets that were able to be transmitted immediately without being delayed due to energy detect or protocol deferral.
Packets Deferred Protocol	The number of packets that were delayed due to 802.11 protocol reasons (such as not enough time left to send the packet).

Table 7-4 Client Adapter Statistics (continued)

Statistic	Description
Packets Deferred Energy Detect	The number of packets that were delayed because RF energy was already detected. This condition is usually caused by another radio transmitting a packet or by some other RF source jamming the signal (such as a microwave oven).
Packets Retry Long	The number of normal data packets that were retransmitted.
Packets Retry Short	The number of request-to-send (RTS) packets that were retransmitted.
Packets Max Retries	The number of packets that failed to be transmitted successfully after exhausting the maximum number of retries.
Packets Ack Received	The number of transmitted packets that had their corresponding acknowledgment (Ack) packet received successfully.
Packets No Ack Received	The number of transmitted packets that did not have their corresponding Ack packet received successfully.
Packets CTS Received	The number of clear-to-send (CTS) packets that were received in response to an RTS packet.
Packets No CTS Received	The number of packets for which no CTS packet was received in response to an RTS packet.
Packets Aged	The number of packets that were discarded by the client adapter because they were not transmitted successfully within 5 seconds.

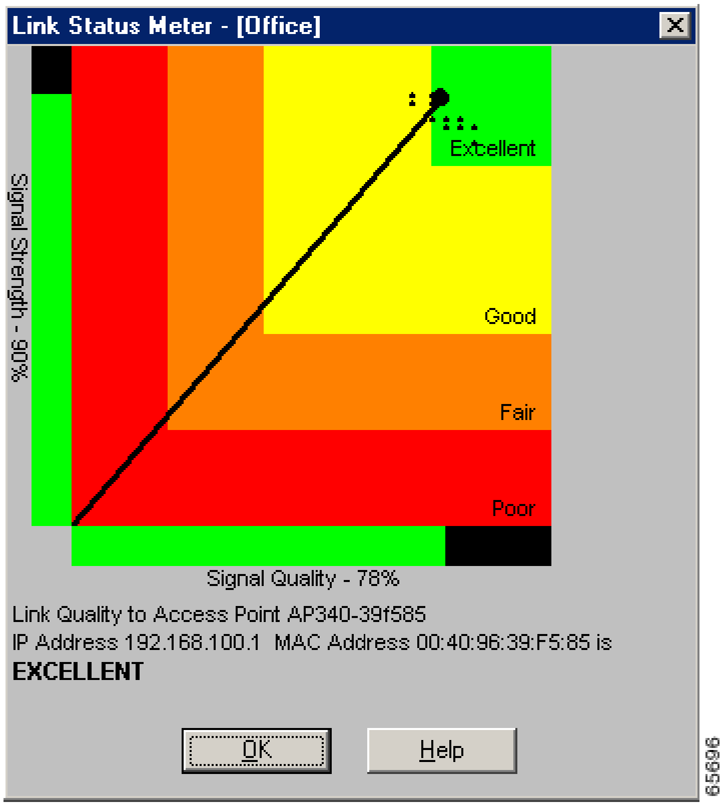
Viewing the Link Status Meter

ACU's link status meter can be used to assess the performance of your client adapter's RF link. If this tool is used to assess the RF link at various locations, you can avoid areas where performance is weak and eliminate the risk of losing the connection between your client adapter and an access point.

To open the link status meter, open ACU; then click the **Link Status Meter** icon or select **Link Status Meter** from the Commands drop-down menu. The Link Status Meter screen appears (see Figure 7-5).

Note The name of the current profile appears in parentheses at the top of the screen.

Figure 7-5 Link Status Meter Screen


Link Status Meter - [Office]

Link Quality to Access Point AP340-39f585
IP Address 192.168.100.1 MAC Address 00:40:96:39:F5:85 is
EXCELLENT

The Link Status Meter screen provides a graphical display of the following:

- **Signal strength** – The strength of the client adapter's radio signal at the time packets are being received. It is displayed as a percentage along the vertical axis.
- **Signal quality** – The quality of the client adapter's radio signal at the time packets are being received. It is displayed as a percentage along the horizontal axis.

The combined result of the signal strength and signal quality is represented by a diagonal line (see Figure 7-5). Where the line falls on the graphical display determines whether the RF link between your client adapter and its associated access point is poor, fair, good, or excellent. The access point that is associated to your client adapter and its MAC address are indicated at the bottom of the display.

Note ACU's Status screen also shows signal strength and signal quality. However on the Status screen, these data are represented by histograms.

If you want to see a recent history of the RF performance between your client adapter and its associated access point, select the **Show History** checkbox on the Aironet Client Utility Preferences screen. Black dots on the graphical display show the performance of the last 50 signals.

Running an RF Link Test

ACU's link test tool sends out pings to assess the performance of the RF link. The test is designed to be performed multiple times at various locations throughout your area and is run at the data rate set on ACU's RF Network Properties screen (see the Data Rate parameter in Table 5-3). The results of the link test can be used to determine RF network coverage and ultimately the required number and placement of access points in your network. The test also helps you to avoid areas where performance is weak, thereby eliminating the risk of losing the connection between your client adapter and its associated access point.

Because the link test operates above the RF level, it does more than test the RF link between two network devices. It also checks the status of wired sections of the network and verifies that TCP/IP and the proper drivers have been loaded.

Note A link test can also be run from an access point through a Telnet session. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for information.

The following prerequisites are required before you can run an RF link test:

- The TCP/IP protocol must be installed on your system.

  Note See the Help section of your Windows operating system for information on installing and setting up TCP/IP.

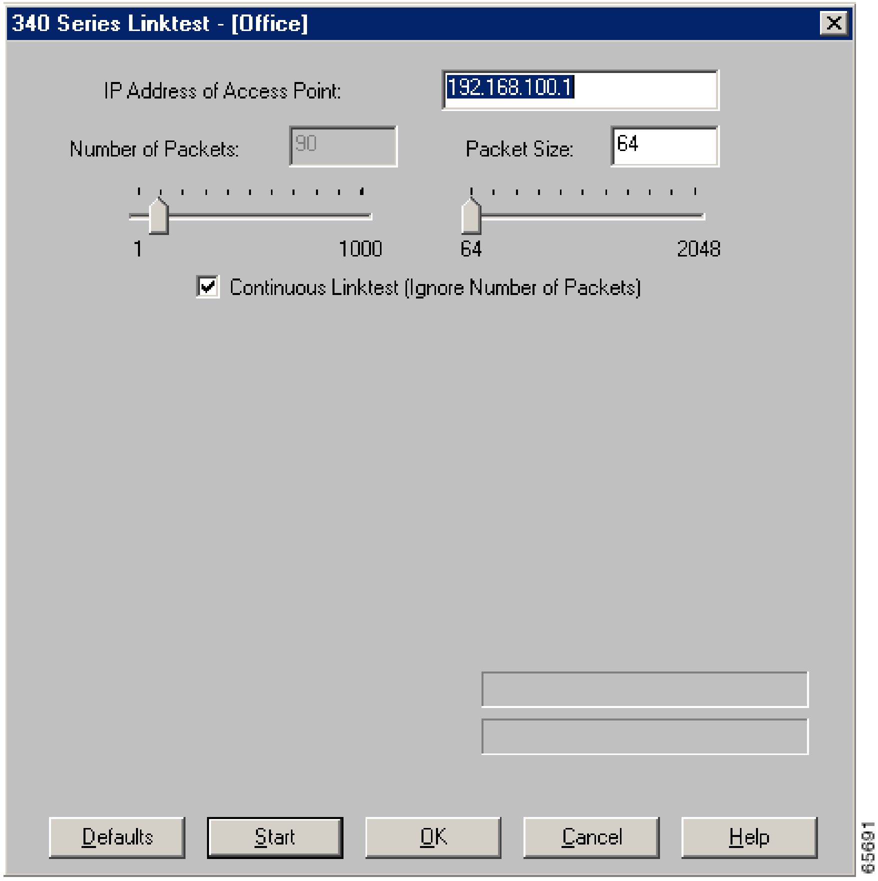
- An IP address must be configured for the access point (or other computer in ad hoc mode).

Follow the steps below to run an RF link test.

Step 1 Open ACU; then click the **Link Test** icon or select **Linktest** from the Commands drop-down menu. The Linktest screen appears (see Figure 7-6).

Note The name of the current profile appears in parentheses at the top of the screen.

Figure 7-6 Linktest Screen



340 Series Linktest - [Office]

IP Address of Access Point: 192.168.100.1

Number of Packets: 90

Packet Size: 64

☑ Continuous Linktest (Ignore Number of Packets)

Step 2 In the IP Address of Access Point field, enter the IP address of the access point or other wireless device with which you want to test the RF link.

Step 3 You can set the link test to run until it has attempted to send a specific number of packets or to run until you stop it. Follow one of the steps below to determine how long the link test will run:

- Select the number of packets that the link test should attempt to send. You can type a number in the Number of Packets field or use the slider to select this value. (The Number of Packets parameter is ignored if the Continuous Linktest checkbox is selected.)

  Range: 1 to 1000

  Default: 4

- Select the Continuous Linktest checkbox to allow the link test to run continuously.

  Default: Deselected

Step 4 Select the size of the data packet that is to be sent to the access point. You can type a number in the Packet Size field or use the slider to select this value.

Range: 64 to 2048

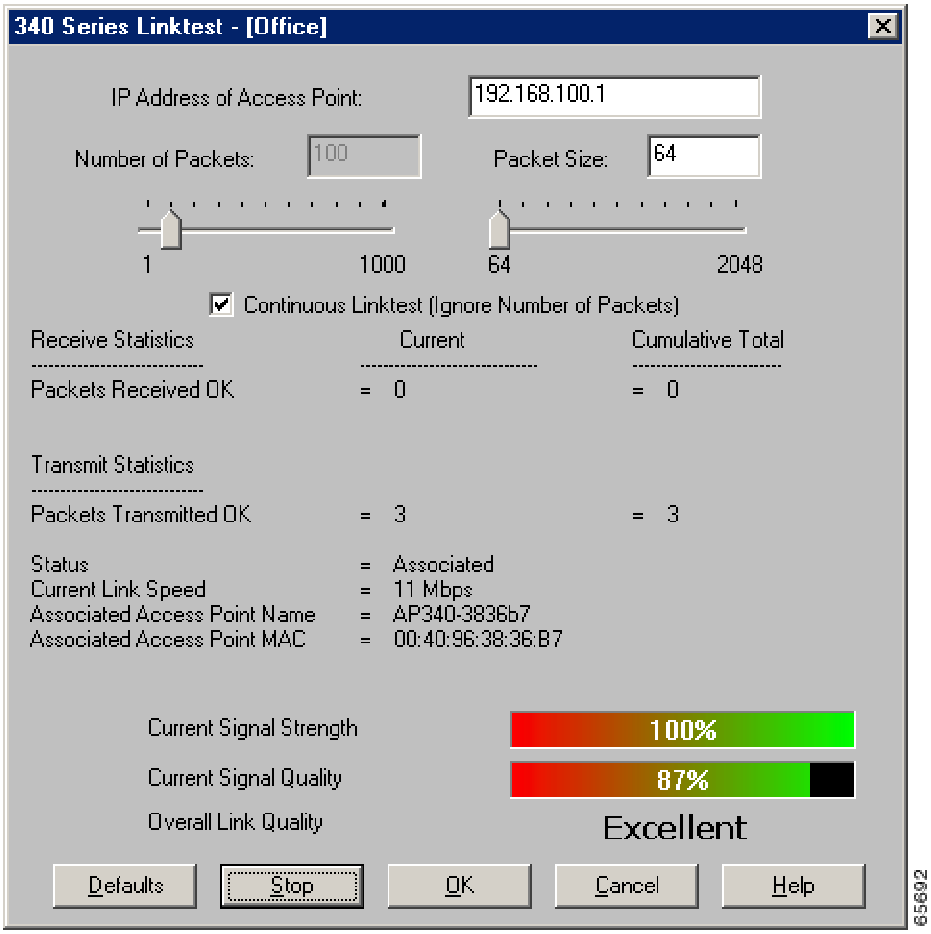
Default: 100

Note The Windows TCP/IP stack fragments (splits up) packets that are greater than 512 bytes. Therefore, the number of transmitted packets does not match the number of received packets (even if none are lost) if the packet size is greater than 512 bytes.

Step 5 Click the **Start** button to run the link test. While the test is running, statistics are displayed and updated periodically.

Figure 7-7 shows the Linktest screen with the signal strength values displayed as percentages, and Figure 7-8 shows the bottom of the same screen with the signal strength values displayed in dBm.

Figure 7-7 Linktest Screen (with Test Running and Signal Strength as a Percentage)



340 Series Linktest - [Office]

IP Address of Access Point: 192.168.100.1

Number of Packets: 100

Packet Size: 64

☑ Continuous Linktest (Ignore Number of Packets)

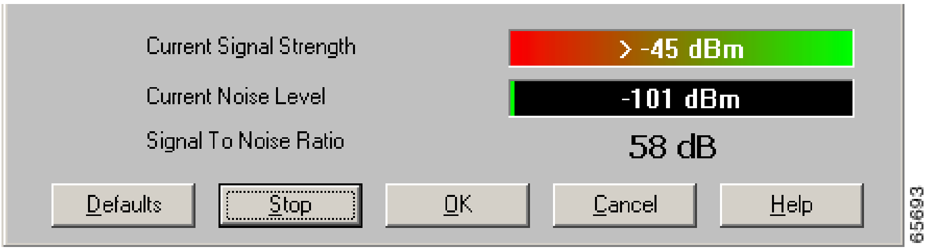
```
Receive Statistics             Current                 Cumulative Total
------------------------       ----------------------- --------------------
Packets Received OK            =  0                    =  0

Transmit Statistics
------------------------
Packets Transmitted OK         =  3                    =  3

Status                         =  Associated
Current Link Speed             =  11 Mbps
Associated Access Point Name   =  AP340-38336b7
Associated Access Point MAC    =  00:40:96:38:36:B7
```

Current Signal Strength: 100%

Current Signal Quality: 87%

Overall Link Quality: Excellent

Figure 7-8 Bottom of Linktest Screen (with Test Running and Signal Strength in dBm)



Current Signal Strength: > -45 dBm

Current Noise Level: -101 dBm

Signal To Noise Ratio: 58 dB

Table 7-5 interprets the statistics that are displayed on the Linktest screen while the link test is running.

Table 7-5 Linktest Statistics

Linktest Statistic	Description
Packets Received OK	The number of packets of the specified size that have been received successfully.
Packets Transmitted OK	The number of packets of the specified size that have been transmitted successfully.
Status	The operational mode of your client adapter. **Value:** Error, Configured, Associated, Not Associated, or Ad Hoc Mode
Current Link Speed	The rate at which your client adapter is currently transmitting data packets. **Value:** 1, 2, 5.5, or 11 Mbps (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)
Associated Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the access point was configured with a name and the client adapter is in infrastructure mode.
Associated Access Point MAC Address	The MAC address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode.
Current 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. **Range:** 0 to 100% or –95 to –45 dBm
Current Signal Quality (2.4-GHz client adapters)	The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal. **Range:** 0 to 100% **Note** This setting appears only for 2.4-GHz client adapters and only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.

Table 7-5 Linktest Statistics (continued)

Linktest Statistic	Description
Current Beacons Received (5-GHz client adapters)	The percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph is, the clearer the signal. **Example:** The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%. **Range:** 0 to 100% **Note** This setting appears only for 5-GHz client adapters (or for 2.4-GHz client adapters using firmware version less than 4.05) and only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.
Current Noise Level	The level of background radio frequency energy in the 2.4- or 5-GHz band. The lower the value and the more green the bar graph is, the less background noise present. **Range:** –100 to –45 dBm **Note** This setting appears only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in Table 7-2 for information.
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 **Note** This setting appears only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.
Signal To Noise Ratio	The difference between the signal strength and the current noise level. The higher the value, the better the client adapter's ability to communicate with the access point. **Range:** 0 to 90 dB **Note** This setting appears only if you selected signal strength to be displayed in dBm. See the "Signal Strength Display Units" parameter in Table 7-2 for information.

Step 6 If you did not set the link test to run continuously, the test ends after the specified number of packets is sent, and the Stop button changes back to the Start button. To stop the link test at any time, click **Stop**, **OK**, or **Cancel**.