

Installation and User Guide

Wireless LAN Client Adapter

Copyright © 2004, 2005 by Airgo Networks. All Rights Reserved.

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of unless such copying is expressly permitted by U.S. copyright law.

Contents

PREFACE	4
OVERVIEW	6
<i>DEVICE TYPES</i>	6
<i>SHIPPING PACKAGE CONTENTS</i>	6
<i>SYSTEM REQUIREMENTS</i>	6
<i>INSERTING AND REMOVING THE WIRELESS LAN CLIENT ADAPTER</i>	6
<i>Checking Adapter Activity</i>	7
<i>INSTALLING THE WIRELESS LAN CLIENT ADAPTER DRIVER AND CLIENT UTILITY</i>	7
<i>Installation Steps</i>	7
<i>CUSTOM INSTALLATION</i>	13
<i>UNINSTALLING THE CLIENT UTILITY AND DRIVERS</i>	14
INTRODUCTION TO THE CLIENT UTILITY	15
<i>SERVICE SET IDENTIFIERS</i>	15
<i>CLIENT UTILITY OVERVIEW</i>	15
<i>ACCESSING THE CLIENT UTILITY</i>	16
<i>Using the Tray Icon</i>	16
<i>NAVIGATING THE USER INTERFACE</i>	17
<i>Top Display</i>	17
<i>Windows Configuration Checkbox</i>	17
<i>Available Networks List</i>	17
<i>Configured Networks List</i>	19
<i>Additional Buttons and Connection Information</i>	20
<i>Monitoring Network Connection Status</i>	20
CONFIGURATION OVERVIEW	22
<i>SCANNING FOR AVAILABLE NETWORKS</i>	22
<i>WORKING WITH PROFILES</i>	22
<i>Profile Tasks</i>	24
<i>Advanced Profile Settings</i>	24
<i>WIRELESS SECURITY</i>	25
USING THE CLIENT UTILITY WITH WINDOWS XP	28
GLOSSARY	30
REGULATORY	36

Preface

This guide explains how to install and configure the Wireless LAN Client Adapter, which provides PC laptop and desktop users with access to 802.11 access points. The guide is intended for business and consumer users who want to install and configure the Wireless LAN Client Adapter quickly and easily. It is also intended for users who are interested in advanced configuration and troubleshooting.

The Wireless LAN Client Adapter products include the following device options:

PC Card adapter for use in laptop and notebook computers

Mini PCI adapter for use in laptop computer mini-PCI expansion slots

The Client Utility, a software tool designed to provide basic configuration options for the device, is shipped with each unit along with the device drivers.

Organization of this Guide

This guide consists of the following chapters:

Chapter 1 describes the features of the Wireless LAN Client Adapter and explains how to install it.

Chapter 2 provides an overview of the Client Utility.

Chapter 3 describes the configuration settings of the Client Utility.

Appendix A explains how to use the profile features of the Client Utility with Windows XP.

Glossary defines terms that apply to wireless and networking technology and the product suite.

Regulatory provides important information about operations of the radio frequency client.

Conventions Used in this Guide

This guide uses the following conventions for instructions and information.

Notes, Cautions, and Warnings

Notes, cautions, and time-saving tips use the following conventions and symbols.



NOTE: Notes contain helpful suggestions or information that is important to the task at hand.



CAUTION: Caution indicates that there is a risk of equipment damage or loss of data when certain actions are performed.



WARNING: Warnings are intended to alert you to situations that could result in injury (such as exposure to electric current, for example).

Related Documentation

The following documentation related to the Airgo Networks wireless networking product line is available on CD-ROM and also on the company website, <http://www.airgonetworks.com>:

_Access Point Installation and Configuration Guide — Describes how to install and configure the Access Point.

_NMS Pro Installation and Configuration Guide — Explains how to install and use the enterprise network management application.

_Access Point Command Line Interface (CLI) Reference Manual — Provides a listing of all the commands available for the Access Point, usable through console access and command line interface; this manual is intended for advanced users and system administrators.

Overview

The Wireless LAN Client Adapter provides the communication link between your laptop and other devices in a wireless network. The adapter operates in the 2.4 GHz radio frequency band and can communicate with any device that meets the compatible IEEE 802.11 standards.

When used with Access Points as part of a wireless network installation, the Wireless LAN Client Adapter offers the following special features:

- Extended range
- Multi mode operation
- Interference handling

The Client Utility, shipped with each Wireless LAN Client Adapter, includes tools for setting the basic configuration.

Device Types

The Wireless LAN Client Adapter is currently offered in two device types:

- **PC Card** — Extended Type II PCMCIA CardBus (32-bit interface) for use in laptop and notebook computers.
- **Mini-PCI**— Mini-PCI adapter for use in laptop computer mini-PCI expansion slots. Mini-PCI adapters are installed by factory personnel when the PC system is configured by the PC manufacturer. For mini-PCI adapter information, consult your PC manufacturer's documentation.

Shipping Package Contents

The Wireless LAN Client Adapter shipping package contains the following items:

- Wireless LAN Client Adapter
- CD containing the device driver and Client Utility

System Requirements

Your PC must meet the following minimum requirements:

- Windows XP or Windows 2000
- 128 MB memory
- CPU 750 MHz or greater
- At least 10 MB disk capacity available for the driver and Client Utility software.
- Type II or Type III CardBus slot for notebooks and laptops

Inserting and Removing the Wireless LAN Client Adapter

To insert the PC card:

- 1 With the computer powered on or off, slide the PC card firmly into an available CardBus slot

(Figure 1).

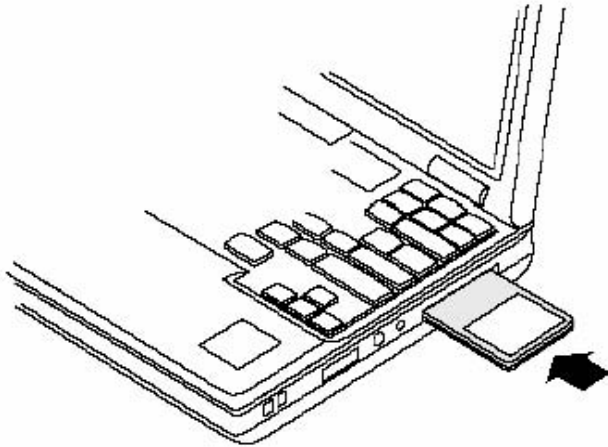


Figure 1: PC Card Installation

To safely remove the PC card while the computer is powered up:

2 Right-click the system tray icon entitled **Safely Remove Hardware** or **Eject or Stop Hardware**.

The system prompts you to select the device to stop.

3 Select **Wireless LAN NIC**, and click **Stop**.

4 Click **OK** when asked to confirm.

5 Press the CardBus eject button on the side of your computer to release the slot locking mechanism and slide the PC card out.

Checking Adapter Activity

The LEDs on the PC card indicate the state of current communications. LED 1 is on the left and LED 2 is on the right when the card is facing up (thick section on top, metallic contact on the bottom):

- **LED 1** — Shows solid green when the adapter is associated (connected) to the network.
- **LED 2** — Blinks green when the adapter is associated to the network and transmitting or receiving data. The blinking speed reflects the level of network activity.

Installing the Wireless LAN Client Adapter Driver and Client Utility

Follow the steps in this section to install the software needed to support your Wireless LAN Client Adapter. The software includes:

- Wireless LAN Client Adapter driver
- Client Utility

Installation Steps

1 Power up your computer.

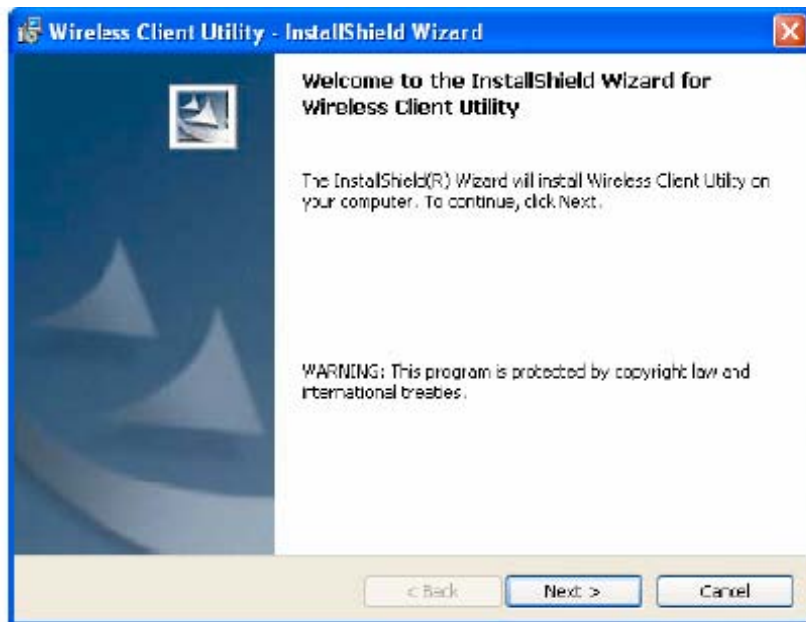
2 Insert the Wireless LAN Client Adapter distribution CD, which should automatically start the Installation Wizard. If the wizard does not start automatically, open the CD and double-click `Setup.msi`.

The Installation Wizard opens.



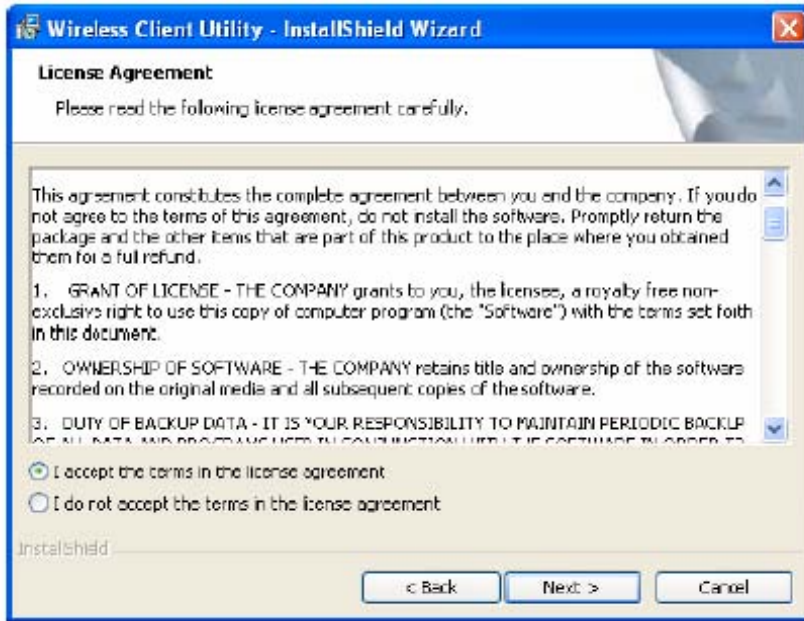
3 Click Install the software.

The Installation Welcome screen opens.



4 Click Next.

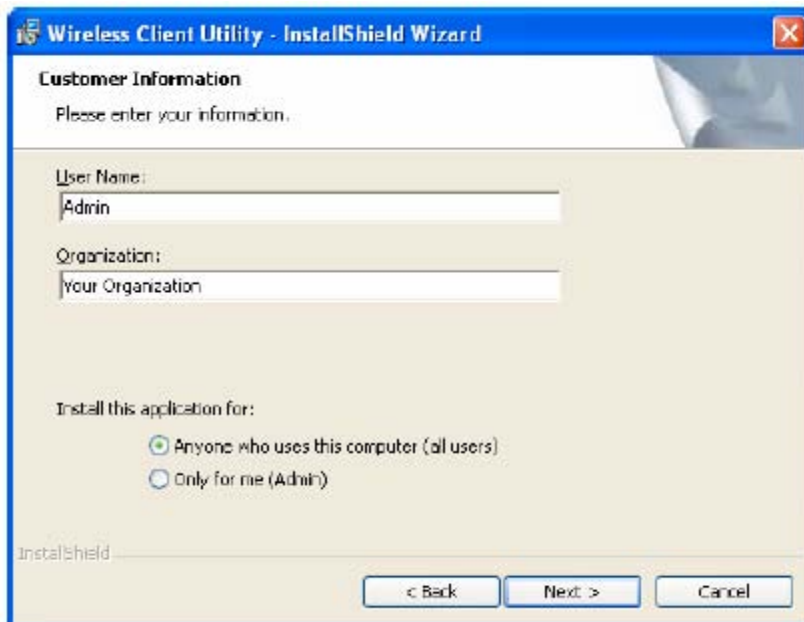
The License agreement window opens.



5 Review the license agreement, and then choose **I accept the terms in the license agreement**.

6 Click **Next**.

7 Enter a user name and organization name, and indicate whether access to the Client Utility will be permitted for all users or just the specified user.

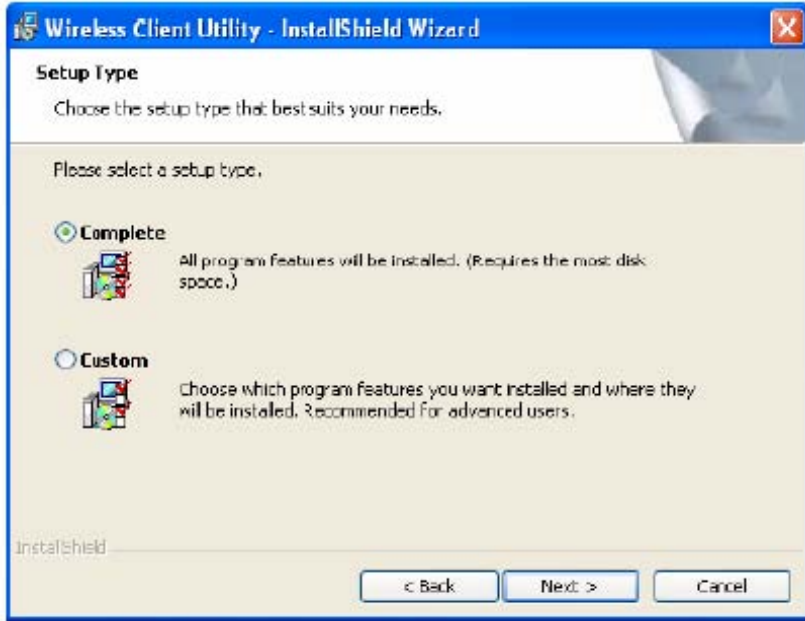


8 Click **Next**.

9 Accept **Complete** as the setup type.

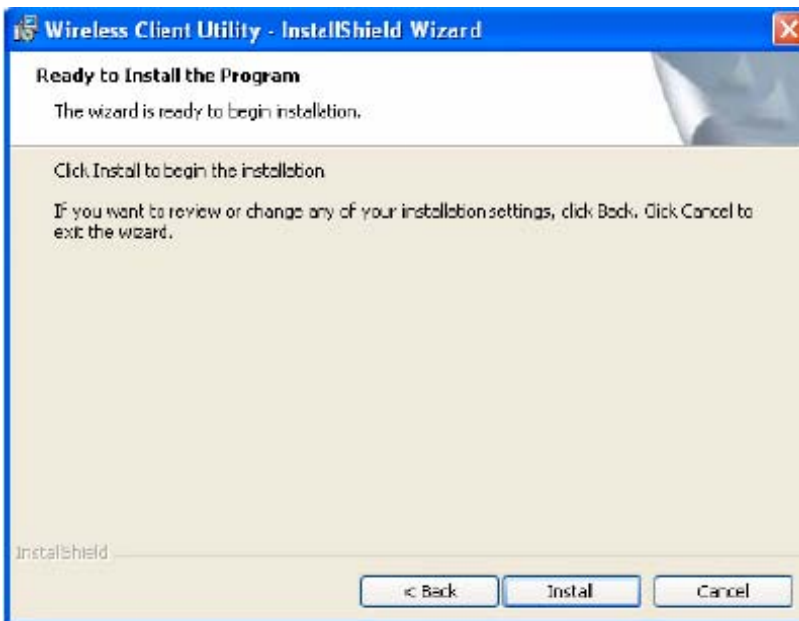


NOTE: If you select **Complete**, the software is automatically installed in the default location. To choose another location, select the Custom option (“Custom Installation”).

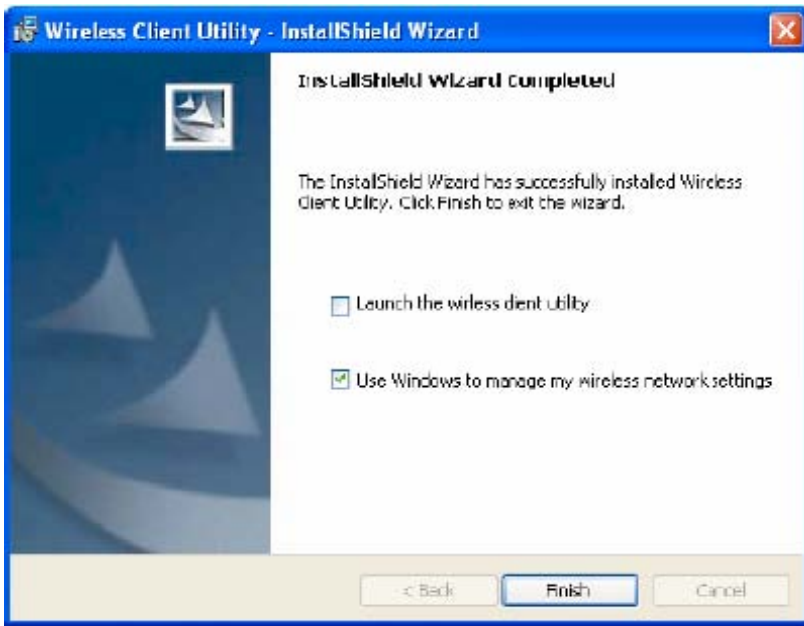


10 Click **Next**.

11 Click **Install** to begin installation. To review previous selections, click **Back**.



The wizard completes the installation of the driver and the Client Utility and presents the completion window.



Select **Use Windows to manage my wireless network settings** if you want to use Wireless Zero Config (WZC) to manage the Client Adapter.

NOTE: It is necessary to use WZC if you want to configure Wi-Fi Protected Access (WPA) security. For information about security, see Chapter 3, “Configuration.” For instructions on enabling or disabling WZC, see Appendix A, “Using the Client Utility With Windows XP.” You can change the WZC option at a later time, from the Client Utility main window, as explained in “Working with Profiles”.

13 Click **Finish** to complete the software installation.

14 Now, insert the Wireless LAN Client Adapter.

The Found New Hardware Wizard opens.



15 If your system has Windows XP Service Pack 2, a welcome window opens. Select **No, not at**

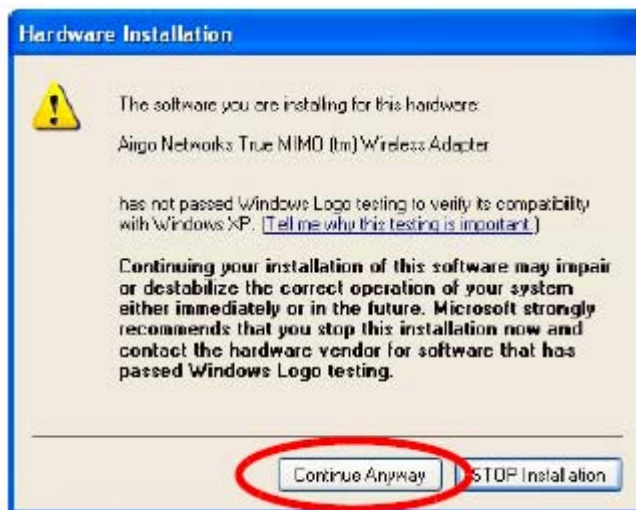
this time to the question, Can Windows connect to Windows Update to search for software and Click **Next**.

16 For all installations, the following window now opens. Accept the default to install the software automatically.



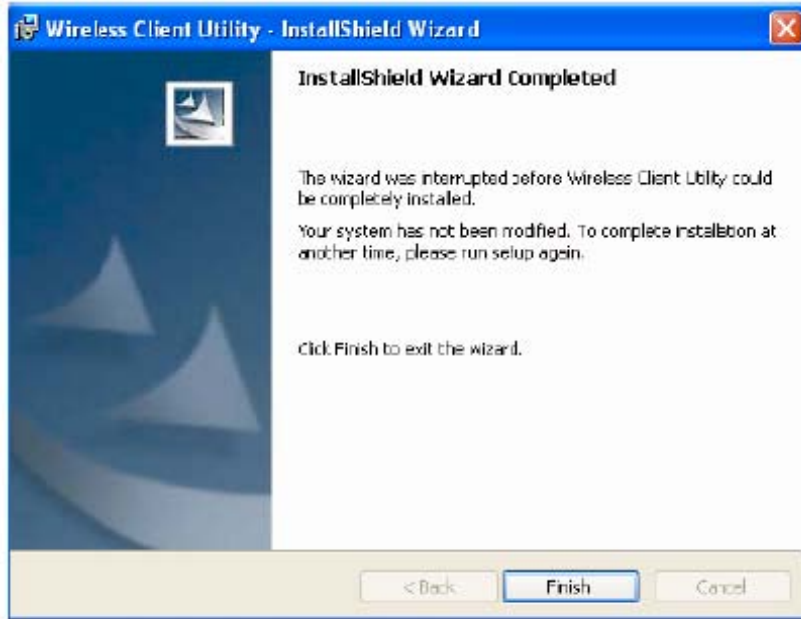
17 Click **Next**.

18 A message appears regarding Windows logo testing. Click **Continue Anyway**.



19 The installation proceeds. When the process is complete, the Completing the Found New Hardware Wizard window opens.

20 Click **Finish**.

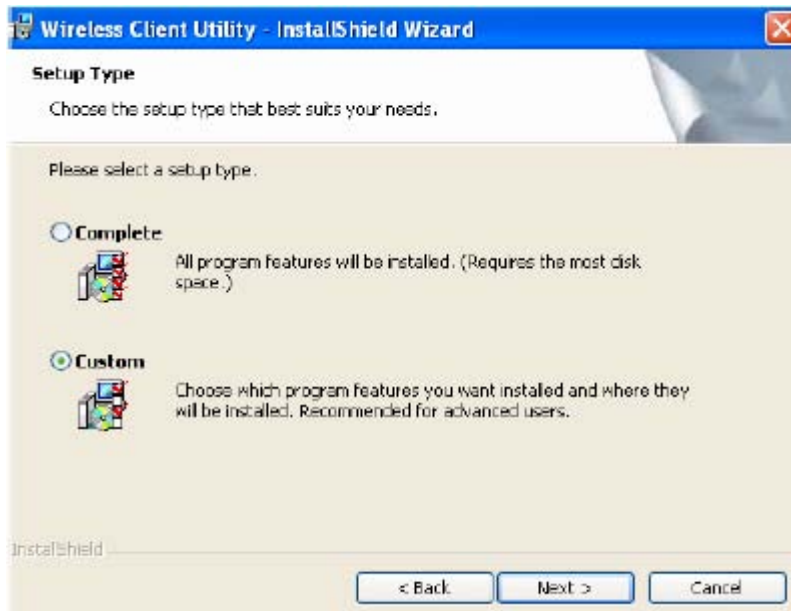


The installation is now complete. Examine the LEDs to confirm that the Client Adapter is installed and working properly. See “Inserting and Removing the Wireless LAN Client Adapter”

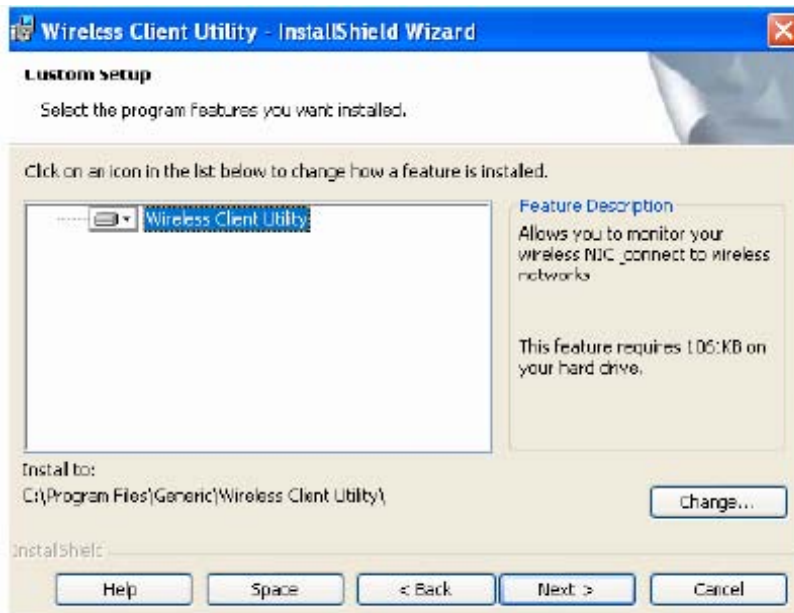
Custom Installation

Follow these steps if you want to change the default software installation location.

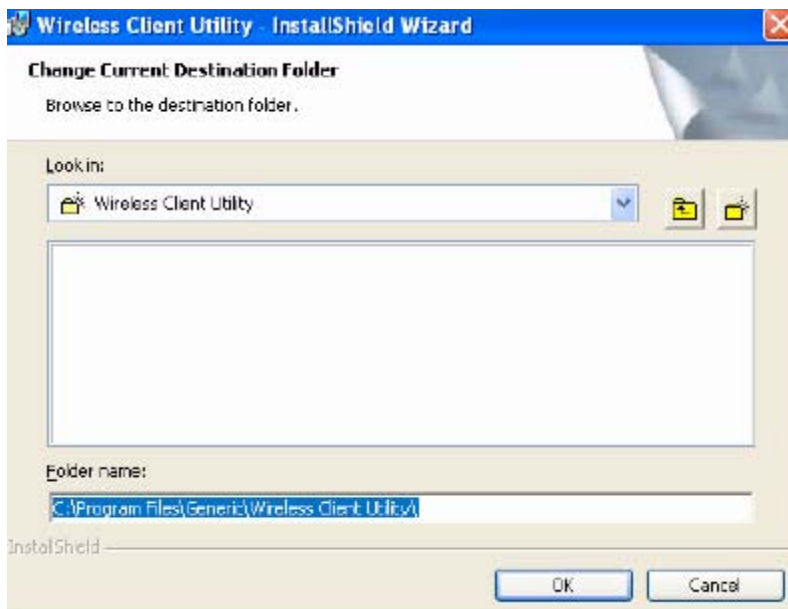
1 In the Customer Information window, select **Custom**, and click **Next**.



2 Click **Change** to select a new location.



3 Enter the path for the new location, or click **Browse** to select a path.



4 Click **OK**.

Uninstalling the Client Utility and Drivers

Uninstall the Client Utility if you are upgrading to a newer version of the utility. To do so, use the Windows Add or Remove Programs utility.

To access Add or Remove Programs:

- 1 Choose **Start > Control Panel > Add or Remove Programs**.
- 2 Select the Client Utility program, and click **Remove**.
- 3 Confirm that you want to remove the program, and following the wizard instructions.

Introduction to the Client Utility

The Wireless LAN Client Adapter connects your PC to a wireless local area network (wireless LAN) by way of radio signals. An access point is the device that forwards data from the wired network to your PC by way of radio signals and connects you with other wireless users. The IEEE 802.11 standard identifies two types of wireless networking modes:

In an *infrastructure* network, an access point links the wireless LAN to a wired network. By attaching to an existing network infrastructure, you can gain access to other resources on the wired network, other wireless LANs, or the Internet. This is the mode to use when setting up a home network or accessing an office network.

In an *ad-hoc* wireless network, you establish communications between your PC and a small number of other wireless users without using an access point.



The Wireless LAN Client Adapter installed on your PC can communicate with any access point that supports the industry standard IEEE 802.11 wireless communications protocol.

Service Set Identifiers

The Service Set Identifier (SSID) is a name that uniquely identifies a wireless local area network. Each device in the wireless network must have the same SSID configured in order to participate in the network. The SSID can be up to 32 alphanumeric characters in length and is also known as the wireless network name.

The 802.11 standard specifies two types of network service sets identified by SSID:

Basic Service Set (BSS) -- collection of wireless devices operating with an access point in infrastructure mode (Basic Service Set - BSS) or without an access point in ad-hoc mode (Independent Basic Service Set - IBSS).

Extended Service Set (ESS) -- collection of BSSs with wireless devices that can roam from one BSS to another while staying connected to wireless network resources.

Client Utility Overview

The Client Utility enables you to perform all these functions:

Obtain a view of your wireless network, including the type of network, the access point with which you are associated, and information about the radio signals currently being transmitted and received.

Scan and connect to wireless networks within radio range of your PC.

Create or select a profile, which stores the specifics of the network connection and security selections for your Wireless LAN Client Adapter. The Client Utility supports multiple profiles, enabling you to connect to different networks, whether at home, at work, or at wireless hotspot locations.



To use the profile features of the Client Utility on Windows XP, you must specify that Windows will not be managing the Client Adapter.

Accessing the Client Utility

The Client Utility normally runs automatically when the Client Adapter is installed, and the application icon appears in the Windows system tray. If the Client Utility is not running, you can start it from the Start menu:

Choose **Start > Programs > ... > Client Utility** .

Using the Tray Icon

When you start the Client Utility, a small signal icon becomes visible in the system tray on the Windows toolbar.



Application icon

The color of the icon reflects the quality of the wireless connection:

Icon	Description
	No adapter present
	Adapter present, radio turned off
	Adapter present, radio on, no association
	Adapter present, radio on, poor signal quality
	Adapter present, radio on, marginal signal quality
	Adapter present, radio on, good signal quality

The tray icon has a right-click menu that includes the following options:

Item	Description
Show	Open the Client Utility window.
Radio On/Off	Turn the Client Adapter radio on or off.
Help	Open the online help system.
About	Display information that may be helpful for technical support.
Exit	Exit the Client Utility. To restart the Client Utility after exiting, you must use the Start menu.

Navigating the User Interface

This section explains how to use the Client Utility interface.

Top Display

The top display section lists characteristics of the current network connection:







Item	Description
Status	Indicates whether the Client Adapter is currently associated to a working AP.
Network	If Status is Connected, lists the name of the network to which the Client Adapter is connected.
AP Name	If Status is Connected, lists the name of the AP to which the Client Adapter is connected.
Channel (Mode)	If Status is Connected, lists the radio channel used and the 802.11 mode (b or g).







Windows Configuration Checkbox

A checkbox entitled Use Windows to configure my wireless networks is located just below the top display section. Select this checkbox to use Wireless Zero Config (WZC) to configure the Client Adapter. WZC is required to use Wi-Fi Protected Access (WPA) as the security mode when connecting to the network. For more information on security, see. If you use WZC to configure the Client Adapter, you can still use the Client Utility to monitor available networks and check connection status.

Available Networks List

The Available Networks section of the Client Utility window lists all the working networks within radio range of your Client Adapter. The following information is presented:

Icon	Column	Description
	SSID	Name of the network, associated
	SSID	Name of the network, not associated
	Signal quality	Signal strength, as a percentage: Four solid green bars, 60% or greater
	Signal quality	Signal strength, as a percentage: Three solid green bars, one hollow green: 40-60%
	Signal quality	Signal strength, as a percentage: Two solid yellow, two hollow yellow bars, 20-40%
	Signal quality	Signal strength, as a percentage: One solid yellow bar, three hollow yellow bars, 5-20%

	Signal quality	Signal strength, as a percentage: All red hollow bars, less than 5%
	Security	Open security
	Security	WEP security
	Security	WPA security
	Channel	Current radio channel used for communications between the Client Adapter and the access point
	Type	Infrastructure Ad-hoc network
wmm, 11e	QoS	Applicable wireless quality of service (QoS) settings for Wi-Fi multimedia (WMM) and 802.11e QoS

Perform any of the following operations on the Available Networks list:

Item	Description
Re-Scan	Causes the Client Adapter software to immediately scan for all the wireless networks within radio range. Detected networks are presented in the Available Networks list. Background scanning for available networks occurs by default every five seconds.
Configure	Open the Profile Editor window (See <i>Profile Tasks</i>).
Resize columns	Select and move the column header dividers.
Sort entries by column	Click the column header. The arrow that appears indicates the sort order (upward facing for ascending and downward facing for descending). To change the sort order, click the column header again.
Add or remove columns	Right-click on the column header, and select or deselect columns.
Reorder columns	Drag the column headers to reorder the columns.
Properties	Displays network details. Select one or more networks and click Properties to open the Properties window. See <i>Properties Window Information</i> lists the information shown in the Properties window. All APs for the selected networks are displayed.

Properties Window Information	
Item	Description
BSSID	IDs of the APs belonging to the selected SSIDs
SSID	ID of the selected networks

Security	Security mode (WEP, WPA, or open)
Supported Rates	All data rates supported by the access point
Basic Rates	Minimum data rates supported by the access point
Channel	Radio channel used for communication between the Client Adapter and access point
Mode	802.11 mode (b or g)
Type	Network type (Infrastructure or Ad-hoc)
Country Code	International Standards Organization (ISO) standards for frequency selection based on country-specific regulations ¹
Environment	Type of physical environment (Indoor, Outdoor or Both)
Channel List	Available operating channels
True MIMO	Use of enhanced, True MIMO, data rates (Yes or No)
Signal strength	Strength of the radio signal, as a percentage

Configured Networks List

The Configured Networks list shows all the networks for which a network profile is defined. For information on using profiles, see *Working with Profiles*. The Configured Networks list includes the following information:

Item	Description
SSID	Name of the network
Signal quality	Quality of the radio signal
Security	Type of active security
Type	Infrastructure or ad-hoc network

Perform any of the following operations on the Configured Networks list:

Item	Description
Add	Click Add to open the Profile Editor to create a new profile.
Remove	Click Remove to eliminate a network from the Configured Networks list.
Edit	Click Edit to edit the selected network using the Profile Editor.
Change network order	Highlight an entry and use the arrows to the right of the list to move the entry up or down.

¹ Client adapters will be channel restricted based on country code programmed in the adapters EEPROM.

Resize columns	Select and move the column header dividers.
Sort entries by column	Click the column header. The arrow that appears indicates the sort order (upward facing for ascending and downward facing for descending). To change the sort order, click the column header again.

Additional Buttons and Connection Information

The following buttons are located below the Configured Networks area:

Button	Description
Expansion arrow	Click the arrow to display or hide current connection information (see <i>Current Connection Information</i>).
Help	Open the online help system.
OK	Save changes and then close the Client Utility window without quitting the application. To exit the application, use the system tray right-click menu.
Cancel	Cancel changes if they have not been saved.
Apply	Make the selected configured network active.

The remaining area displays read-only information about the current connection and settings:

Current Connection Information	
Item	Description
Transmit Rate	Current connection rate for data transmitted from your PC to the access point.
Transmit Bytes	Number of bytes of data transmitted since your Client Adapter was last enabled.
Receive Rate	Current connection rate for data received by your PC from the access point.
Receive Bytes	Number of bytes of data received since the Client Adapter was last enabled.
Band	802.11 radio frequency band used for communications.
Channel	Radio channel used for communications.
Authentication	Method of client identification.
Encryption	Method of protecting data integrity.

Monitoring Network Connection Status

Once a profile is activated and you are associated to the selected network, the main Client Utility presents status information. The SSID icon changes to active and in the top left

area of the window, an SSID signal indicator shows the overall strength of all APs that are configured for that SSID.

Configuration Overview

The Client Utility uses profiles to store information describing how your Wireless LAN Client Adapter connects to the wireless network. Each profile contains information about the type of network connection and security settings.

To make it easy to connect to wireless networks at home, office, or wireless hotspot locations, Client Utility allows you to create multiple profiles, each containing information about a different network or a different set of configuration values. When you move from one location to another, your Client Adapter automatically detects which network is currently available and applies the correct profile. The Configured Networks list in the Client Utility main window contains an entry for each profile.

The following rules apply when connecting to a wireless network:

The Client Utility always attempts to connect to a network with a configured profile, in the order in which the configured networks are listed.

If there are no previously configured networks, or if it is not possible to connect to any currently configured networks, the Client Adapter attempts to connect to the AP with the best signal quality, open authentication, and no encryption.

If all the connection options fail, or if you want to connect to a different available network, you can create a profile for the network with appropriate security parameters. This adds the network to the Configured Networks list and makes it available for automatic connection in the future.

Scanning for Available Networks

Upon driver load, the Client Adapter scans for all access points within radio range and attempts to connect to one of them based on previously scanned profiles. It associates to the first access point it finds for which it can establish radio communications. Although association normally happens automatically; it is recommended that you keep the Client Utility running while you are connected. This enables you to verify the configuration and confirm that the access point to which you are connected is a trusted component of your network.

Whenever you open the Client Utility, the system performs an automatic scan. You can also scan for networks on demand, at any time.

To scan for available networks:

Choose ***Start > Programs > ... > Client Utility*** .

This displays the application icon in the system tray.

Click ***Re-Scan*** .

The Re-Scan button is disabled while scanning takes place. When the scan is complete, the Available Networks list displays all the discovered networks.

Working with Profiles

Profiles store configuration information about how your Wireless LAN Client Adapter connects to specific wireless networks. Use the Profile Editor to create new profiles or modify existing ones.

The Profile Editor contains the following fields:

Field	Description
SSID	Service Set Identifier (SSID) is a name that uniquely identifies a wireless local area network. Each device in the wireless network must have the same SSID configured in order to participate in the network.
BSSID	Basic Service Set (BSS) is the collection of wireless devices operating with an individual access point in infrastructure mode or without an access point in ad-hoc mode. For further information on service set identifiers.
Network Type	The Network Type indicates the type of network arrangement. Infrastructure -- Refers to an existing wireless network, usually with an interface to a wired network, for Internet and email access, file sharing, and print and other services. Ad Hoc -- Refers to a temporary wireless network that has been set up by another user. Start Ad-Hoc Network -- Permits you to set up a new ad-hoc network to communicate with other PCs without using an access point.
Channel	In infrastructure networks, the channel used for radio communications is determined at the access point and for ad-hoc networks; the channel is determined by the user who starts the network. It is necessary to select a channel only if you are starting a new ad-hoc network. ²
Authentication	The authentication and encryption settings provide options for configuring a secure connection between your PC and access point. The following authentication options are available: Open -- No authentication Share -- Authentication based on shared keys See <i>Wireless Security</i> for background on wireless security options and guidelines for security settings in the enterprise, small office, and home environments.
Encryption Type	The following encryption options are available: None -- No encryption WEP -- Encryption based on shared WEP keys See <i>Wireless Security</i> for background on wireless security options and guidelines for security settings in the enterprise, small office, and home environments.
Encryption	Encryption Enter up to 4 encryption keys, if the encryption type is WEP. The radio buttons under Default provide for default selection of one of the up to 4 WEP keys that may be entered. The keys are 64-bit or 128-bit and may be specified in ASCII (text) or hexadecimal (numeric) format: ASCII - 5 ASCII characters (64-bit); 13 ASCII characters (128-bit) Hexadecimal - 10 ASCII characters (64-bit); 26 hexadecimal digits (128-bit)

² Channel selection will be restricted based on country code programmed into the client adapter EEPROM.

Profile Tasks

To create a profile for an available network:

Select the Network and click **Configure**.

The Profile Editor window opens with the SSID, BSSID, Network Type, and Channel fields already filled in.

Select an authentication method and encryption type. If you select WEP as the encryption type, enter encryption key information. For information on encryption keys, see *Encryption*.

Click **OK**.

The Profile window closes and the newly created profile appears in the Configured Networks list in the Client Utility window.

You can edit any profile in the list, including the active one. If you edit and apply the active profile, the system temporarily drops the network connection while implementing the changes. When the configuration change is complete, the network connection is restored.

To make a profile active:

Select the profile in the Configured Networks list, and click **Apply**.

To edit a profile:

Highlight a name in the Configured Networks list and click **Edit**.

The Profile Editor window opens.

Enter or confirm authentication and encryption type, and enter WEP keys, if appropriate.

Click **OK**.

To add a new profile not based on an existing profile or network:

Click **Add**.

The Profile Editor window opens.

Enter the SSID of the network. The BSSID is determined automatically when your Client Adapter associates to an access point.

Select the network type. If you select Start Ad-Hoc, enter a radio channel setting for the network. If you select Infrastructure or Ad-Hoc (for an existing ad-hoc network), the channel is automatically set.

Select authentication and encryption type, and enter WEP keys, if appropriate.

Click **OK**.

To delete a profile:

Highlight the profile name and click **Delete**.

Click **OK** when prompted to confirm.

Advanced Profile Settings

The Advanced button to the right of the Profile Name opens the Advanced Profile Settings window. The settings in this window enable you to take advantage of the enhanced performance features of the Access Point. It is recommended that you retain the default Auto settings, which provide compatibility with basic, enhanced data rates, network density, and power usage.

Wireless Security

Although security is important in any network, the characteristics of wireless networks can make them vulnerable to attack. Unlike wired networks, which require a physical connection that can be secured with lock and key, wireless networks require only a radio signal for communication, and physical barriers do not provide protection. A concern since the introduction of the IEEE 802.11 wireless communication standard, wireless security continues to evolve, as shortcomings of existing security solutions are uncovered and new solutions are adopted.

Wireless security encompasses two major components: encryption and authentication. Encryption is the means by which data transferred across the wireless link are protected from eavesdropping. *Authentication* is the means by which the identity of your PC or your identity, or both, are confirmed so that you have permission to use the network.

Authentication



This section provides an overview of authentication options. The most effective authentication options available today are supported either through the Client Utility or by leveraging the Microsoft Wi-Fi software implementations. For further information, see *Client Utility Security Options*.

Effective authentication methods rely on manual distribution of shared or pre-shared authentication keys or automatic generation of keys by a RADIUS (Remote Authentication Dial-In User Service) server.

A shared or pre-shared key is an authentication string entered at the access point and client PCs. Authentication takes place by matching the key stored in each PC with the key stored in the access point.

Automatic key-generation methods rely upon digital certificates, which contain encoded user and encryption information to verify the identity of a user and match it with a database of secure user records. A certificate authority is the network service that manages digital certificates and guarantees their integrity. The IEEE 802.1X standard specifies certificate-based authentication using EAP (Extensible Authentication Protocol). EAP, in turn, comes in numerous variations.

Most enterprises manage remote access to the certificate authority using a RADIUS (Remote Authentication Dial-In User Service) server. In this arrangement, client PC users install RADIUS client software on their local PCs to provide RADIUS server access. Funk Software and Microsoft are the major suppliers of RADIUS client software.

For home or small office networks, shared or pre-shared keys can provide adequate authentication without the burden of centralized management and control. A built-in RADIUS security portal is provided in the Access Point to extend the management and scalability features of centralized management to administrators in small-to-mid sized office environments.

Encryption



This section provides an overview of encryption options. The most effective authentication options available today are supported either through the Client Utility or by leveraging the Microsoft Wi-Fi software implementations. For further information, see *Client Utility Security Options*.

Encryption protects wireless data from being intercepted and deciphered during transmission, and thereby assures the security of your data. The Client Adapter is compatible with the following options:
AES (Advanced Encryption Standard) -- Excellent, financial-grade security
TKIP (Temporal Key Integrity Protocol) -- Good security, used as an upgrade to legacy systems

WEP (Wired Equivalent Privacy) -- Minimal protection security, acceptable for non-critical data

Open or no encryption -- No protection, use for non-critical communications or with other security protection such as https or VPN/IPsec for corporate communications

The most effective encryption methods are part of the WPA (Wi-Fi Protected Access) cipher suite and are recommended for all environments in which security is an important consideration, whether in the enterprise, small office or home. WPA provides much more complete protection against discovery of encryption keys than do the WEP standards. WPA itself has already spawned two generations of encryption technology, with AES being the latest and most effective standard. TKIP is the encryption protocol that was first introduced with WPA, but it provides less complete protection than does AES.

The original 802.11 wireless communication specification standard included WEP for wireless security. Still widely used today, WEP security provides some security protection, but can be vulnerable to attack. Use WEP in cases where the access point does not support higher level security and security is a consideration in your network design.

The WEP algorithm requires an encryption key or keys to be used in the encrypting and decrypting of data. The Client Utility uses 64-bit or 128-bit encryption keys, which may be specified in ASCII (text) or hexadecimal (numeric) format:

ASCII keys must be 5 characters in length (64-bit) or 13 characters in length (128-bit) Example: 64-bit: *mynm5* ; 128-bit: *17keycode1298*

Hexadecimal keys must be 10 hex digits in length (64-bit) or 26 hex digits in length (128-bit), where hex digits are in the range 0-9, a, b, c, d, e, f). Example: 64-bit: *55772abbcc* ; 128-bit: *12340987afcb45677fdc789045*

The Client Utility supports as many as four WEP keys.

Client Utility Security Options

The Available Networks list in the Client Utility window displays the security advertised by the AP.

The Client Utility supports configuration of WEP or shared key options for authentication and WEP or None options for encryption. In the Profile window, you can select WEP or open security for the radio connection between your PC and the access point and enter choices for encryption and authentication within the selected security framework. For instructions, see *Working with Profiles*.

Windows XP users can connect to networks that support WPA security provided that the appropriate Microsoft security updates have been installed. To use WPA security, it is necessary to use the Wireless Zero Config (WZC) capability native to Windows XP. When WZC is managing the device, the profile features of the Client Utility are automatically disabled; however, it is still recommended to use the Client Utility to view scanned networks.

To use WZC to configure security settings:

Select *Use Windows to configure my wireless networks* in the Client Utility main window.

Click **OK**.

Now use WZC to configure security settings:

Right-click the wireless icon on the system tray.

Select View Available Wireless Networks.

The appearance of the next dialog box depends upon whether your computer has Service Pack 1 or Service Pack 2 installed.

Select the network, and click **Connect**.

If the network requires a security password or key, you are prompted to enter the key. This occurs, for instance, if WPA-PSK security is currently used in the network.

The system connects the Client Adapter to the network and presents a star icon, indicating that a successful connection was made. A balloon message also appears in the system tray.

For Service Pack 1, a window opens to show the list of available networks.

Select your network, and click Advanced to open the Wireless Network Connection Properties window, Wireless Networks tab.

Confirm that Use Windows to configure my wireless network settings is selected.

Select the network, and click Configure.

Confirm the authentication and encryption selections exactly match those of the access point to which you are connecting. Enter a network key, if required.

If you selected AES for data encryption, open the Authentication tab and select the EAP type appropriate to your network.

Click OK as needed to close the WZC windows.



To revert to using the Client Utility to manage the network, you must clear the Use Windows to configure my wireless network settings checkbox shown in *Confirm that Use Windows to configure my wireless network settings is selected*.

Using the Client Utility With Windows XP

To use the profile features of the Client Utility on Windows XP, you must specify that Windows XP will not be managing the wireless adapter.

To specify that Windows will not be managing the wireless adapter:

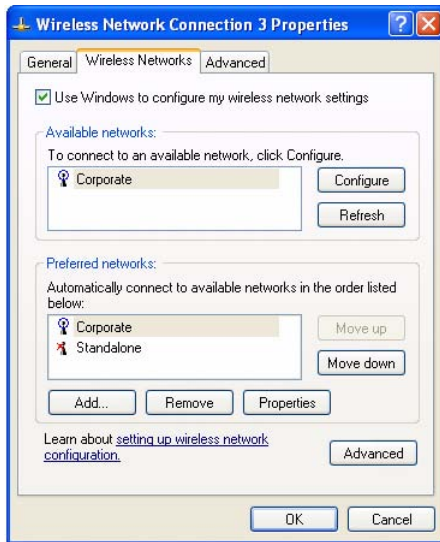
Right-click the wireless icon on the system tray.

Select View Available Wireless Networks.

The window shows the list of available networks.



Click Advanced to open the Wireless Network Connection Properties window, Wireless Networks tab.



Clear the checkbox entitled Use Windows to configure my wireless network settings.

Click OK.

You can now use the Client Utility to manage your wireless connections.

Glossary

This glossary defines terms that apply to wireless and networking technology.

802.1x Standard for port-based authentication in LANs. Identifies each user and allows connectivity based on policies in a centrally managed server.

802.11 Refers to the set of WLAN standards developed by IEEE. The three commonly in use today are 802.11a, 802.11b, and 802.11g, sometimes referred to collectively as Dot11.

access control list (ACL) A list of services used for security of programs and operating systems. Lists users and groups together with the access awarded for each.

access point (AP) An inter-networking device that connects wired and wireless networks together. Also, an 802.11x capable device that may support one or more 802.11 network interfaces in it and coordinates client stations to establish an Extended Service Set 802.11 network

Advanced Encryption Standard (AES) An encryption algorithm developed for use by U.S. government agencies; now incorporated into encryption standards for commercial transactions.

ad-hoc network A group of nodes or systems communicating with each other without an intervening access point. Many wireless network cards support ad-hoc networking modes.

authentication server A central resource that verifies the identity of prospective network users and grants access based on pre-defined policies.

authentication zone A administrative grouping of resources for user authentication.

backhaul The process of getting data from a source and sending it for distribution over the main backbone network. Wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. Also referred to as WDS.x.

Basic Service Set (BSS) The set of all wireless client stations controlled by a single access point.

bridge A connection between two (or more) LANs using the same protocol. Virtual bridges are used as a means of defining layer 2 domains for broadcast messages. Each virtual bridge uniquely defines a virtual local area network (VLAN).

Class of Service (COS) A method of specifying and grouping applications into various QoS groups or categories.

client utility This application executes on a station and provides management and diagnostics functionality for the 802.11 network interfaces.

Differentiated Services Code Point (DSCP) A system of assigning Quality of Service "Class of Service" tags.

Domain Name Service (DNS) A standard methodology for converting alphanumeric Internet domain names to IP addresses.

Dynamic Host Configuration Protocol (DHCP) A communications protocol enabling IP address assignments to be managed both dynamically and centrally. With DHCP enabled on a node (a system, device, network card, or access point), when it boots or is connected to a network, an address is automatically assigned. Each assigned address is considered to be "leased" to a specific node; when the lease expires, a new IP can be requested and/or automatically reassigned. Without DHCP, IP addresses would need to be entered manually for each and every device on the network.

dynamic IP address A TCP/IP network address assigned temporarily (or dynamically) by a central server, also known as a DHCP server. A node set to accept dynamic IPs is said to be a "DHCP client."

Extensible Authentication Protocol (EAP) Standard that specifies the method of communication between an authentication server and the client, or supplicant, requesting access to the network. EAP supports a variety of authentication methods.

Extensible Authentication Protocol Over LAN (EAPOL) Protocol used for 802.1x authentication.

EAP-TLS EAP using Transport Layer Security. EAP-based authentication method based on X.509 certificates, which provides mutual, secure authentication. Certificates must be maintained in the authentication server and supplicant.

EAP-PEAP Protected EAP-based authentication method based on X.509 certificates. Uses a two-phase approach in which the server is first authenticated to the supplicant. This establishes a secure channel over which the supplicant can be authenticated to the server.

Extended Service Set (ESS) A set of multiple connected BSSes. From the perspective of network clients, the ESS functions as one wireless network; clients are able to roam between the BSSs within the ESS.

ESSID Name or identifier of the ESS used in network configuration.

hostname The unique, fully qualified name assigned to a network computer, providing an alternative to the IP address as a way to identify the computer for networking purposes.

Hypertext Transfer Protocol (HTTP) Protocol governing the transfer of data on the World Wide Web between servers and browser (and browser enabled software applications).

Hypertext Transfer Protocol over SSL (HTTPS) A variant of HTTP that uses Secure Sockets Layer (SSL) encryption to secure data transmissions. HTTPS uses port 443, while HTTP uses port 80.

Independent Basic Service Set (IBSS) A set of clients communicating with each other or with a network via an access point.

Internet Protocol (IP) The network layer protocol for routing packets through the Internet.

IP address 32-bit number, usually presented as a period-separated (dotted decimal) list of three-digit numbers, which identifies an entity on the Internet according to the Internet Protocol standard.

local area network (LAN) A group of computers, servers, printers, and other devices connected to one another, with the ability to share data between them.

management information bases (MIBs) A database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allows any SNMP and RMON tools to monitor any device defined by a MIB.

maskbits Number of bits in the subnet prefix for an IP address, (provides the same information as subnet mask). Each triplet of digits in an IP address consists of 8 bits. To specify the subnet in maskbits, count the number of bits in the prefix. To specify using a subnet mask, indicate the masked bits as an IP address. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Media Access Control (MAC) address A unique hardware-based equipment identifier, set during device manufacture. The MAC address uniquely identifies each node of a network. Access points can be configured with MAC access lists, allowing only certain specific devices to connect with the LAN through them, or to allow certain MAC-identified network cards or devices access only to certain resources.

MAC address authentication Method of authenticating clients by using the MAC address of the client station rather than a user ID.

Network Address Translation (NAT) The translation of one IP address used within a network to another address used elsewhere. One frequent use of NAT is the translation of IPs used inside a company, versus the IP addresses visible to the outside world. This feature helps increase network security to a small degree, because when the address is translated, it is an opportunity to authenticate the request and/or to match it to known, authorized types of requests. NAT is also used sometimes to map multiple nodes to a single outwardly visible IP address.

Network Interface Card (NIC) Generic term for network interface hardware that includes wired and wireless LAN adapter cards, PC Cardbus PCMCIA cards, and USB-to-LAN adapters.

network management system (NMS) Software application that controls a network of multiple access points and clients.

node Generic term for a network entity. Includes an access point, network adapter (wireless or wired), or network appliance (such as a print server or other non-computer device).

Network Time Protocol (NTP) NTP servers are used to synchronize clocks on computers and other devices. APs have the capability to connect automatically to NTP servers to set their own clocks on a regular basis.

Packet Internet Groper (PING) A utility that determines whether a specific IP address is accessible, and the amount of network time (measured in milliseconds) needed for response. PING is used primarily to troubleshoot Internet connections.

policy-based networking The management of a network with rules (or policies) governing the priority and availability of bandwidth and resources, based both on the type of data being transmitted and the privileges assigned to a given user or group of users. This allows network administrators to control how the network is used in order to help maximize efficiency.

Power over Ethernet (PoE) Power supplied to a device by way of the Ethernet network data cable instead of an electrical power cord.

preamble type The preamble defines the length of the cyclic redundancy check (CRC) block for communication between the access point and a roaming network adapter. All nodes on a given network should use the same preamble type.

Quality of Service (QoS) QoS is a term encompassing the management of network performance, based on the notion that transmission speed, signal integrity, and error rates can be managed, measured, and improved. In a wireless network, QoS is commonly managed through the use of policies.

Remote Authentication Dial-In User Service (RADIUS) A client/server protocol and software that enables remote access servers to communicate with a central server in order to authenticate users and authorize service or system access. RADIUS permits maintenance of user profiles in a central repository that all remote servers can share.

radio frequency (RF) The electromagnetic wave frequency radio used for communications applications.

roaming Analogous to the way cellular phone roaming works, roaming in the wireless networking environment is the ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

rogue AP An access point that connects to the wireless network without authorization.

Secure Shell (SSH) Also known as the Secure Socket Shell, SSH is a UNIX-based command line interface for secure access to remote systems. Both ends of a communication are secured and authenticated using a digital certificate, and any passwords exchanged are encrypted.

Service Set Identifier (SSID) The SSID is a unique identifier attached to all packets sent over a wireless network, identifying one or more wireless network adapters as "belonging" to a common group. Some access points can support multiple SSIDs, allowing for varying privileges and capabilities based on user roles.

Secure Sockets Layer (SSL) A common protocol for message transmission security on the Internet. Existing as a program layer between the Internet's Hypertext Transfer

Protocol (HTTP) and Transport Control Protocol (TCP) layers, SSL is a standard feature in Internet Explorer, Netscape, and most web server products.

Simple Mail Transfer Protocol (SMTP) Protocol used to transfer email messages between email servers.

Simple Network Management Protocol (SNMP) An efficient protocol for network management and device monitoring.

SNMP trap A process that filters SNMP messages and saves or drops them, depending upon how the system is configured.

Spanning Tree Protocol (STP) A protocol that prevents bridging loops from forming due to incorrectly configured networks.

Station (STA) An 802.11 capable device that supports only one 802.11 network interface, capable of establishing a Basic Service Set 802.11 network (i.e., peer-to-peer network).

static IP address A permanent IP address assigned to a node in a TCP/IP network.

subnet A portion of a network, designated by a particular set of IP addresses. Provides a hierarchy for addressing in LANs. Also called a subnetwork.

subnet mask A TCP/IP addressing method for dividing IP-based networks into subgroups or subnets (compare with maskbits). Each triplet of digits in an IP address consists of 8 bits. To specify using a subnet mask, indicate the masked bits as an IP address. To specify the subnet in maskbits, count the number of bits in the prefix. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Temporal Key Integrity Protocol (TKIP) Part of the IEEE 802.11i encryption standard, TKIP provides improvements to WEP encryption, including per-packet key mixing, message integrity check, and a re-keying mechanism.

Traffic Class Identifier (TCID) Part of the standard 802.11 frame header. The 3-bit TCID is used for mapping to class-of-service values.

Transmission Control Protocol/Internet Protocol (TCP/IP) One of the most commonly used communication protocols in modern networking. Addresses used in TCP/IP usually consist of four triplets of digits, plus a subnet mask (for example, 192.168.25.3, subnet 255.255.255.0).

Transport Layer Security (TLS) A protocol that provides privacy protection for applications that communicate with each other and their users on the Internet. TLS is a successor to the Secure Sockets Layer (SSL).

True MIMO? The Airgo Networks, Inc. implementation of the data multiplexing technique known as Multiple Input Multiple Output (MIMO). MIMO uses multiple spatially-separated antennas to increase wireless throughput, range, and spectral efficiency by simultaneously transmitting multiple data streams on the same frequency channel.

Trunk In telecommunications, a communications channel between two switching systems. In a wireless network, a trunk is a wireless connection from one Access Point to another.

Type of Service (ToS) Sometimes also called IP Precedence, ToS is a system of applying QoS methodologies, based on headers placed into transmitted IP packets.

User Datagram Protocol (UDP) A connectionless protocol similar to TCP/IP, but without the same level of error checking. UDP is commonly used when some small degree of error and packet loss can be tolerated without losing program integrity, such as for online games.

virtual LAN (VLAN) A local area network with a definition that addresses network nodes on some basis other than physical location or even whether the systems are wired together or operating using the same local equipment. VLANs are, on average, much easier to manage than a physically implemented LAN. In other words, moving a user from one VLAN to another is a simple change in software, whereas on a regular LAN, the computer or device would need to be connected physically to a different switch or router to accomplish the same thing. Network management software of some sort is used to configure and manage the VLANs on a given network.

Wired Equivalent Privacy (WEP) Security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. Uses dynamically or manually assigned keys for encryption and authentication, as dictated by the capabilities of the client station. The WEP algorithms are vulnerable to compromise; therefore, WEP security is only recommended for legacy clients that do not support the newer generation security standards.

Windows Internet Name Server (WINS) The Windows implementation of DNS, which maps IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of by IP address.

Wi-Fi A play on the term "HiFi," Wi-Fi stands for Wireless Fidelity, a term for wireless networking technologies.

Wi-Fi Protected Access Wi-Fi Alliance-sponsored security solution that addresses many of the WEP inadequacies. Originally promulgated as an interim solution, WPA is now included as part of the IEEE 802.11i standard.

wireless local area network (WLAN) A type of local area network that employs radio frequencies to transmit data (usually encrypted), much like LANs transmit data over wires and fiber optic cables.

Regulatory

FCC Certifications

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ⌚ Reorient or relocate the receiving antenna.
- ⌚ Increase the separation between the equipment and receiver.
- ⌚ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ⌚ Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment, and users must follow specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other transmitter or antenna. This equipment has been SAR – evaluated and is authorized for use in laptop and notebook computers.