

# **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

---

Contents .....	3
Preface.....	4
Overview .....	5
Device Types .....	5
Shipping Package Contents.....	5
System Requirements.....	5
Inserting and Removing the Wireless LAN Client Adapter .....	5
Checking Adapter Activity .....	6
Installing the Wireless LAN Client Adapter Driver and Client Utility .....	6
Installation Steps .....	6
Custom Installation .....	12
Uninstalling the Client Utility and Drivers .....	14
Introduction to the Client Utility.....	15
Service Set Identifiers .....	15
Wireless Bands and Channels.....	15
Client Utility Overview.....	16
Accessing the Client Utility .....	16
Using the Tray Icon .....	16
Navigating the User Interface .....	18
Default View .....	18
Networks Tab.....	22
Profiles .....	26
Monitoring Network Status.....	28
Configuration Overview .....	32
Scanning for Available Networks.....	32
Working with Profiles.....	33
Wireless Security .....	35
Regulatory.....	38
Glossary .....	39
Index .....	45

# 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 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.

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

## 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 Airgo Networks 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. Depending on the adapter configuration, it can operate in the 2.4 GHz radio frequency band or in the 2.4 and 5 GHz frequency bands and can communicate with any device that meets the compatible IEEE 802.11 standards. The Airgo product number determines the operating bands for any given adapter.

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***

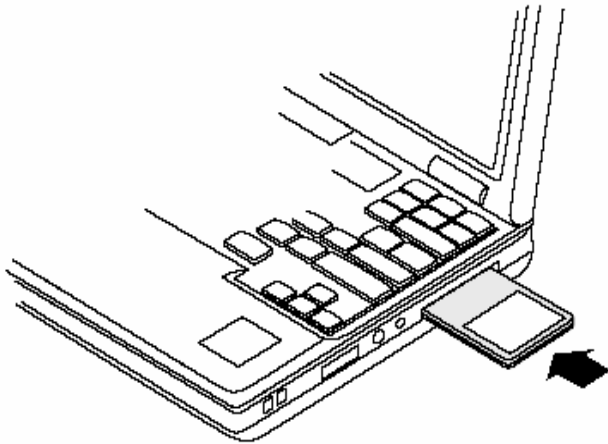
Your PC must meet the following minimum requirements:

- Windows XP SP1 or SP2 or Windows 2000 SP4
- 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 Adapter**, 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 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**

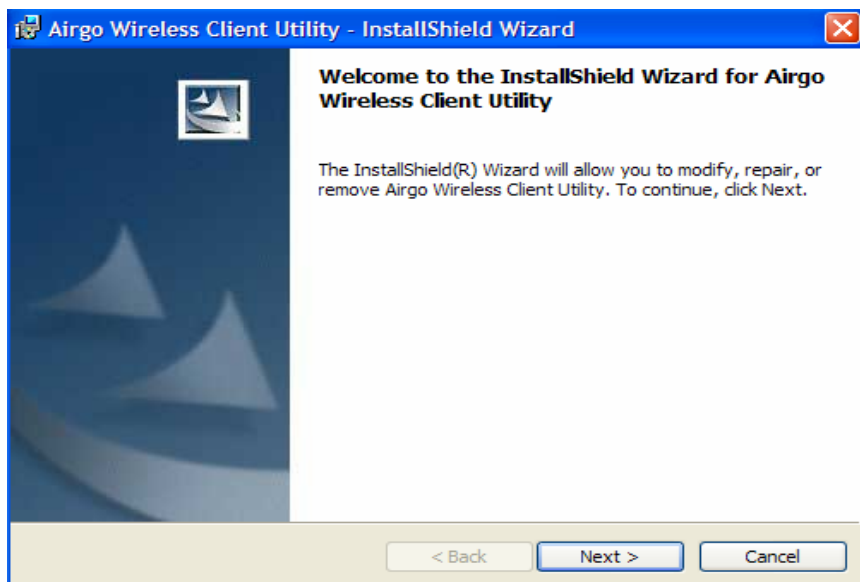
**1** Power up the computer in which the Wireless LAN Client Adapter will be installed.

**2** Insert the Wireless LAN Client distribution CD, which should automatically start the Client Utility Setup. If the wizard does not start automatically, open the CD and double-click `Setup.exe`, the Client Utility Setup opens.



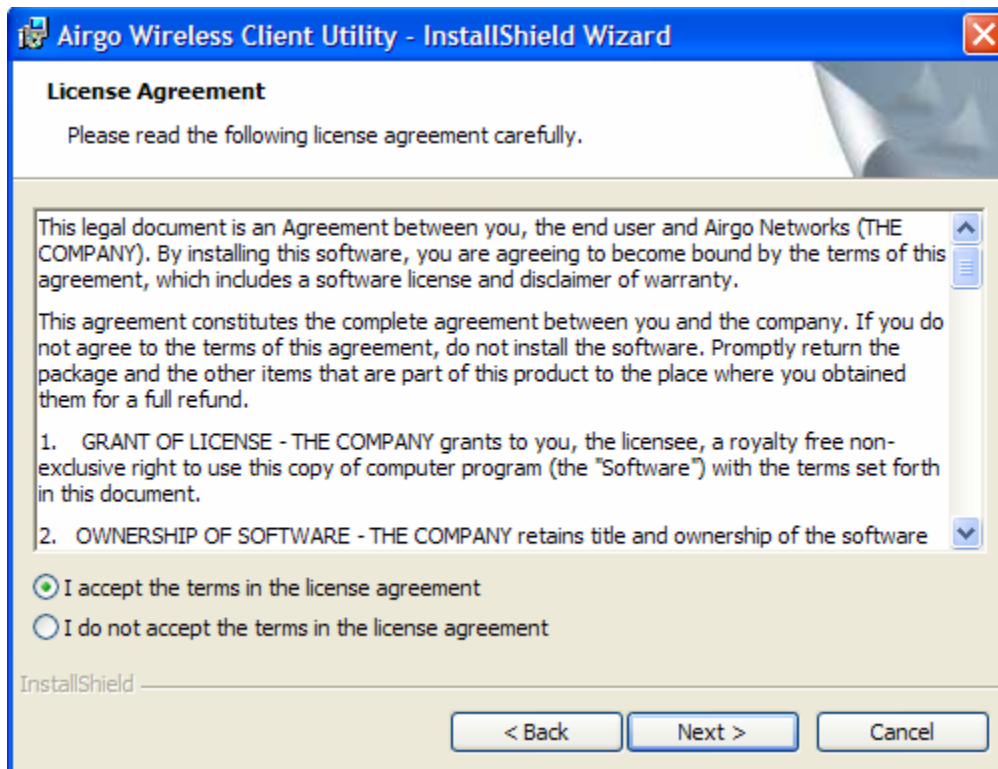
3 Click **Install Software**.

The Installation Wizard 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.



The screenshot shows the 'Customer Information' step of the 'Airgo Wireless Client Utility - InstallShield Wizard'. The window has a blue title bar with the text 'Airgo Wireless Client Utility - InstallShield Wizard' and a close button. Below the title bar, the text 'Customer Information' is displayed in bold, followed by the instruction 'Please enter your information.' The main area contains two text input fields: 'User Name:' with the placeholder text 'Your Name' and 'Organization:' with the placeholder text 'Your Organization'. Below these fields, the text 'Install this application for:' is followed by two radio button options: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for me ( )'. At the bottom of the window, the 'InstallShield' logo is visible on the left, and three buttons ('< Back', 'Next >', and 'Cancel') are on the right.

8 Click **Next**.

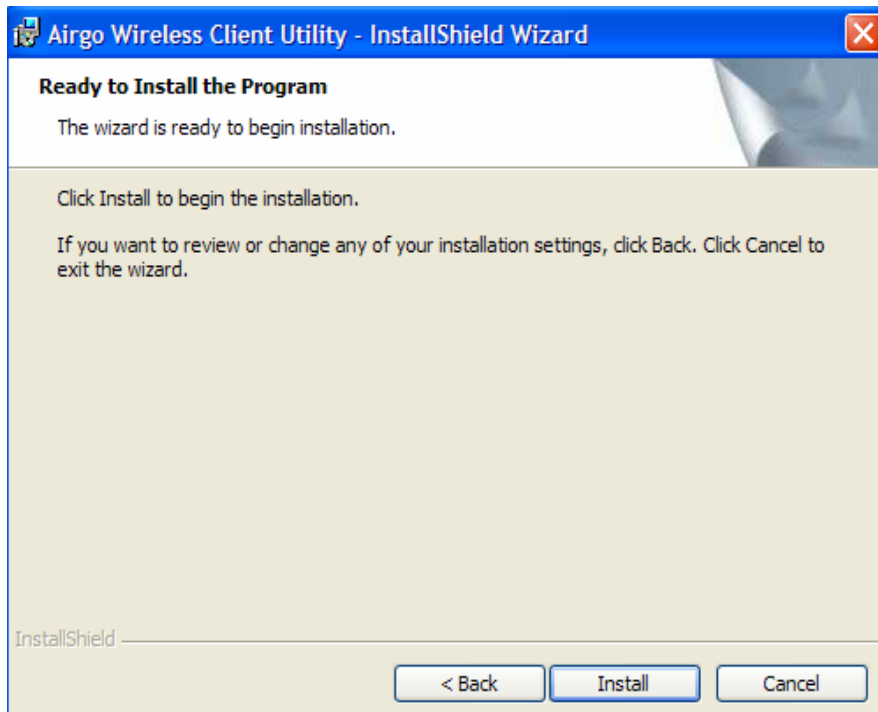
9 Accept **Complete** as the setup type.

 **NOTE:** If you select **Complete**, the software is automatically installed in the default location. To choose another location, select the Custom option; see *Custom Installation* in this chapter for additional information.

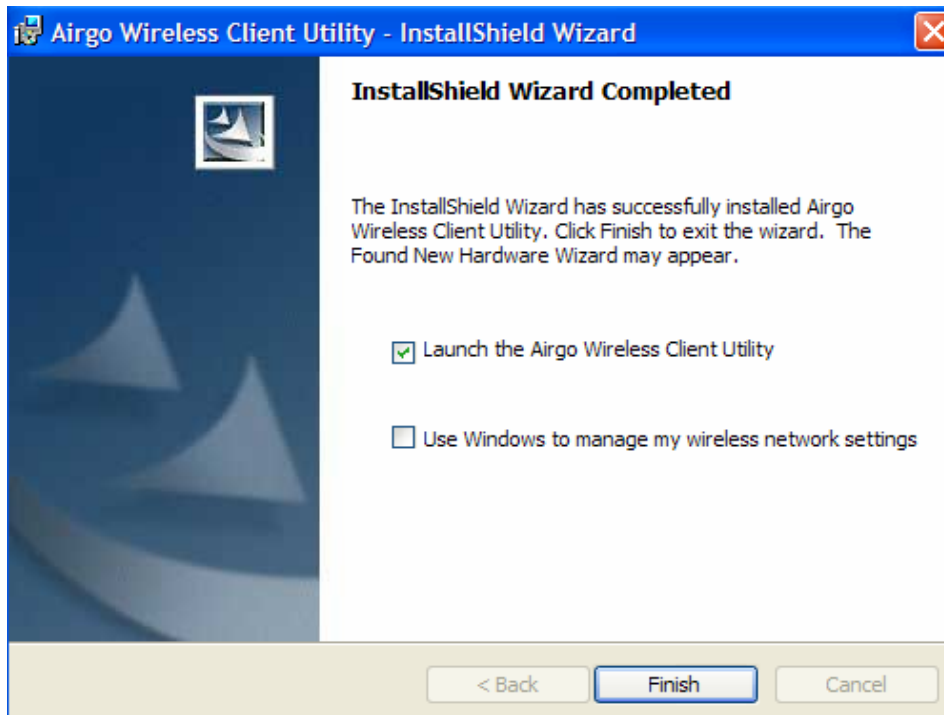
The screenshot shows the 'Setup Type' step of the 'Airgo Wireless Client Utility - InstallShield Wizard'. The window has a blue title bar with the text 'Airgo Wireless Client Utility - InstallShield Wizard' and a close button. Below the title bar, the text 'Setup Type' is displayed in bold, followed by the instruction 'Choose the setup type that best suits your needs.' The main area contains the text 'Please select a setup type.' followed by two radio button options: 'Complete' (which is selected) and 'Custom'. Each option is accompanied by a small icon of a computer monitor and a brief description: 'All program features will be installed. (Requires the most disk space.)' for Complete, and 'Choose which program features you want installed and where they will be installed. Recommended for advanced users.' for Custom. At the bottom of the window, the 'InstallShield' logo is visible on the left, and three buttons ('< Back', 'Next >', and 'Cancel') are on the right.

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 Microsoft Wireless Zero Configuration (WZC) to manage the Client Adapter.

 **NOTE:** 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 by clicking Client Utility WZC button.

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

**13** Now, insert the Wireless LAN Client Adapter.

The Found New Hardware Wizard opens.



**14** 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**.

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

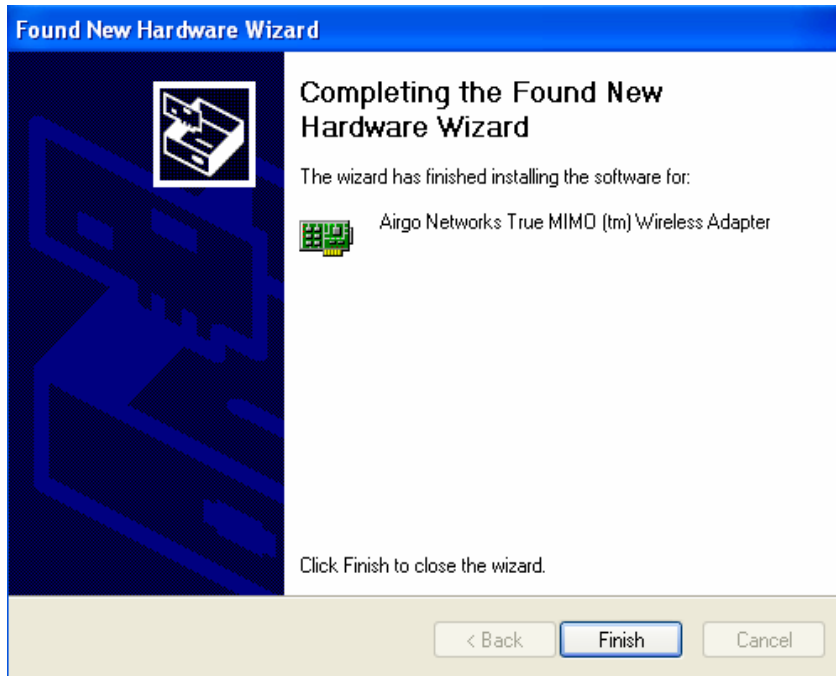
**16** Click **Next**.

**17** Should a message appear regarding Windows logo testing, click **Continue Anyway** to install the Client Adapter drivers.



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

19 Click **Finish**.

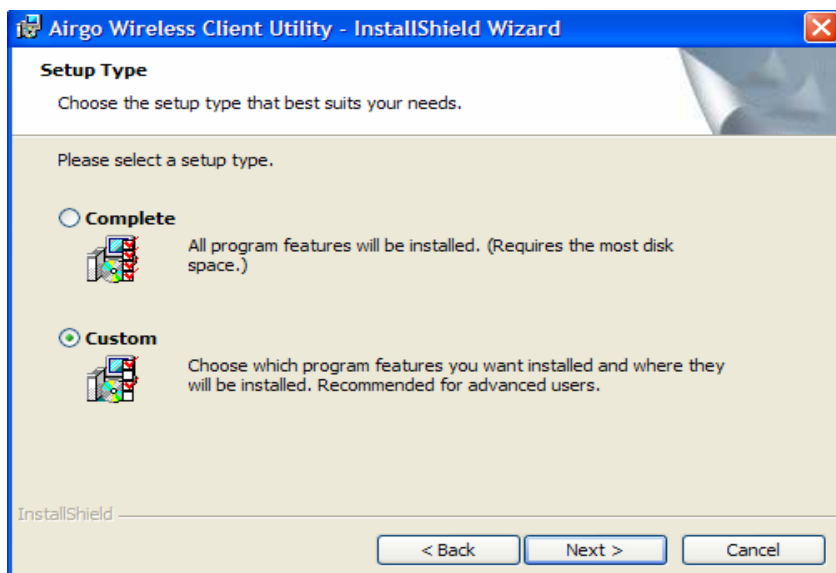


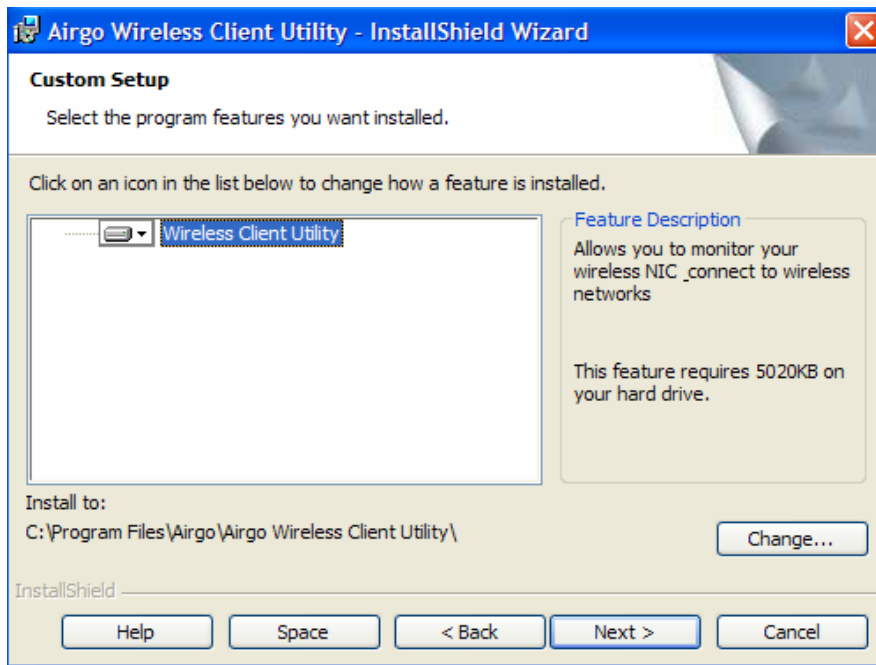
The installation is now complete. Examine the LEDs to confirm that the Client Adapter is installed and working properly. See “Inserting and Removing the Wireless LAN Client Adapter”.

## ***Custom Installation***

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

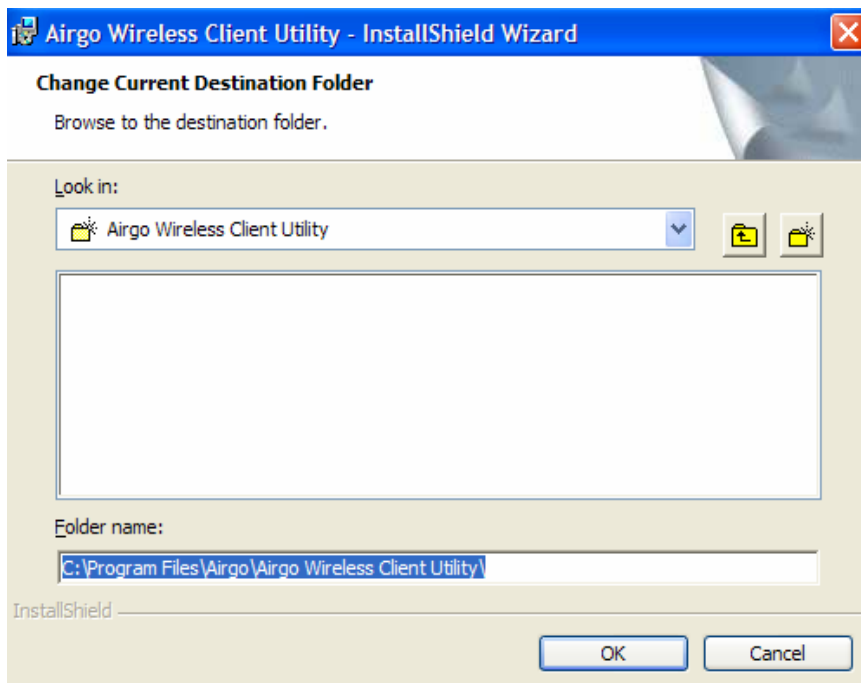
1 In the Customer Information window, select **Custom**, and click **Next>**.





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

3 Enter the path for the new location, or select a location for the pull-down “Look in:” window 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 or wish to remove the Client Utility and Client Adapter drivers from the PC system. To do so, use the Windows Add or Remove Programs utility.

To access Add or Remove Programs:

- 1** Exit the Client Utility from the icon in the system tray.
- 2** Choose **Start > Control Panel > Add or Remove Programs**.
- 3** Select the Client Utility program, and click **Remove**.
- 4** Confirm that you want to remove the program, and follow the wizard instructions for program removal.


# Introduction to the Client Utility

---

The Wireless LAN Client Adapter connects your PC to a wireless local area network (WLAN) using radio frequency signals. An access point is a wireless device that forwards data from the wired network to your WLAN equipped PC using radio frequency signals and provides network connectivity between your PC and other wireless and wired users and resources. The IEEE 802.11 standard identifies two types of wireless networking types:

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 resources on the wired network, other wireless LANs, or the Internet. This is the network type 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 one or 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 in infrastructure mode or other PCs in ad-hoc mode if those devices support the industry standard IEEE 802.11 wireless communications protocols.

## ***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 use the same SSID in order to participate in that 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)***—A 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)***—A collection of BSSs with wireless devices that can roam from one BSS to another while remaining connected to wireless network resources.

## ***Wireless Bands and Channels***

The IEEE 802.11 specification addresses wireless devices that operate in the 2.4 and 5 GHz radio frequency bands. Within each band (range of radio frequencies) individual *channels* carry a separate radio signal. Automatic and manual channel selection is provided, along with monitoring and analysis capabilities to assess the status of radio coverage and signal quality.

 **NOTE:** The WLAN Client Adapter may be limited to a single frequency band or a restricted range of radio frequencies (channels) within a frequency band depending on regulatory requirements. See the *Regulatory* section of this document for additional regulatory information.

## ***Client Utility Overview***

The Client Utility enables you to perform the following functions:

Obtain a view of your wireless network, including the type of network, the access point or ad-hoc network 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 wireless LAN adapter.

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 and signal strength indicators of this icon reflect the quality of the wireless connection:

Icon	Description
	No adapter present
	Adapter present, radio on, no association
	Adapter present, radio on, poor signal quality
	Adapter present, radio on, good signal quality
	Adapter present, radio on, excellent signal quality

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

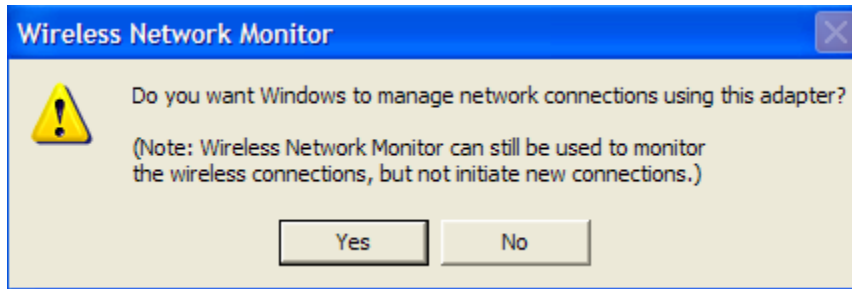




The Exit selection closes the Client Utility. Reopen the Client Utility from the Windows Start>Programs.

The Auto Connect to Best Network selection provides for auto connection to a wireless network with the highest signal strength and most appropriate security settings.

The Use Windows to Manage This Adapter selection provides for the selection of Microsoft WZC for managing the adapter. A window will appear for confirmation to allow Windows to manage the network connections for the adapter.



Click the **Yes** button to confirm.

Open the Wireless Network Monitor displays the default view for the Client Utility.



Click to close the Client Utility on the desktop. The CU is still active. To exit the CU, right click the system tray CU icon and select the Exit option or press Alt+F4 to exit the CU when the CU is on the desktop.

## Navigating the User Interface

This section explains how to use the Client Utility interface.

### Default View

The default view is the Status view. The Status view provides information about the current connection if one exists. The Client Utility will use the list of saved profiles in descending order to initiate an association. If none of the networks in the profile list are available networks, association with the Best Network will be initiated.



**NOTE:** Networks (SSIDs) in the profile list that do not have the Auto Connect option enabled will not be automatically scanned upon Client Utility initiation.



The security, network mode and Internet access is shown pictorially in the Status view. In addition, the following information is displayed:

Item	Description
Network Name (SSID)	If Status is Connected, lists the name of the network to which the Client Adapter is connected.
Network Type	If Status is Connected, indicates the type (Infrastructure or Ad-Hoc) of network association.
Authentication	If Status is Connected, indicates the security method used to authenticate this client to the network.
Encryption	If Status is Connected, indicates the security method used to encrypt information transmitted and received by this client.
Channel	If Status is Connected, lists the radio channel used for this connection.
Max Transmit Rate	If Status is Connected, indicates the current transmit rate in megabits per second (Mbps) for this connection.
AP Beacon Name	If Status is Connected, lists the name of the AP transmitted in Beacon frames, if name is supported by the AP, to which the Client Adapter is connected, when the Network Type is Infrastructure. For an ad-hoc network type, this field will always be blank.
AP Radio MAC	If Status is Connected, lists the Media Access Control (MAC) address of the WLAN device to which the Client Adapter is associated.
IP Address	If Status is Connected and an Internet Protocol (IP) address has been assigned either dynamically by a DHCP server or statically by manual input, the IP address is listed here in dotted decimal format.
Signal Strength	If Status is Connected, the strength of the wireless connection is shown in decibels per meter (dBm) where the more negative the number, the lower the signal strength (power of the radio signal).

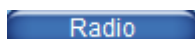
In addition to the Status tab, there is a tab for viewing available wireless networks (Networks tab), for creating profiles (Profiles tab) for association to networks that are commonly accessed by the client adapter, and for determining the health and performance of the current connection (Diagnostics tab).

In addition to the four selection tabs, there are four buttons: Radio, Auto-Connect, WZC and Help. These buttons are toggles for the functions they affect.

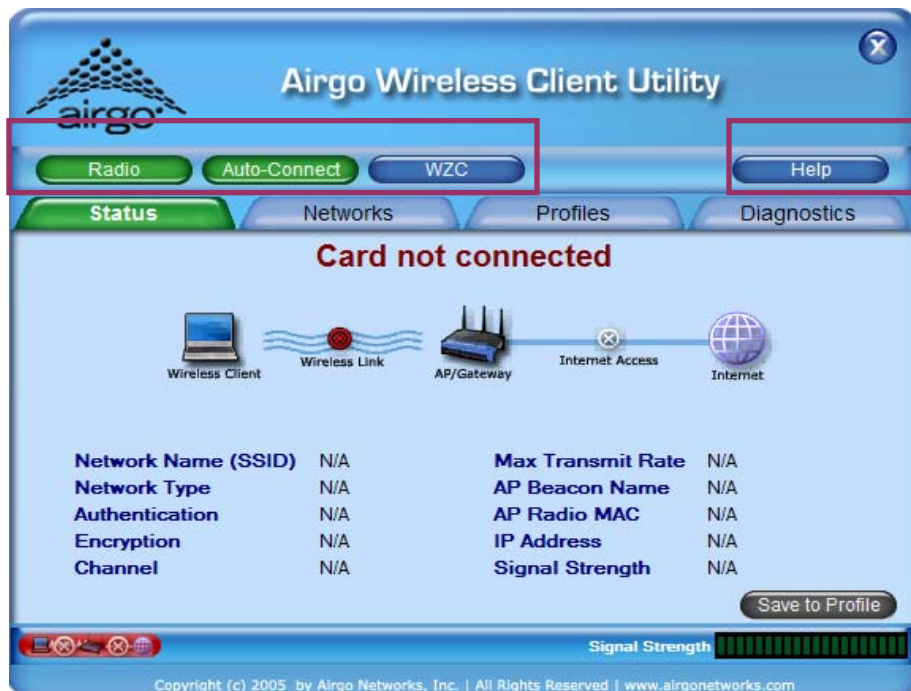
**Radio** The Radio button toggles the state of the radio from on to off or off to on. The transition from on to off and off to on requires a few seconds. The color change in the Radio button will indicate the transition as follows:



The Radio is in the ON state.



The Radio is in the OFF state.

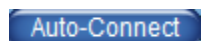


## Auto-Connect

The Auto-Connect button can be used to force an association to the previously connected network or to the “best” network currently available or can be set to the off or disabled state.



Auto-Connect is in the enable/on state. Connection to the previously connected network or to the “best” network currently available will occur automatically.



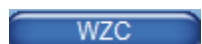
Auto-Connect is in the disabled/off state. Connections will not be established automatically.

## WZC

The WZC button toggles the management of the network connection between WZC and the Client Utility (Windows XP only).



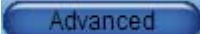
Microsoft Windows Wireless Zero Configuration is currently managing the network connection.



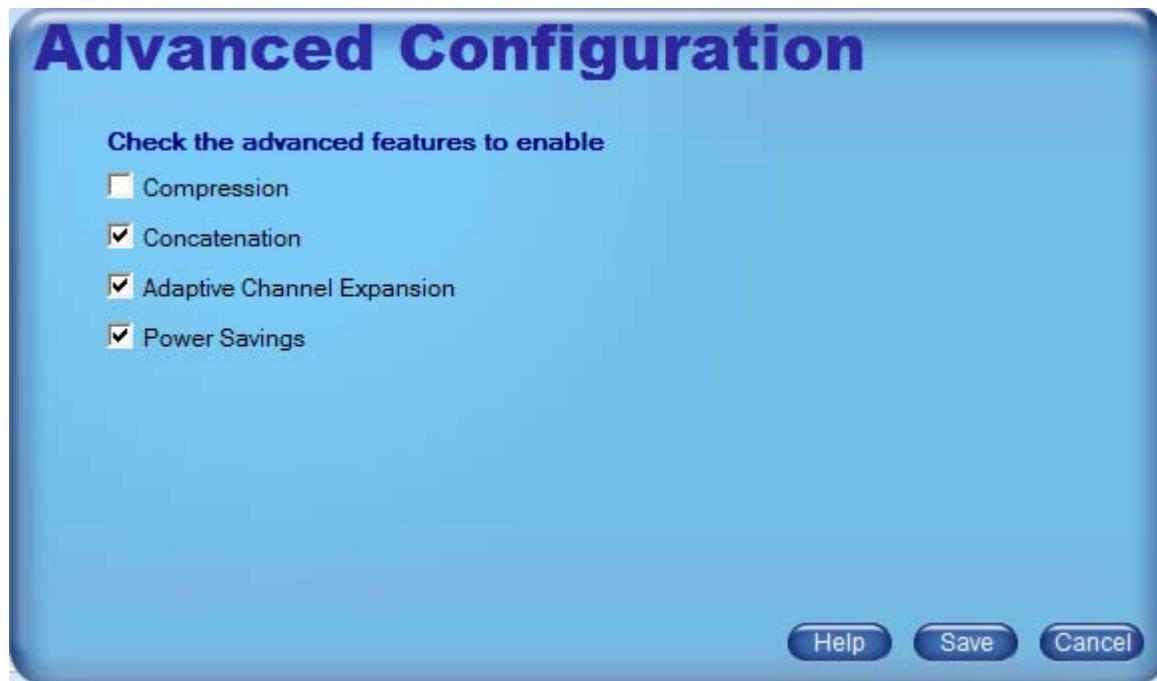
The Client Utility is currently managing the network connection.

## Help

The Help button provides context sensitive help for the current page. All help files can be printed. All help pages can be resized during viewing.

For AGN3xx based adapters an additional  tab will appear between the WZC and Help tabs.

Provides configuration options for the following:




**Compression**—provides real-time hardware data compression which increases data throughput using pre-compressed frames with no impact on host processor. OFF by default.


**Concatenation**-- provides for the merging of data from several packets into one which increases throughput by removing overhead due to inter frame spacing and preambles. The performance benefit is in enhancing throughput at higher data rates. ON by default.

**Adaptive Channel Expansion**-- provides increased data rates by increasing the RF bandwidth. The existing 20 MHz bandwidth is increased to 40 MHz by combining adjacent channels. Driver includes support for data rates up to 240 Mbps:

- ◆ 802.11b: 1, 2, 5.5, 11 Mbps
- ◆ 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- ◆ Airgo True MIMO: Single Channel--24, 36, 40, 42, 48, 72, 80, 84, 96, 108, 120, 126 Mbps. Channel Expansion--48, 72, 80, 84, 96, 144, 160, 168, 192, 216, 240 Mbps.

**Power Savings**—provides battery life savings by powering off adapter components during periods of idle network activity. OFF by default.




Above the Copyright notice on the left is a Link Status area . Moving the mouse over this area will display the status in a text box. The Link Status area shows whether a connection has been established to the AP/Gateway, and if so, the type of connection (either Infrastructure or Ad-hoc), whether a connection has been established to the Internet, and whether the connections are secure. The image changes with the current status. The Link Status area is visible in each view.

On the right, the Signal Strength Indicator  shows incremental signal strength where each segment is equal to 5% of the maximum of 100% signal strength.

There are additional functions and indicators available in the default view. The Save to Profile button in the bottom right of the Status view creates a profile with the properties of the current connection. The new profile will appear in the Profiles view.

Networks Tab

The Networks tab lists all the networks within radio range of your Client Adapter. The Networks view provides information about the networks available for association.


Item	Description
 Infrastructure	Network Type Icons
 Secured Infrastructure	
 Ad-Hoc	
Network Name (SSID)	The name of each of the networks within radio range.
Signal	The relative signal strength as a percentage.
Security	The security method enforced for each of the networks.
Channel	The channel number and 802.11 physical mode (a/b/g) of each network.
QoS	Quality of Service capability advertised by each network.
	The currently associated network appears colored.

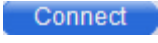





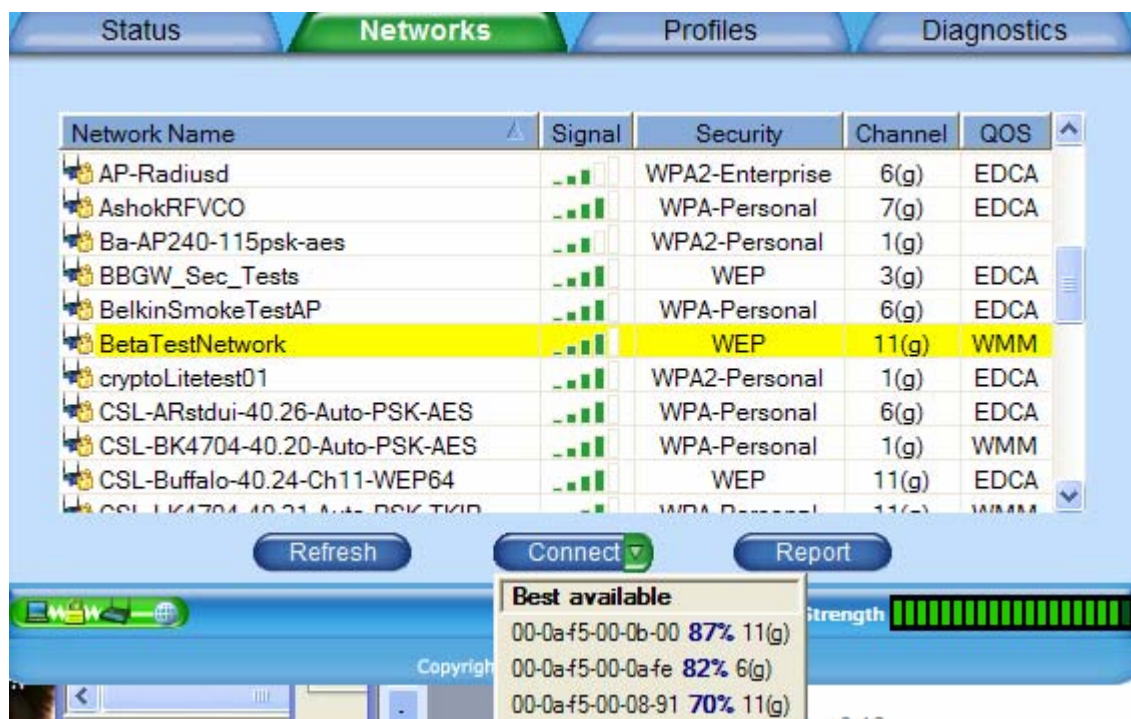
Any of the following operations can be performed on the Networks list:

Item	Description
Refresh	Causes the Client Adapter software to immediately scan for all the wireless networks within radio range. Detected networks are presented in the Networks list.
Connect	Opens appropriate security dialog boxes as necessary and attempts association with the selected SSID.
Report	Generates a color coded list of networks within radio range including the network SSID, BSSID(s), Security Mode, Support Rates, Basic Rate Set, Channel Mode, Network Type, Advertised Country Code, Advertised Channels and Maximum Output Power, True MIMO capability and Signal Strength as a percentage. The report generated can be resized, printed, saved and copied to the clipboard.
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.

Clicking the  button will cause the Client Utility to scan for available networks.

Highlighting a particular network and clicking the  button will cause initiation of a connection to that network which, depending on the network parameters, may invoke the configuration dialog boxes for security parameters, etc.

When there is more than one radio (BSSID) for a given SSID, the connect button will have a selector arrow on the right hand side . Clicking on the selector arrow will provide a list of all radios (BSSIDs) their signal strength, channel and mode for the select SSID (Network Name).



Any of the BSSIDs may be selected. By default the BSSID with the best signal strength will be selected.

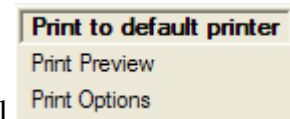
**NOTE:** The selection of a specific AP within an SSID (e.g. a BSSID) may prevent access to network-wide resources in a mobile environment.

Clicking the **Report** button will generate a report for all of the networks in the Networks list. The report can be resized while viewing. Report information contains:

Report Information	
Item	Description
SSID	Network Name of each of the networks in radio range.
BSSID	MAC addresses of the radios belonging to the SSIDs within radio range.
Security	Security mode (WEP, WPA/WPA2 Personal, WPA/WPA2 Enterprise, or Disabled) for the BSSID.
Supported Rates	All data rates supported by each BSSID.
Basic Rates	Minimum data rates supported by each BSSID.
Channel Mode	Radio channel and IEEE 802.11 physical mode (a/b/g) for each BSSID.
Type	Network type (Infrastructure or Ad-Hoc) of each BSSID.
Country	International Standards Organization (ISO) two character Country Code advertised by each BSSID.

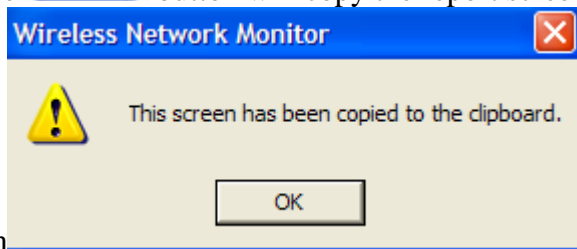


Item	Description
Channels	Advertised operating channels and maximum output power for each BSSID. <sup>1</sup>
True MIMO	Use of enhanced, True MIMO, data rates (Yes or No).
Signal %	Strength of the radio signal, as a percentage.




Clicking the selector arrow  on the Print button provides several print selections.

Clicking the  button will copy the report screen to the clipboard with an accompanying

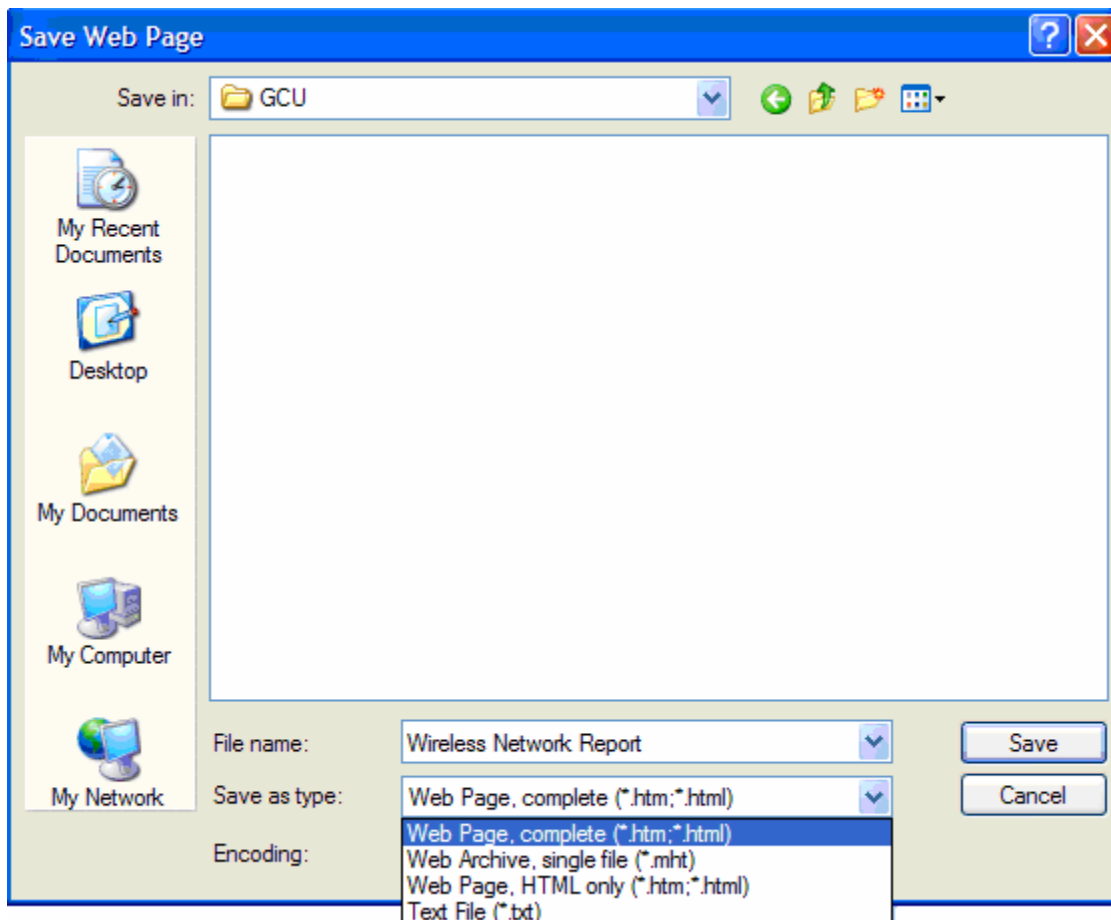


notification. Click OK to continue.

Clicking the  button will allow the report to be saved to a file. There are several options for saving the report file, including location, file name, file type and file encoding:

---

<sup>1</sup> The available channels are governed by regulatory law. The client adapter contains an ISO country code programmed into EEPROM which defines the operational channels for a given regulatory domain.



Clicking the  button closed the Network report.

## Profiles

The Profiles tab shows all the networks (SSIDs) for which a network profile is defined. Any of the following operations can be performed in the Profiles tab view:

Item	Description
New	Click New to open the Create Connection Profile dialog box which launches the Profile Wizard.
Modify	To change information in an existing profile, highlight an entry and use the arrows at the bottom of the list to move the entry up or down.
Import	Click Import to add profile configuration information from an external source. The .cfg profile exported is a text file that can be edited with any text editor.
Item	Description
Export	Click Export to save profile configuration information as an external .cfg file. Each profile is saved as a separate file in the selected location with a file name the same as the profile name and a file type of cfg.
Delete	Click Delete to eliminate a profile.

The icons adjacent to the Profile name indicate auto connect and connection state for the profile.

Icon      Description

**This Profile is the active profile.**





Auto Connect is enabled for the profile.



Auto Connect is disabled for the profile.



The up  and down  arrows move the selected profile up or down in the profile selection list. SSIDs in profiles at or near the top of the list which have auto connect enabled are scanned for before other SSIDs in the ordered profile list.

The remaining area on the Profiles tab displays read-only information about the profile and its settings:

Profile Details	
Item	Description
Network Type	The network type (Infrastructure or Ad-Hoc) for profile.
Authentication	The security method used to authenticate this client to the network for this profile.
Encryption	The security method used to encrypt information transmitted and received by this client using this profile.
Access Point	The BSSID for this profile. The Client Utility provides for association to a specific Access Point within an SSID. <b>NOTE:</b> The selection of a specific AP within an SSID (e.g. a BSSID) may prevent access to network-wide resources in a mobile environment.
Auto Connect	The profile Auto Connect option is checked by default for each profile. To disable this option, click the checkbox. When the Auto Connect option for a profile is disabled (unchecked), the network (SSID) for this profile will not be automatically scanned for nor connected with when the Client Utility is launched.

## Monitoring Network Status

Once a profile is activated and you are associated to the selected network, the Status tab presents status of the connection and the Diagnostics tab shows performance, client health and client software information.

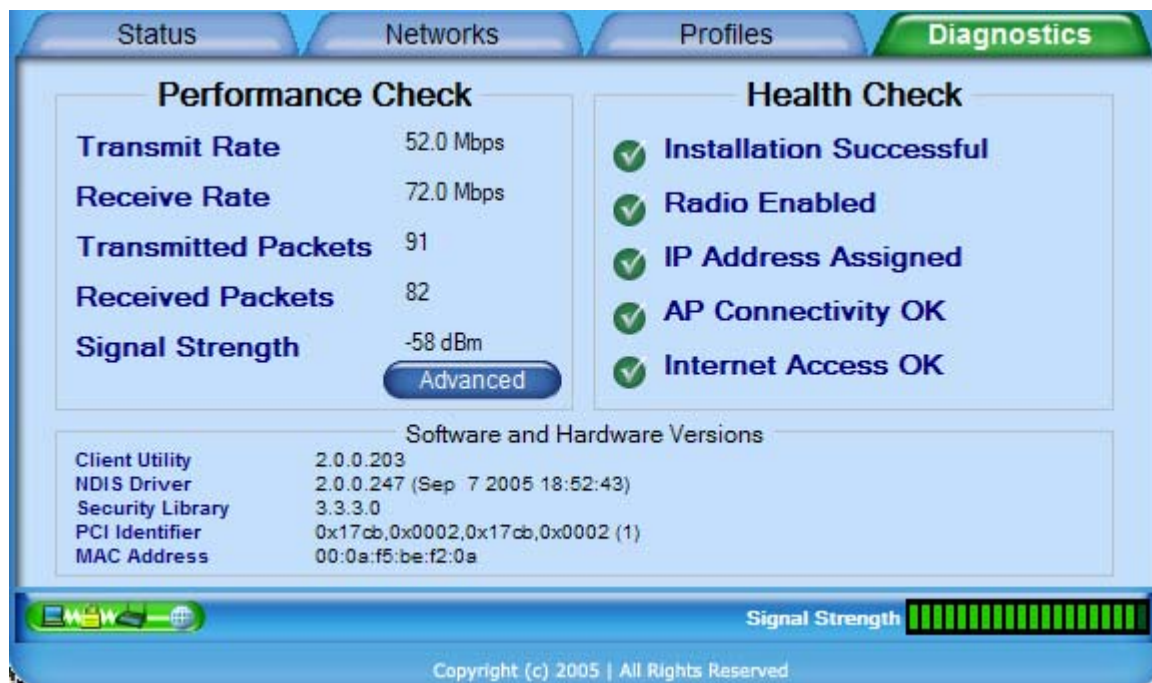
Performance	
Item	Description
Transmit Rate	The rate at which data was last being transferred from this client adapter. Beacons are always sent at 6 Mbps.
Receive Rate	The rate at which data was last being received from this client adapter. Beacons are always received at 6 Mbps.
Transmitted Packets	The cumulative number of packets of data transmitted since the driver was loaded onto this client adapter.
Received Packets	The cumulative number of packets of data received since the driver was loaded onto this client adapter.
Signal Strength	The strength of the wireless connection in decibels per meter (dBm) where the more negative the number, the higher the signal strength (power of the radio signal).

Health	
Item	Description
Installation Successful	The status of the client adapter driver and client utility.
Radio Enabled	The status of the radio on the client adapter.
IP Address Assigned	The status of IP address assignment.
AP Connectivity OK	The status of an infrastructure connection (an AP found and associated for the SSID or BSSID).
Internet Access OK	The status of an internet connection for the active wireless connection (successful ping to www.google.com).



Versions	
Item	Description
Client Utility	The version of the Client Utility that is currently managing the network connection.
NDIS Driver	The version of the client adapter driver that is currently loaded on the adapter.
Security Library	Version of the Meetinghouse Aegis Security library.
PCI Identifier	The Vendor ID (PID/SVID) and System ID (SID) of the client adapter.
MAC Address	The MAC address of the wireless client adapter.

For AGN3xx based adapters an additional **Advanced** button is available in the Performance Check section to display advanced statistics.



The advanced button provides the following tabular information:

Advanced Statistics	
Statistic	Value
TransmittedFragmentCount	100
MulticastTransmittedFrameCount	101
FailedCount	102
RetryCount	103
MultipleRetryCount	104
RTSSuccessCount	105
RTSFailureCount	106
ACKFailureCount	107
FrameDuplicateCount	108
ReceivedFragmentCount	109
MulticastReceivedFrameCount	110
FCSErrorCount	111
TKIPLocalMICFailures	112
TKIPICVErrors	113
TKIPCounterMeasuresInvoked	114
TKIPReplays	115
CCMPFormatErrors	116
CCMPReplays	117
CCMPDecryptErrors	118
FourWayHandshakeFailures	119
WEPUndecryptableCount	120
WEPICVErrorCount	121
DecryptSuccessCount	122
DecryptFailureCount	123
ReceivedBeaconCount	200
TransmitFrameCount	201
ReceivedFrameCount	202
ReceivedFrameErrorCount	203
AuthenticationTimeout	204
AuthenticationRejects	207
AssociationTimeout	206

Close






# Configuration Overview

---

The Client Utility uses profiles to store connection parameters defining how your Wireless LAN Client Adapter associates to a wireless network. Each profile contains information about the target network including type of network connection and security settings.

To make it easy to connect to wireless networks at home, office, or wireless hotspot locations, the Client Utility allows you to create multiple profiles, each profile contains information about a different network and its set of configuration values. When you move from one location to another, your Client Adapter automatically detects the currently available network(s) and applies the correct profile. The Profiles tab on the Client Utility contains an entry for each profile.

The following rules apply when connecting to a wireless network:

-  The Client Utility always attempts to connect to the last successfully connected network. If that network is not available, then the utility attempts to connect to a network with a configured profile, in the order in which the profiles are listed.
-  If there are no previously configured profiles, or if it is not possible to connect to any currently configured networks, the Client Adapter attempts to connect to an 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 or double click that network from the Available Networks tab. Clicking Save to Profile on the Connection tab will make this network available for automatic connection in the future.

## ***Scanning for Available Networks***

Upon driver load, the Client Adapter scans for all networks within radio range and attempts to connect to one of them based on previously created profiles with auto-connect enabled. It associates to the first network 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 SSID/BSSID to which you are connected is a trusted component of your network.

Whenever the Client Utility is opened, an automatic scan is performed. You can also scan for networks on demand, at any time.

To scan for available networks:

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

This sequence displays the application icon in the system tray.

Right click and select Open Wireless Network Monitor.

The Client Utility will open to the default view (Status); select the Networks tab and click the Refresh button. Subsequent closing and reopening of the Client Utility from the system tray will return the Client Utility to the last open view.



## ***Working with Profiles***

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

To utilize an available network to create a profile, double click that network from the Networks tab, a prompt for security information, if required, will appear.

Use the Connect button to associate to that selected network. When the connection is complete, click the Save to Profile button on the Status tab to save the parameters of this connection in a profile for future use.

When ever a profile is created or modified from the Profiles tab, the Profile Wizard will prompt for the following configuration parameters:

Field	Description
Profile Name	The name to be associated with this profile. This will also be used as the filename should this profile be Exported to a .cfg file.
Network Name (SSID)	Service Set Identifier (SSID) is a name that uniquely identifies a wireless local area network. Each device in the wireless network must use the same SSID in order to participate in a cohesive wireless network.
Network Type	<p>The Network Type indicates the type of wireless network.</p> <p>Infrastructure—Refers to a wireless network in which clients associate to access points or broadband gateways which usually interface to a wired local or wide area network, for Internet and email access, file sharing, and print and other services.</p> <p>Ad-Hoc—Refers to wireless network in which clients associate with each other, typically on a temporary basis and usually without a wired local or wide area network connection.</p>
BSSID	BSSID of specific AP/Gateway to connect to. Default is “Best available” which is the one with the highest signal strength.
Channel	<p>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. The Profile Wizard presents a channel selection<sup>2</sup> if the Network Type selected was Ad-Hoc.</p>
Network Mode	<p>If the Network Type selected was Ad-Hoc, in addition to selecting a radio channel on which the ad-hoc network will communicate, one or more of the IEEE 802.11 physical layer modes which include 802.11a, 802.11b and 802.11g needs to be selected. The valid network mode(s) for the client adapter is shown in the network mode pull-down list.</p>

---

<sup>2</sup> Channel selection is governed by regulatory law.

The authentication and encryption settings provide options for configuring a secure connection between your PC and the wireless network. The following security options are configurable when using the Client Utility:  
Disabled—No authentication or encryption.

WEP (Wired Equivalent Privacy)—64 or 128-bit key based encryption.

WPA-Personal (Wi-Fi Protected Access)—Passphrase/PSK based authentication with TKIP encryption and AES encryption for forward compatibility.

WPA2-Personal—Passphrase/PSK based authentication with AES encryption and TKIP encryption for backward compatibility.

## Security

WPA-Enterprise—RADIUS server based authentication using PSK and IEEE 802.1x; with TKIP encryption and AES encryption for forward compatibility.

WPA2-Enterprise—RADIUS server based authentication using IEEE 802.1x/EAP with AES encryption and TKIP encryption for backward compatibility.

RADIUS (Remote Authentication Dial-In User Service)—Server based authentication using EAP TLS, or EAP TTLS, or EAP PEAP with no encryption.

See the *Wireless Security* section in this document for additional background information on wireless security options and guidelines for security settings in the enterprise, small office, and home environments.

### Encryption

WEP encryption based on shared WEP keys. The keys are 64-bit or 128-bit and must be specified in hexadecimal (base-16) format.

### WEP Key

#### 64-bit WEP requires:

10 hexadecimal digits including the characters A-F and 0-9 or  
5 valid ASCII characters.

## WEP

#### 128-bit WEP requires:

26 hexadecimal digits including the characters A-F and 0-9 or  
13 valid ASCII characters.

### Tx Key

Select from one of 4 Tx (transmit) encryption keys. The Tx encryption key of choice is typically provided by the network administrator.

### Authentication

Auto—System determined Open or Shared.

Open—No authentication.

Shared—Authentication based on a WEP key exchange.

**Encryption**

**WPA/****WPA2-****Personal**  
**PSK**  
**WPA-Personal** requires the support of TKIP (Temporal Key Integrity Protocol) as an encryption method. This client utility and driver also support AES (Advanced Encryption Standard) as a WPA-Personal encryption method.  
**WPA2-Personal** requires the support of AES as an encryption method. This client utility and driver also support TKIP as a WPA2-Personal encryption method.

**Authentication**

Passphrase—Enter the pre-shared key required for network access.

**Encryption**

**WPA-Enterprise** requires TKIP (Temporal Key Integrity Protocol) as an encryption method. This client utility and driver also support AES (Advanced Encryption Standard) as a WPA-Enterprise encryption method.

**WPA2-Enterprise** requires AES as an encryption method. This client utility and driver also support TKIP as a WPA2-Enterprise encryption method.

**WPA/****WPA2-**  
**Enterprise**  
**(RADIUS**  
**server required)**

**Authentication Method**

Authentication using EAP TLS, or EAP TTLS, or EAP PEAP requiring certificates which must be maintained in the authentication server and supplicant.

**Login Name**

Network login provided by your network administrator.

**Certificate**

Select the security certificate that has been installed on this PC to provide server authentication for this network name (SSID).

**Authentication Method**

Authentication using EAP TLS, or EAP TTLS, or EAP PEAP requiring certificates which must be maintained in the authentication server and supplicant.

**RADIUS**

**Login Name**

Network login provided by your network administrator.

**Certificate**

Select the security certificate that has been installed on this PC to provide server authentication for this network name (SSID).

## ***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 provides a mechanism for protecting data transferred across the wireless link from eavesdropping. *Authentication* provides a mechanism so that the identity of your PC or your identity, or both, are confirmed so that you may gain access to the network.

## Authentication

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 some Access Points to extend the management and scalability features of centralized management to administrators in small-to-mid sized office environments.

## Encryption

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 enhancement for legacy systems.

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

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

The most effective encryption/authentication 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 does the WEP standards. WPA has progressed through two generations of encryption technology to date, with AES being the

latest and most effective. TKIP is the encryption protocol that was first introduced with WPA, but it provides less comprehensive 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 can be specified in hexadecimal (numeric) or ASCII format.

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-F).

Example: 64-bit: *55772abbcc* ; 128-bit: *12340987afcb45677fdc789045*

ASCII characters must be 5 (64-bit) or 13 (128-bit) characters in length.

# 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.

# 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.

## **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.

# Index

---