



# **Installation and User Guide**

## **WFB400 Windows Wireless LAN Client Adapters**

Copyright © 2007 by QUALCOMM, Inc. 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

---

<b>CONTENTS .....</b>	<b>3</b>
<b>PREFACE .....</b>	<b>4</b>
<b>OVERVIEW .....</b>	<b>6</b>
<i>Device Types.....</i>	<i>6</i>
<i>Shipping Package Contents.....</i>	<i>6</i>
<i>System Requirements.....</i>	<i>6</i>
<i>Inserting and Removing the Wireless LAN Client Adapter.....</i>	<i>6</i>
Checking Adapter Activity .....	7
<i>Installing the Wireless LAN Client Adapter Driver.....</i>	<i>7</i>
Installation Steps.....	7
<i>Confirming the Installation.....</i>	<i>9</i>
Verifying the Installation — Windows XP .....	10
<i>Uninstalling the Windows Wireless Drivers.....</i>	<i>12</i>
<b>INTRODUCTION TO WIRELESS ZERO CONFIGURATION.....</b>	<b>14</b>
<i>Service Set Identifiers.....</i>	<i>14</i>
<i>Wireless Bands and Channels.....</i>	<i>14</i>
<i>WZC Overview.....</i>	<i>15</i>
<i>Accessing WZC.....</i>	<i>15</i>
<i>Wireless Security.....</i>	<i>18</i>
<b>CONFIGURATION OVERVIEW .....</b>	<b>20</b>
<b>REGULATORY .....</b>	<b>22</b>
<b>GLOSSARY .....</b>	<b>23</b>
<b>INDEX .....</b>	<b>29</b>

# Preface

---

This guide explains how to install and configure the Windows 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 Qualcomm WFB/WFR4xxx-based Windows Wireless LAN Client Adapters 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 (CardBus) adapter for use in laptop and notebook computers
- PCI Express (PCIe) miniCard adapter for use in laptop computer PCIe minCard expansion slots
- USB (Universal Serial Bus) adapter for use in laptop, notebook and desktop computers.

This guide assumes that the PC used with Qualcomm WFB/WFR4xxx-based Windows Wireless LAN Client Adapters is configured to support Microsoft Wireless Zero Configuration (WZC)<sup>1</sup>. 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 Windows Wireless LAN Client Adapter and explains how to install it.

*Chapter 2* provides an overview of Microsoft Wireless Zero Configuration

*Chapter 3* describes configuration settings available through Microsoft Device Manager Advanced Properties Page

*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).

---

<sup>1</sup> For information about WZC see the Microsoft Webpage at:  
[http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wlan\\_client\\_configure.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wlan_client_configure.mspx?mfr=true)

## **Related Documentation**

The information related to the Qualcomm wireless networking product line (WLAN) is available on the company website, <http://www.cdmatech.com/products/wlan.jsp>.

# Overview

---

The Qualcomm Windows Wireless LAN Client Adapters provide 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 Qualcomm 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

## *Device Types*

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

- **PC Card** — Extended Type II PCMCIA CardBus (32-bit interface) for use in laptop and notebook computers.
- **PCI Express (PCIe)** — PCIe miniCard adapter for use in laptop computer PCIe minCard expansion slots. PCIe minCard adapters are installed by factory personnel when the PC system is configured by the PC manufacturer. For PCIe minCard adapter information, consult your PC manufacturer's documentation.
- **USB** — Universal Serial Bus version 2.0 for use in laptop, notebook, and desktop computers.

## *Shipping Package Contents*

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

- Wireless LAN Client Adapter
- CD containing the device driver

## *System Requirements*

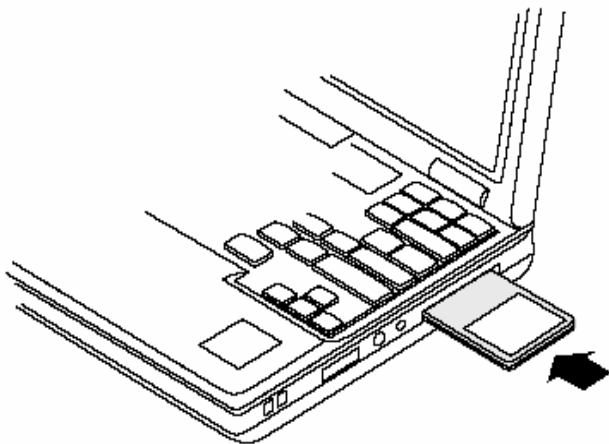
Your PC must meet the following minimum requirements:

- Windows XP SP2
- 128 MB memory
- CPU 750 MHz or greater
- At least 10 MB disk capacity available for the driver 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*

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

## Installation Steps

- 1) If you are using a PCIe miniCard<sup>2</sup>, make sure that it is physically installed in your computer (see “Device Types” section above **Error! Bookmark not defined.**). If you are using the PC card, slide it into the CardBus slot on your computer.
- 2) Power up the computer.

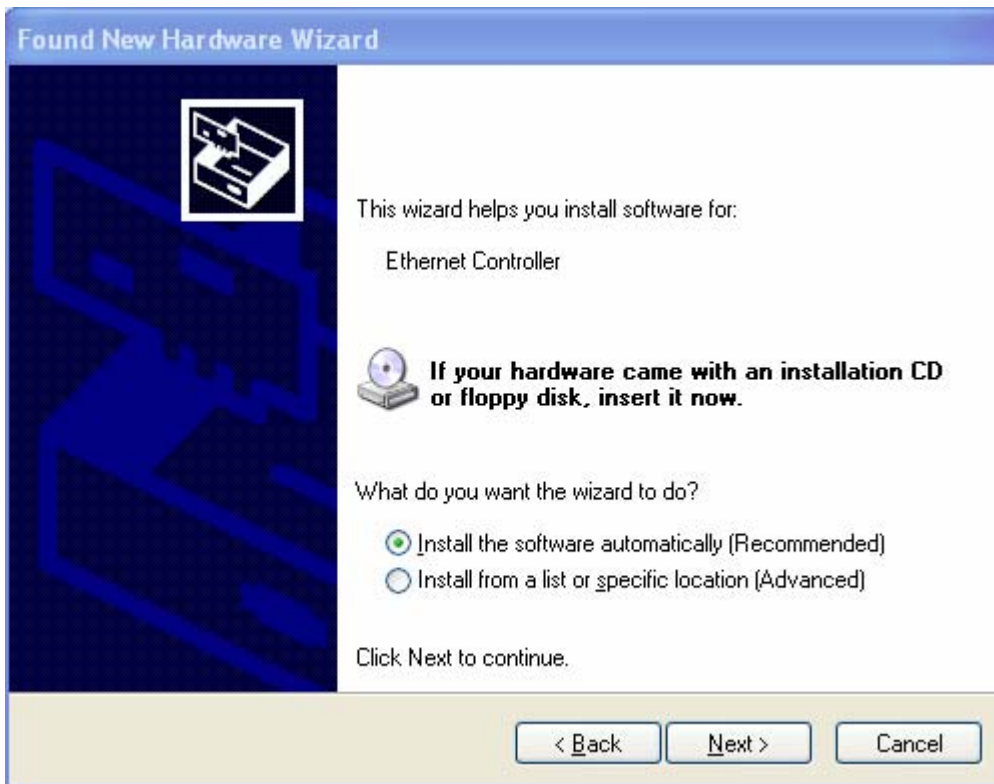
The Found New Hardware wizard opens and prompts you to insert the installation CD into your computer.

---

<sup>2</sup> PCIe minCards and appropriate drivers will have been installed by the PC manufacturer.



- 3) Insert the Qualcomm Network Driver CD into the CD drive on your computer; click the “No, not this time” radio button and click **Next**.





- 4) Click Next to have the driver software automatically installed from the CD.

The wizard locates the driver software on the CD. A warning may appear regarding compatibility testing. Click **Continue Anyway**



The system prompts you to wait while the driver is installed. The system copies the driver files onto your computer and then displays the Installation Complete screen.



- 5) Click **Finish** to complete the installation.

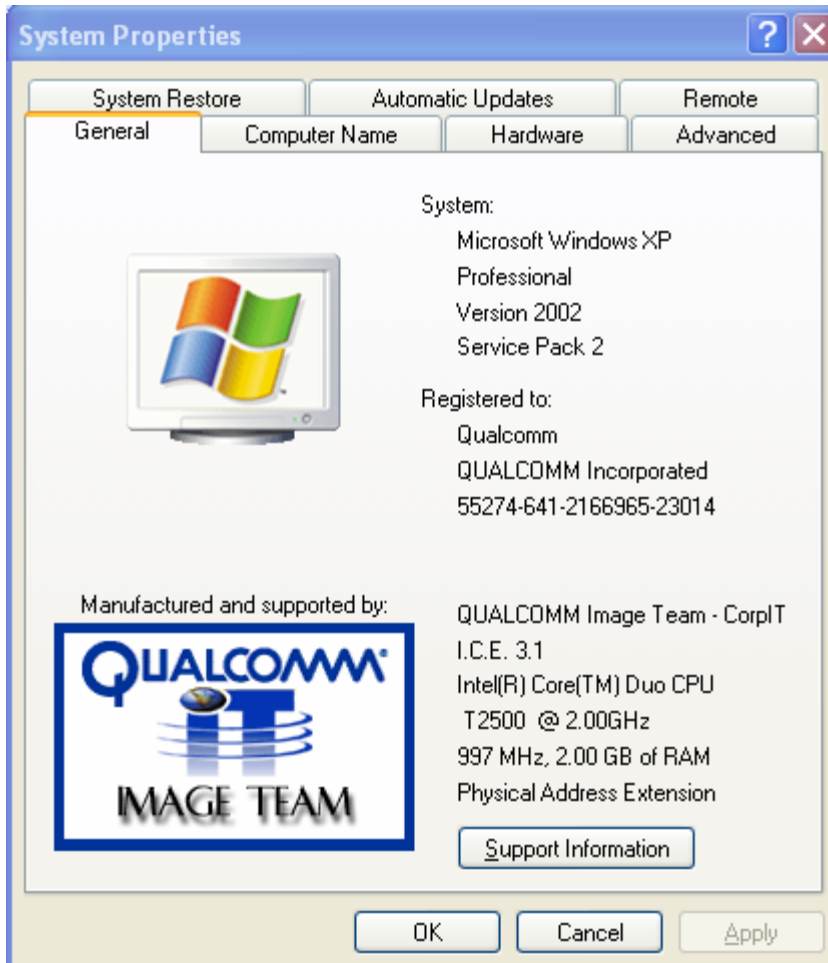
### ***Confirming the Installation***

After you have installed the Qualcomm Airgo Wireless LAN Client Adapter, confirm that the system recognizes it.

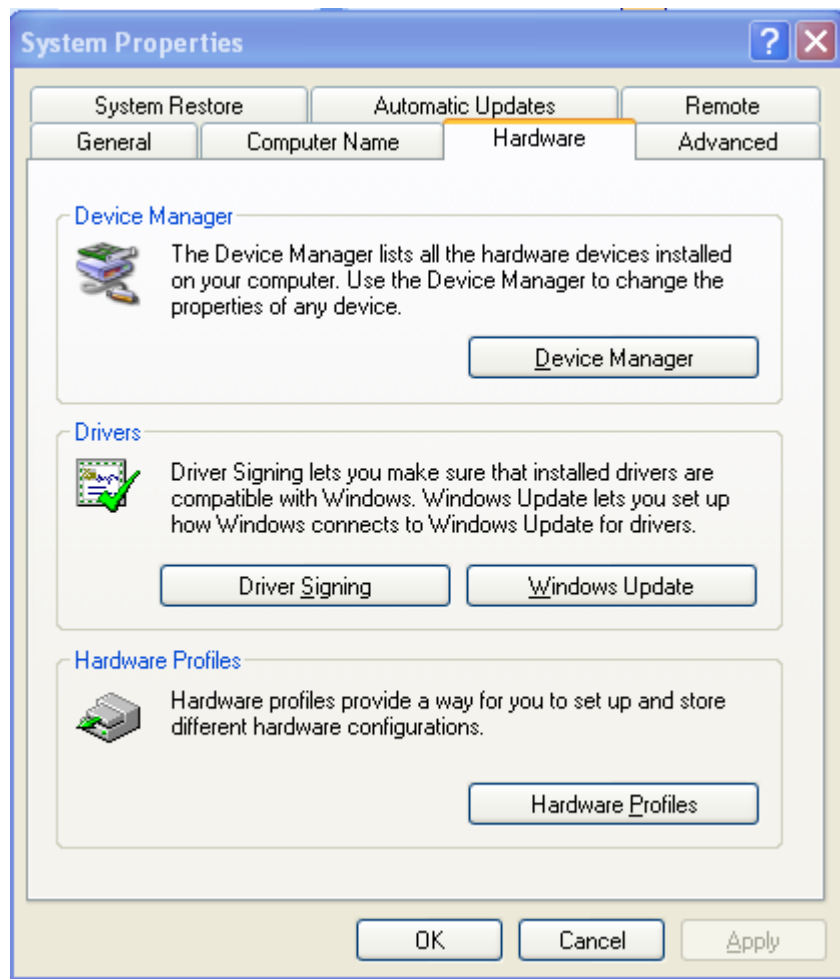
## Verifying the Installation — Windows XP

Open the Properties window in the Control Panel:

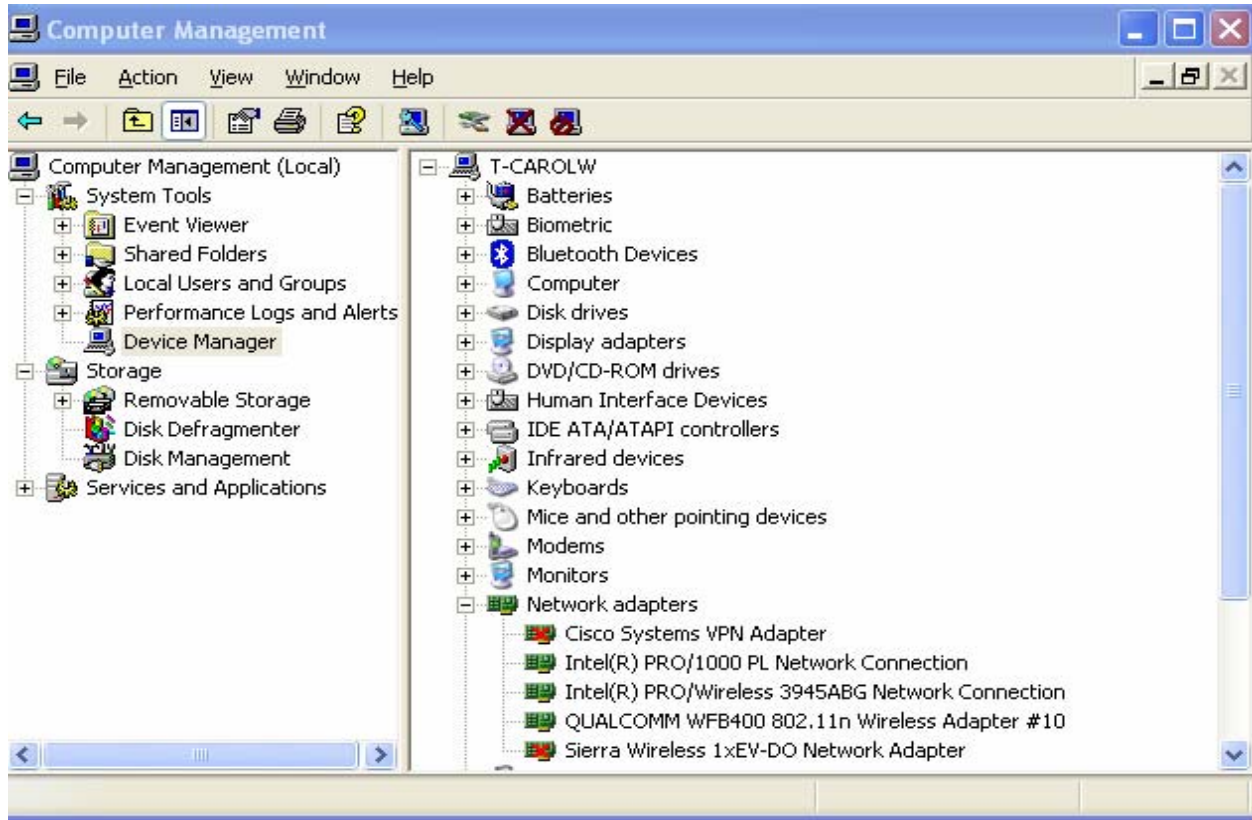
- 1) From the Start menu, select **Control Panel**.
- 2) Select **System** to open the System Properties window.




- 3) Select the Hardware tab.



4) Click the Device Manager Button.



- 5) Click the + sign to expand the Network adapter listing. Confirm that the QUALCOMM WFB400 802.11n Wireless Adapter is listed without a red X icon or yellow exclamation mark.

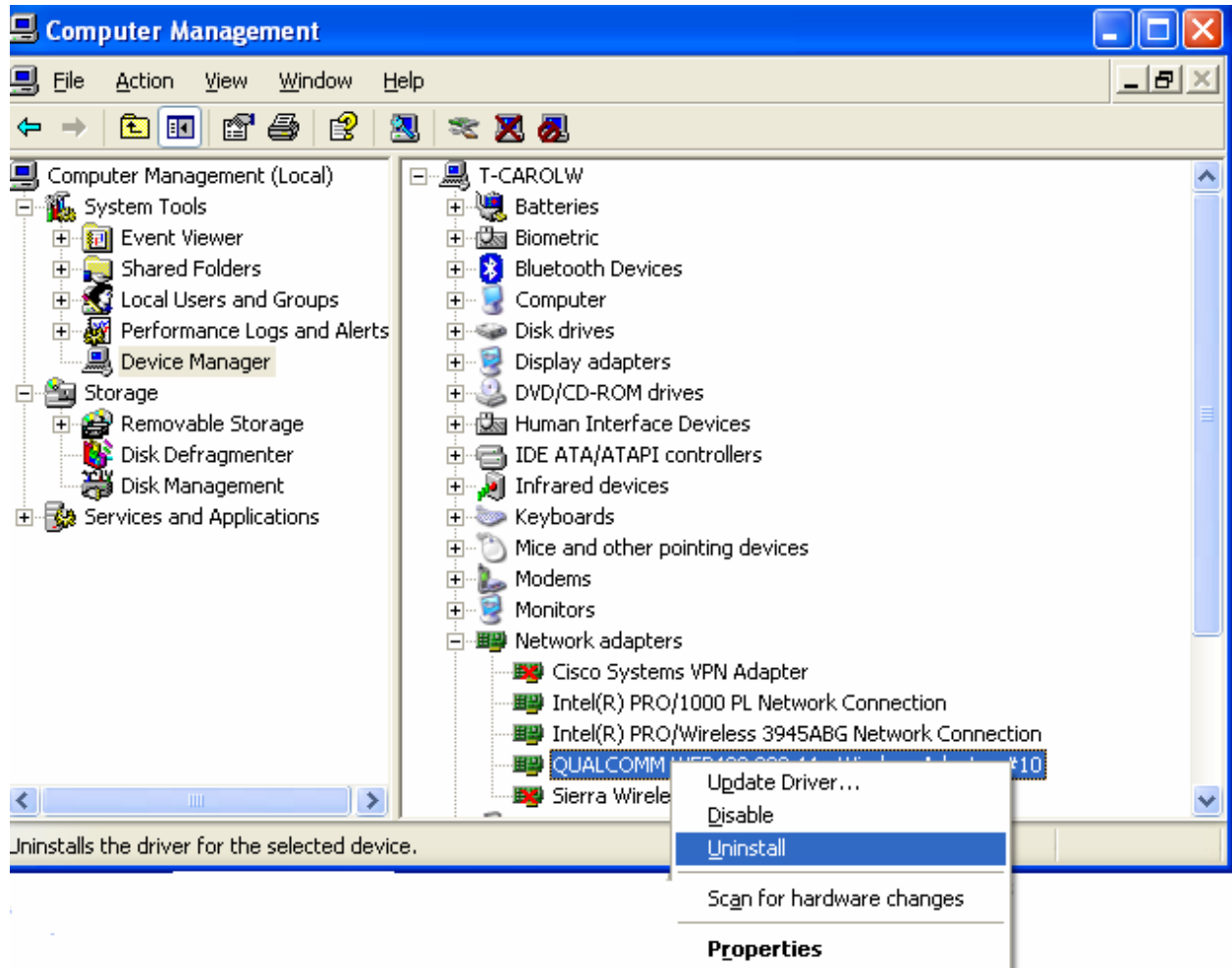
 **NOTE:** If you see the red **X** or yellow exclamation mark icon, contact your network administrator or technical support..

- 6) Double-click **QUALCOMM WFB400 802.11n Wireless Adapter** to open its Properties window. Confirm that the Device Status area displays the message “Device is working properly.”

Driver installation verification is now complete.

## ***Uninstalling the Windows Wireless Drivers***

Uninstall the Client Adapter drivers from the PC system. To do so, use the Windows Device Manager Uninstall feature.



# Introduction to Wireless Zero Configuration<sup>3</sup>

---

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.

---

<sup>3</sup> Wireless Zero Configuration (WZC) is a trademark of Microsoft.

**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.

## ***WZC Overview***

WZC enables you to perform the following functions:

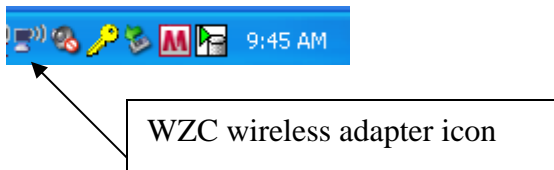
Obtain a view of the wireless networks within radio range, including the security mode of the wireless network, the signal strength of the wireless network and the wireless network with which you are associated.

Scan (Refresh Network List) and connect to wireless networks within radio range of your wireless LAN adapter.

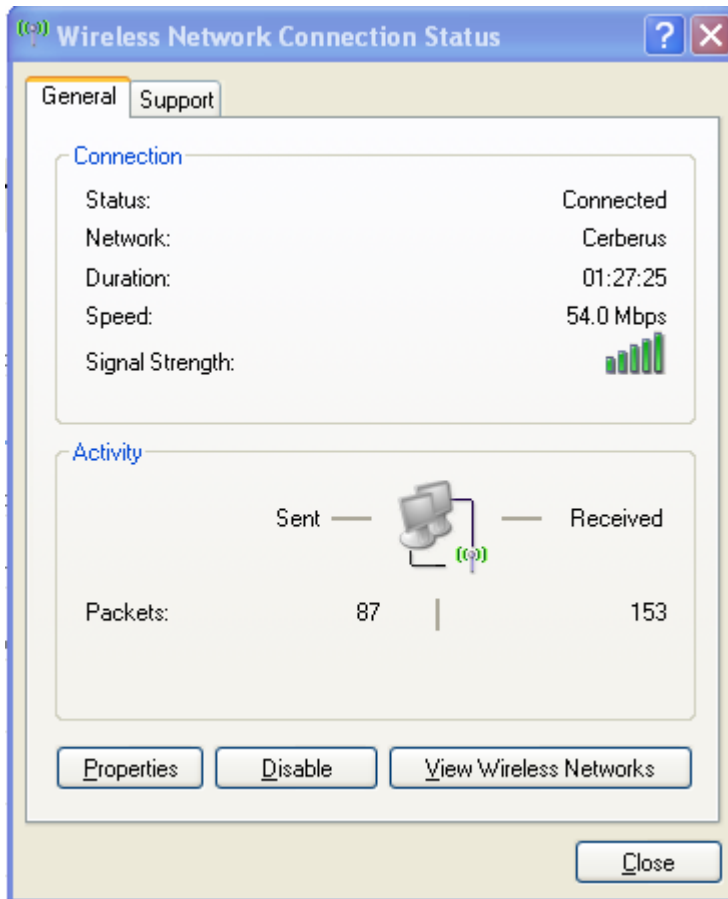
Create or select a profile, which stores the specifics of the network connection and security selections for your Wireless LAN Client Adapter.

## ***Accessing WZC***

Typically, the default setting for network adapters is to have a wireless icon appear in the system tray which typically appears in the right bottom corner of the Windows XP display:



Double clicking on this icon will cause the display of the Wireless Network Connection Status page.



Click on the View Wireless Networks button to view the available Wireless Networks and to configure Network and related tasks.

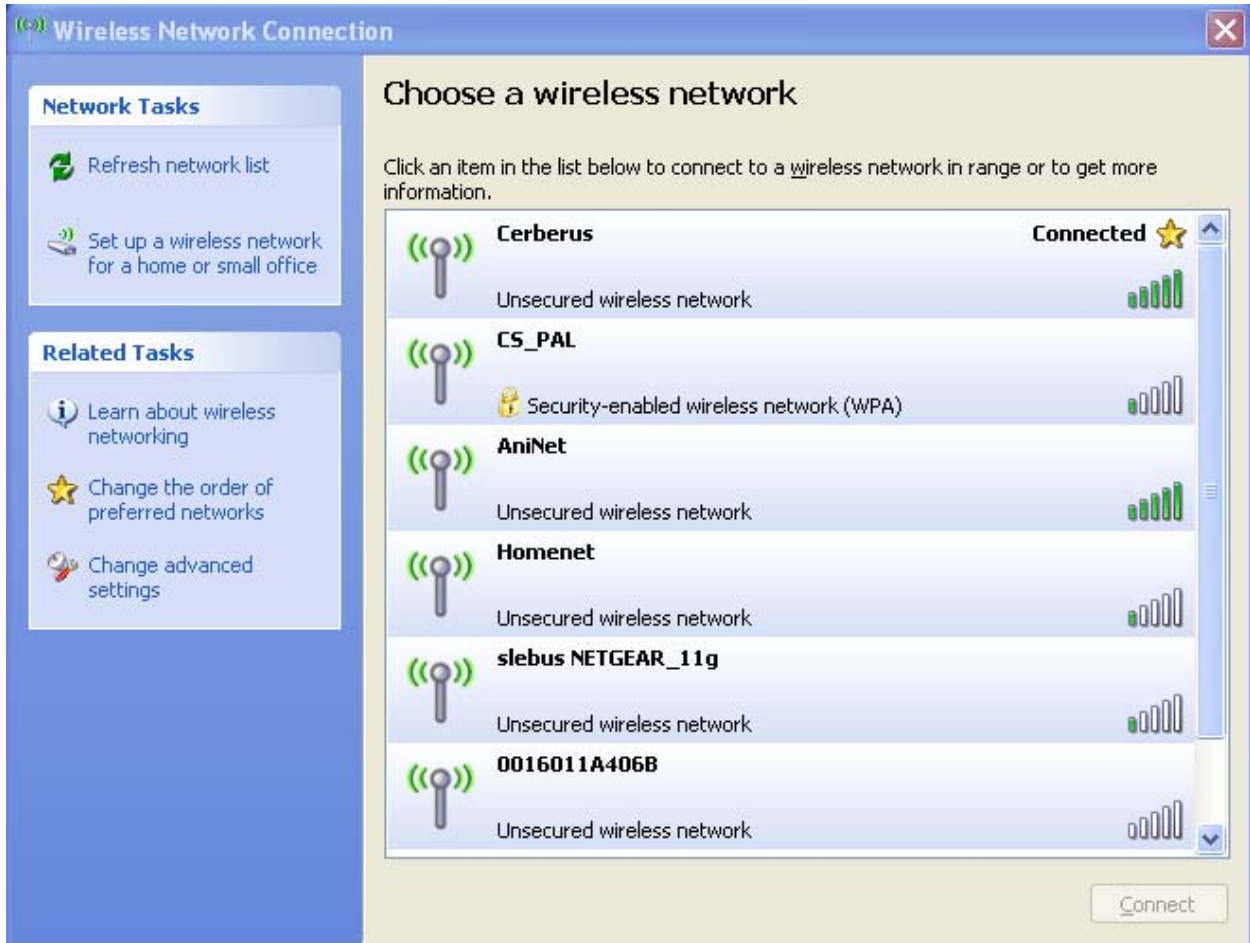
Network Tasks that can be performed with WZC include refreshing the available networks list and setting up a home or office wireless network. Related tasks include a tutorial on wireless networking as well as changing the order of preferred networks and configuring advanced settings<sup>4</sup>.

The wireless networks within radio range are shown graphically on the WZC Wireless Network Connection page. The graduated signal bars show the relative radio signal strength of the wireless network. Indication is also given

---

<sup>4</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. For operation in countries governed by FCC regulations, operation in the 5150-5250 MHz band is limited to indoor use.





Double clicking on an unsecured network within radio range will initiate an association with that network. Clicking on a secured network within radio range will cause a network key page to appear. See the Wireless security section below for more information on wireless security.



## ***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.

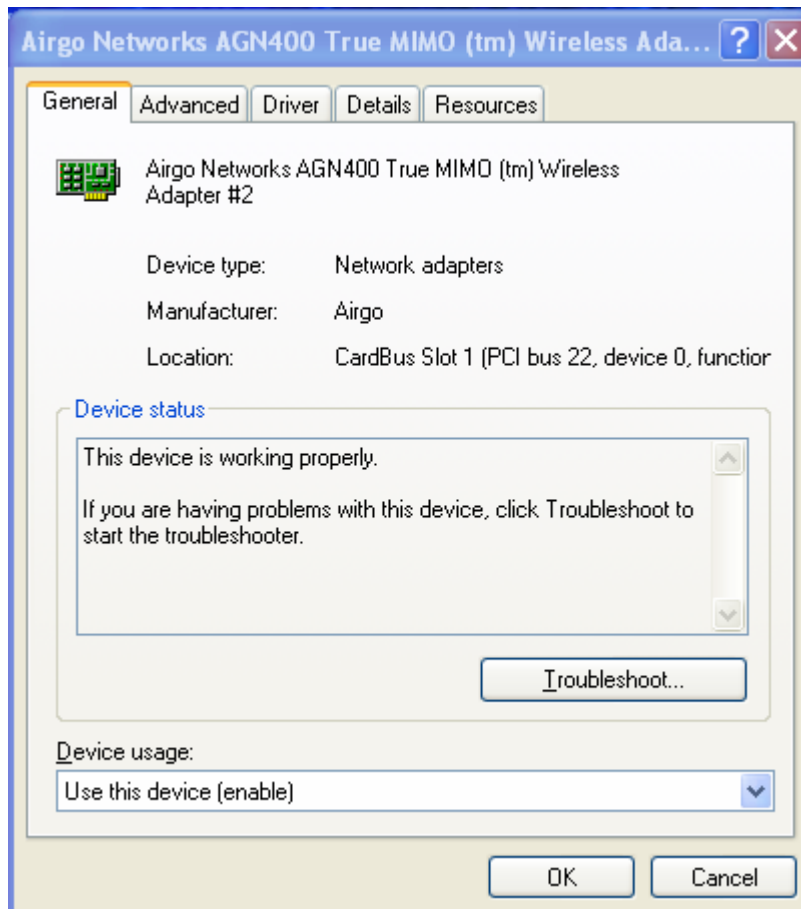
The most effective encryption/authentication methods are part of the WPA (Wi-Fi Protected Access) cipher suite and are recommended for all environments in which security is an important consideration, whether in the enterprise, small office or home. WPA provides much more complete protection against 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.

# Configuration Overview

Advanced settings can be configured through the Microsoft Advanced Properties page. The Advanced Properties page is launched by selecting the Change advanced settings on the Wireless Network Connection page.



Select the Advanced tab. The following advanced properties can be configured:

- 802.11 Mode
- 802.11d Support
- 802.11 e Support
- 802.11n High Throughput
- Adaptive Channel Expansion
- Background Scanning Period
- Compression
- Enhanced Rates

- Fragmentation Threshold
- LongRetryLimit
- Network Density
- RTS Threshold
- ShortRetryLimit
- Transmit Power
- Transmit Rate
- Wi-Fi Multimedia (WMM) Support

Defaults for each of these IEEE 802.11 parameters have been chosen to maximize the WFB/WFR4xxx wireless client experience.

# 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.

# 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 Qualcomm 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

---