

# **WLAN 802.11 b/g Embedded Module**



## **User Manual**

**(DRCM-81)**

**Version: 1.0**

**Nov. 2005**

## **Copyright Statement**

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the prior writing of the publisher.

Windows<sup>™</sup> 98SE/2000/ME/XP are trademarks of Microsoft<sup>®</sup> Corp.

Pentium is trademark of Intel.

All copyright reserved.

## **Contents**

<u>FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT .3</u>	
<u>FOR OEM INTEGRATORS.....4</u>	
<u>HARDWARE INSTALLATION &amp; ANTENNA INFORMATION.....5</u>	
<u>1. INTRODUCTION .....8</u>	
<u>1.1 THE WLAN 802.11G .....8</u>	
<u>1.2 FEATURES .....8</u>	
<u>2. PLANNING YOUR WIRELESS NETWORK .....9</u>	
<u>2.1 WLAN .....9</u>	
<u>2.2 AD-HOC AND INFRASTRUCTURE .....9</u>	
<u>3. SOFTWARE INSTALLATION AND UNINSTALLATION..... 11</u>	
<u>3.1 SETUP WIZARD INSTALLATION ..... 11</u>	
<u>3.2 ADDITIONAL SETUP PROCESSES..... 15</u>	
<u>3.3 UNINSTALLATION..... 16</u>	
<u>4. USING IEEE802.11G WLAN UTILITY ..... 17</u>	
<u>4.1 OVERVIEW ..... 17</u>	
<u>4.2 ACCESSING THE CONFIGURATION UTILITY ..... 17</u>	
<u>4.3 LINK STATUS..... 18</u>	
<u>4.4 CONFIGURE PROFILE ..... 19</u>	
<u>4.5 SITE SURVEY..... 23</u>	
<u>APPENDIX A: GLOSSARY .....24</u>	

## **Federal Communication Commission Interference Statement**

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 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.

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.

### **Information**

To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## **For OEM integrators**

This device is intended only for OEM integrators under the following conditions:

- 1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
- 2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as the 2 conditions above are met, further transmitter testing will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

**IMPORTANT NOTE:** In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

### **End Product Labeling**

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example Notebook PC, access points, routers, wireless ASDL modems, and similar equipment). The final end product must be labeled in a visible area with the following: "Contains TX FCC ID: NKRDRCM".

### **Manual Information That Must be Included**

The users manual for end users must include the following information in a prominent location "IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

### **Additional Information That Must be Provided to OEM Integrators**

The end user should NOT be provided any instructions on how to remove or install the device.

The module is for OEM installation only and can not be sold to end user directly.

## Hardware Installation & Antenna Information

- Module is installed in the Personal Computer, located on the bottom side of the Personal Computer.
- Antennas are embedded in the two sides (see the two antennas shown below)



### **Only the antenna types listed below can be used:**

Antenna 1: Dipole (Model: F1B-204406-52, made by Long-Chu Co.)

Antenna 2: Dipole (model: C478-510028-A, made by Wha Yu Co.)

### **Important Note:**

This module is restricted to mobile configuration. The antennas of module should be installed and operated with minimum distance 20cm between the radiator and all persons. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The end user should NOT be provided any instructions on how to remove or install the device.

The module is for OEM installation only and can not be sold to end user directly.

## \*Caution !!

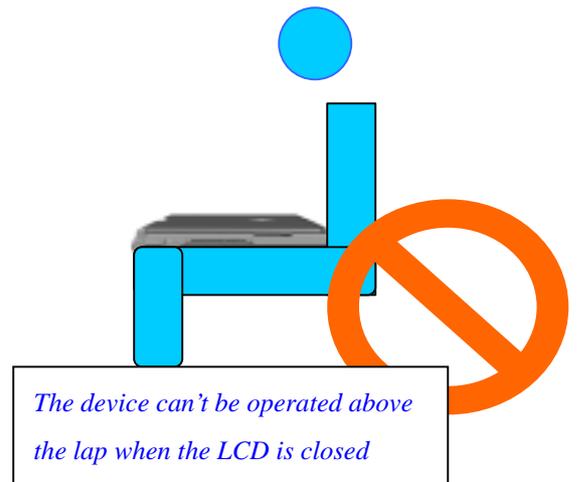
(1). This module cannot be bound in a tablet computer for RF exposure issues.

(See label 1)

(2). Due to the RF exposure issues, this module can be used in a laptop computer in normal operation, but cannot be used when it is put above the lap and the LCD screen is in the closed position. (See label 2)



**Label 1**



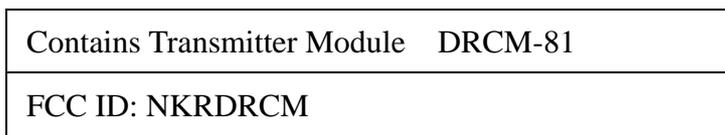
**Label 2**

**(3). This module must be labeled with FCC ID. (See label 3)**



**Label 3**

**(4). If the FCC ID is not visible when the module is installed inside another device, then the outside of device must also display a label referring to the enclosed module. The exterior label can be “ Contains Transmitter Module FCC ID:NKRDRCM ” or similar wording. (See label 4)**



**Label 4**

***Please put Label 3 & Label 4 to the enclosure of end product to note the end user.***

## **1. Introduction**

### **1.1 The WLAN 802.11g**

802.11g is a 54Mbps wireless networking standard that's almost five times faster than the widely deployed 802.11b products found in homes, businesses, and public wireless hotspots. Because both 802.11b and 802.11g share the same 2.4GHz radio band, 802.11g devices can also work with existing 11Mbps 802.11b equipment.

Once connected to a wireless network, you can keep in touch with your e-mail, access the Internet, and share files and other resources such as printers and network storage with other computers on the network, wherever you wander. At home, you can surf the web or use instant messaging to chat with friends while sitting out on the patio. You'll also be able to connect with any of the growing number of public wireless hotspots springing up in coffee shops, airport lounges, hotels and convention centers. And as those hotspots upgrade to the new high-speed 802.11g standard, you'll be ready to take advantage of the increased speeds. Get connected to current-standard 802.11b networks today, and be prepared for the future with the 802.11g miniPCI.

### **1.2 Features**

- CF Interface
- Dimensions: 20 x 20 x 3.5mm
- Driver Supporting:
  - Linux Driver Source Code & Porting Guide
  - WinCE v4.2 & 5.0 DLL I/F
- WLAN Plug-in Modules for Non-Wireless Systems
- Supports Contention Free (CF)-poll and CF-ACK for Operation under Point Coordination Function(PCF)
- Supports Request to Send(RTS) / Clear to Send(CTS) for Operation under Distribution Coordination Function(DCF)
- 54Mbps high-speed wireless transfer rate

## 2. Planning Your Wireless Network

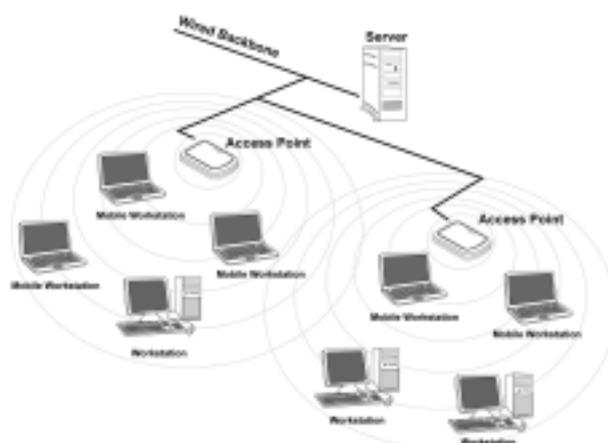
### 2.1 WLAN

A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers in a WLAN share the same frequency channel and SSID, which is an identification name for wireless devices.

### 2.2 Ad-Hoc and Infrastructure

Unlike wired networks, wireless networks have two different modes: **Ad-Hoc** and **Infrastructure**. An Ad-Hoc configuration is wireless-equipped computers communicating directly with each other. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. Choosing between these two modes depends on whether or not the wireless network needs to share data or peripherals with a wired network.

If the computers on the wireless network need to be accessed by a wired network or need to share a peripheral, such as a printer, with the wired network computers, the wireless network should be set up in **Infrastructure** mode. (See Figure 2-1.) The basis of infrastructure mode centers around an access point, which serves as the main point of communications in a wireless network. Access points transmit data to PCs equipped with wireless network devices, which can roam within a certain radial range of the access point. Multiple access points can be arranged to work in succession to extend the roaming range, and can be set up to communicate with your Ethernet (wired) hardware as well.



**Figure 2-1**

If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the **Ad-Hoc** mode can be used. (See

Figure 2-2.) Ad-Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for an access point. The drawback of this mode is that, in Ad- Hoc mode, wireless-equipped computers are not able to communicate with computers on a wired network.



**Figure 2-2**

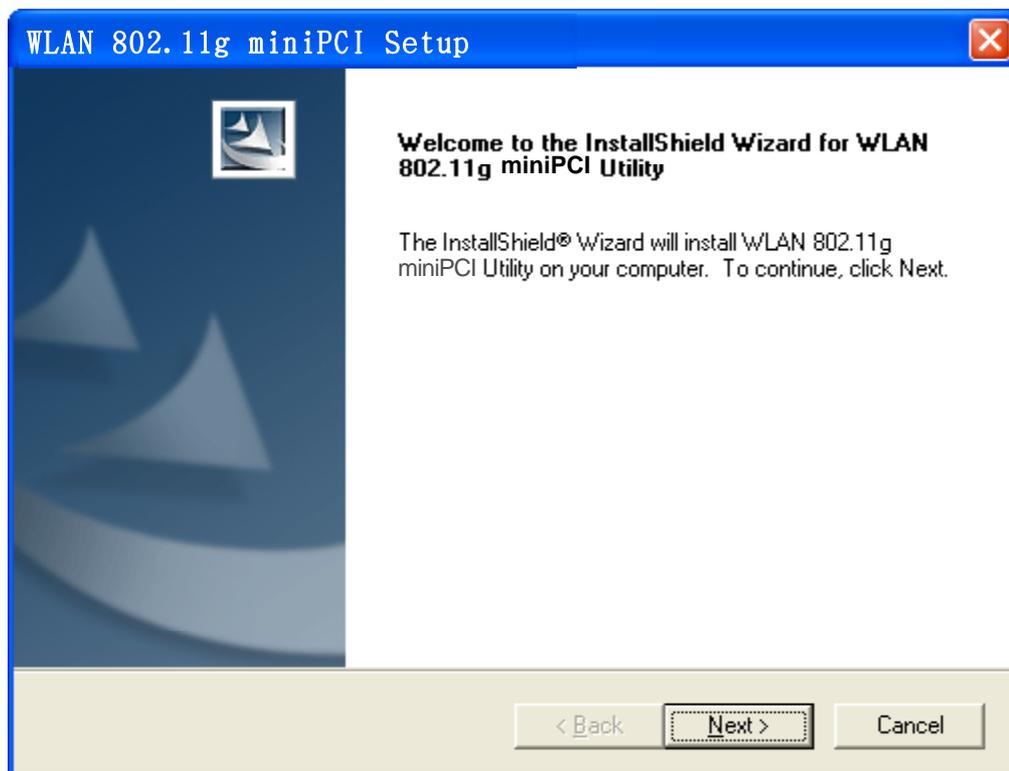
### 3. Software Installation and Uninstallation

**Note!** The Installation Section in this Manual describes the first-time installation for Windows. To re-install the driver, please first uninstall the previously installed driver. See Chapter “3.4 Uninstallation” in this Manual.

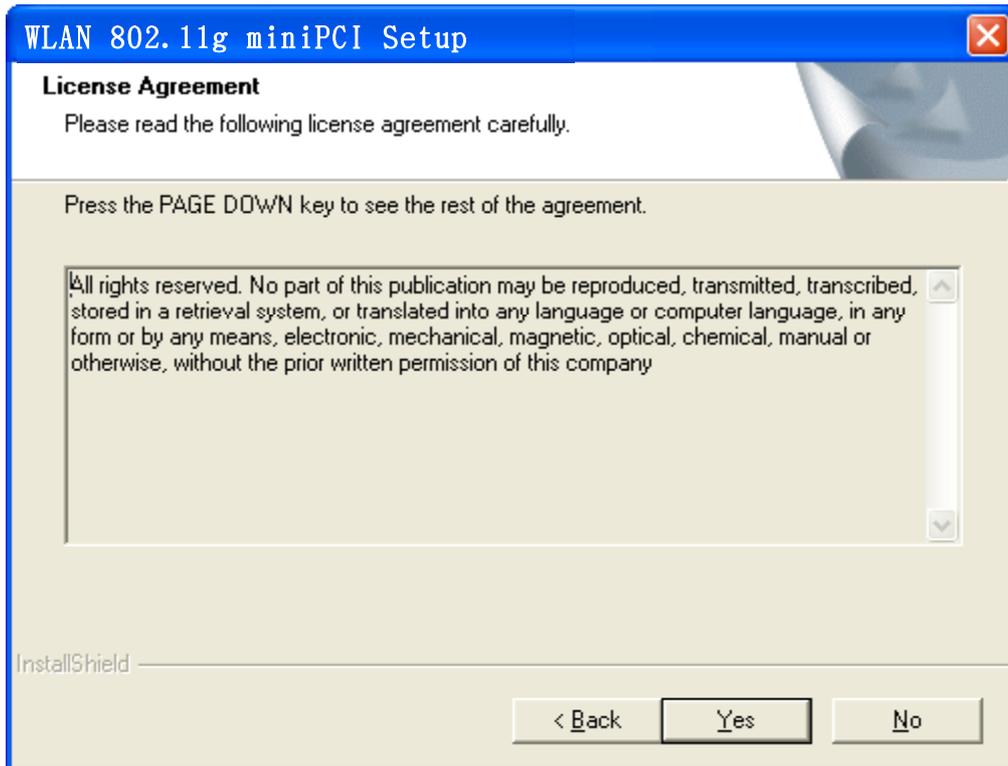
#### 3.1 Setup Wizard Installation

Follow the steps below to complete the driver/utility installation:

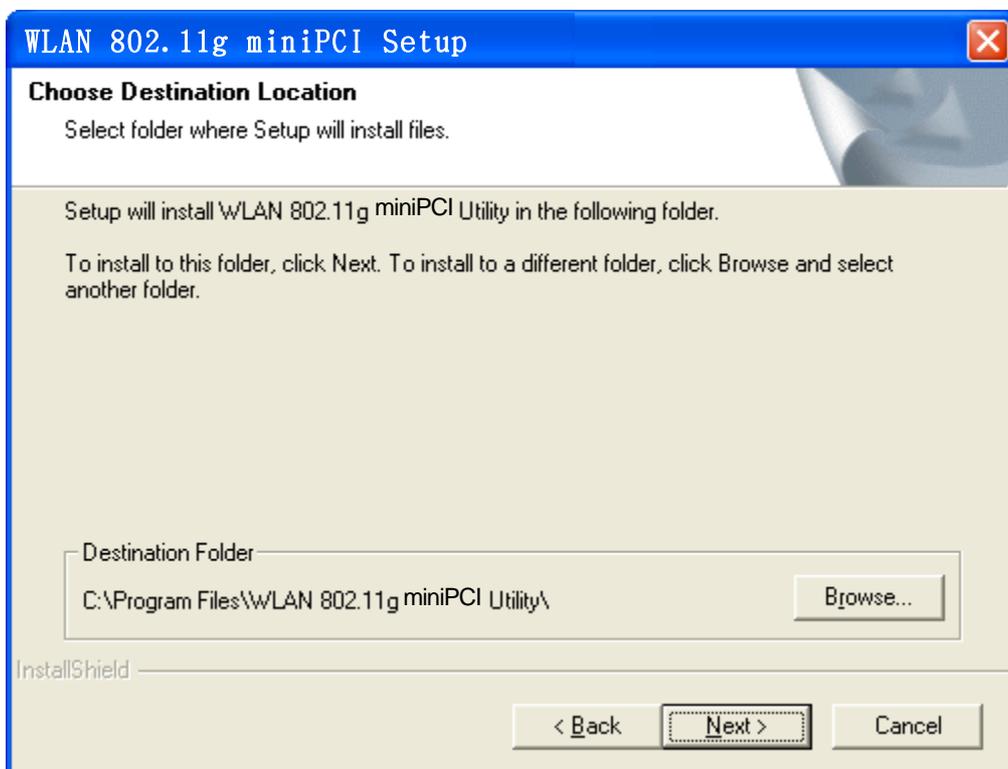
1. Insert the **Installation Software CD** into the CD-Rom Drive.
2. Click “**Next**” button.



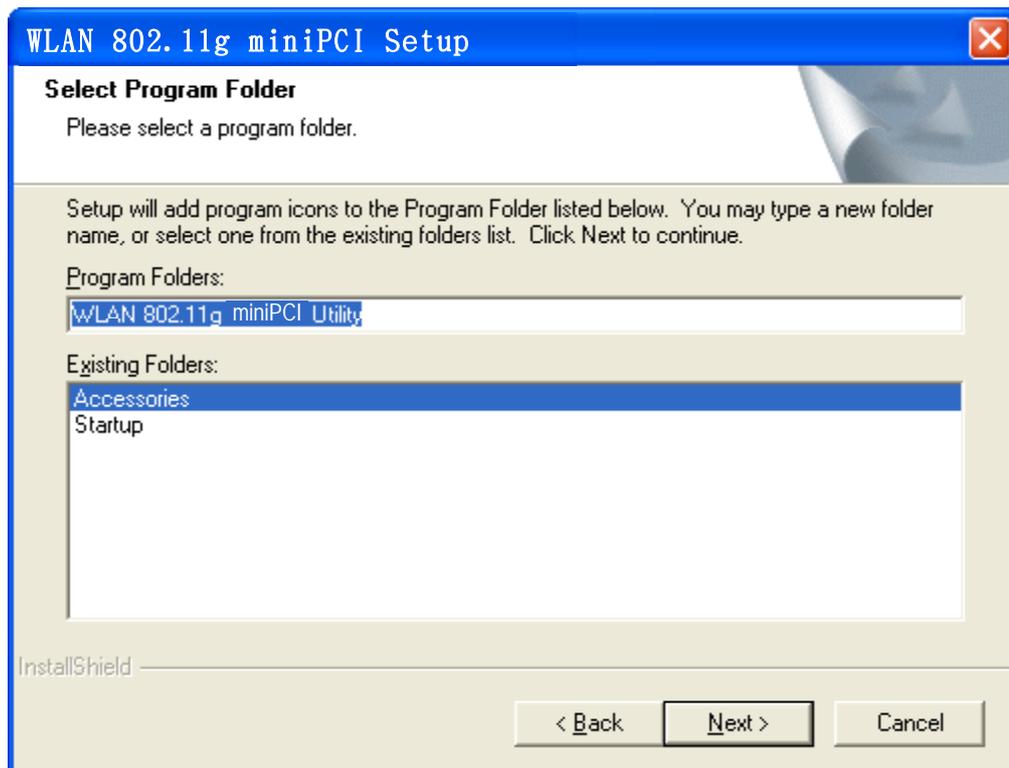
3. Read the **License Agreement** and click “**Yes**” button.



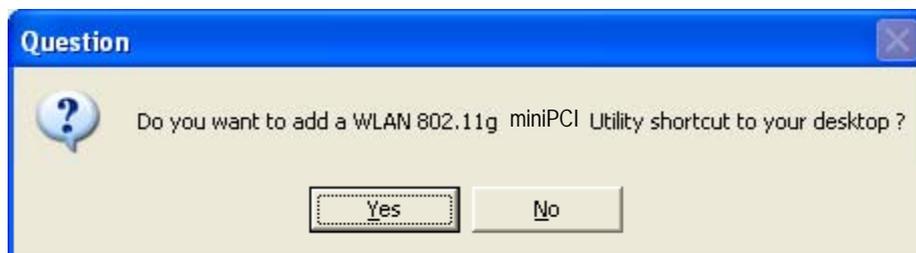
4. Click “**Next**” button to continue or click “**Browse**” button to choose a destination folder.



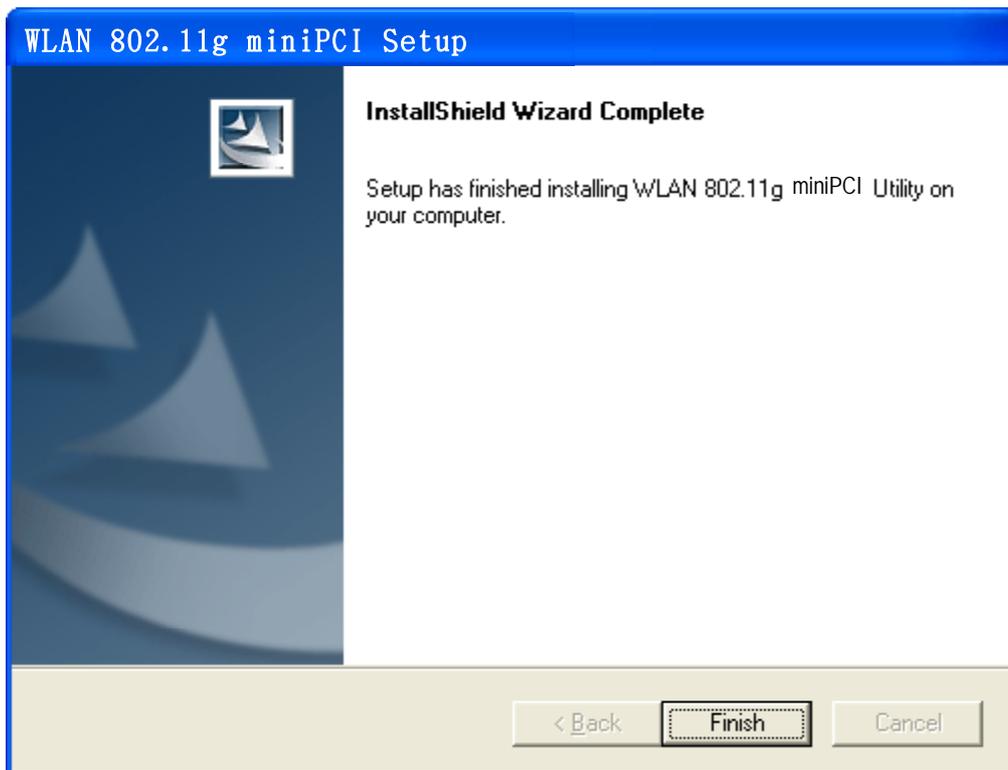
5. Click “Next” button.



6. Click “Yes” button.



7. Click **“Finish”** button. Restart your computer if necessary.



8. You may now see the WLAN 802.11g Utility shortcut icon on the desktop.

## **3.2 Additional Setup Processes**

During software installation procedure, each operating system may prompt different specific options. Mostly, you will be asked to add some necessary protocols and to edit some networking settings. Please contact the network administrator for details.

1. **Windows 98SE:** The system may request the original Windows CD during the installation process. When the installation is finished, you'll have to restart your computer.
2. **Windows Me:** Please restart your computer when the installation is finished.
3. **Windows 2000/XP:** Select "Install the software automatically" when the window with this option appears, and then click "Next" button to continue installation.

### **3.3 Uninstallation**

**Note!** Before uninstallation, please close all running programs.

1. Click Start>Programs>WLAN 802.11g miniPCI Utility>UnInstall WLAN 802.11g miniPCI.
2. Choose “**Remove-Remove all installed features**” and click “**Next**” button.
3. Click “**OK**” button to reconfirm.
4. Click “**Finish**” and restart your computer to complete Uninstallation steps.

## **4. Using IEEE802.11g WLAN Utility**

### **4.1 Overview**

Use IEEE802.11g WLAN Utility to search for available wireless networks, connect to wireless network, or check the link status.

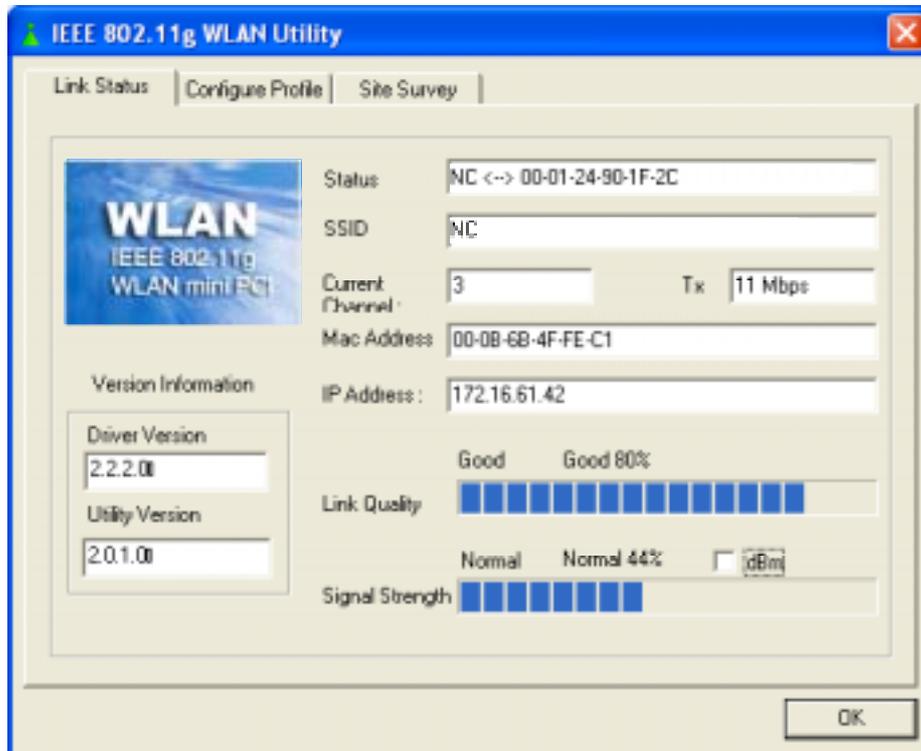
### **4.2 Accessing the Configuration Utility**

1. After software installation, the WLAN 802.11g Utility icon will appear on your desktop. Double click the icon.
2. The WLAN 802.11g Utility will appear and automatically link with the available network that has the best signal strength and is not WEP encrypted.  
If all the available network (Access Point) is WEP encrypted, please contact with the network administrator for the WEP setting.

**Note:** Once connected, the link-status icon will become green .

### 4.3 Link Status

The **Link Status** tab shows the link status, including SSID, channel, Mac Address, IP address, Link Quality and Signal Strength.

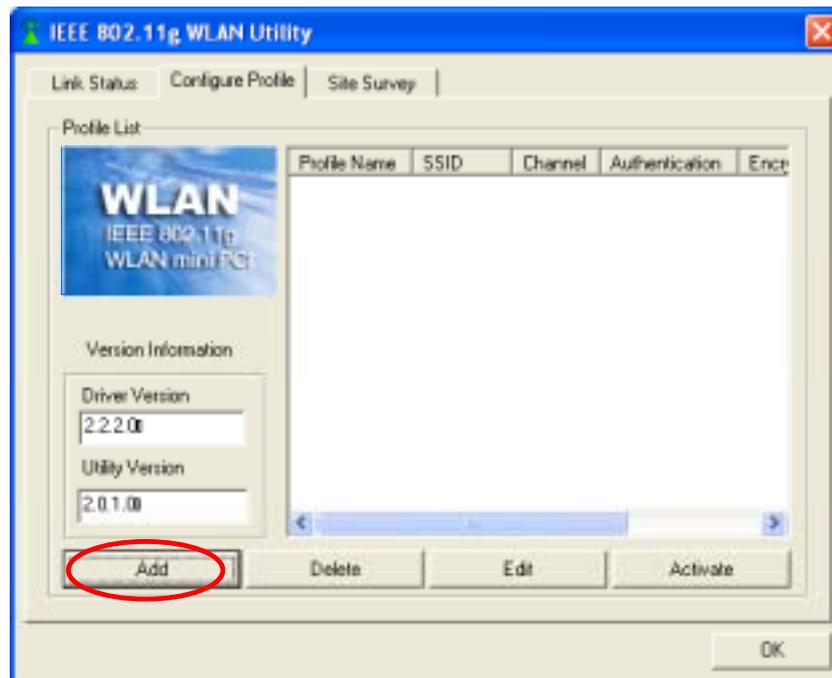


## 4.4 Configure Profile

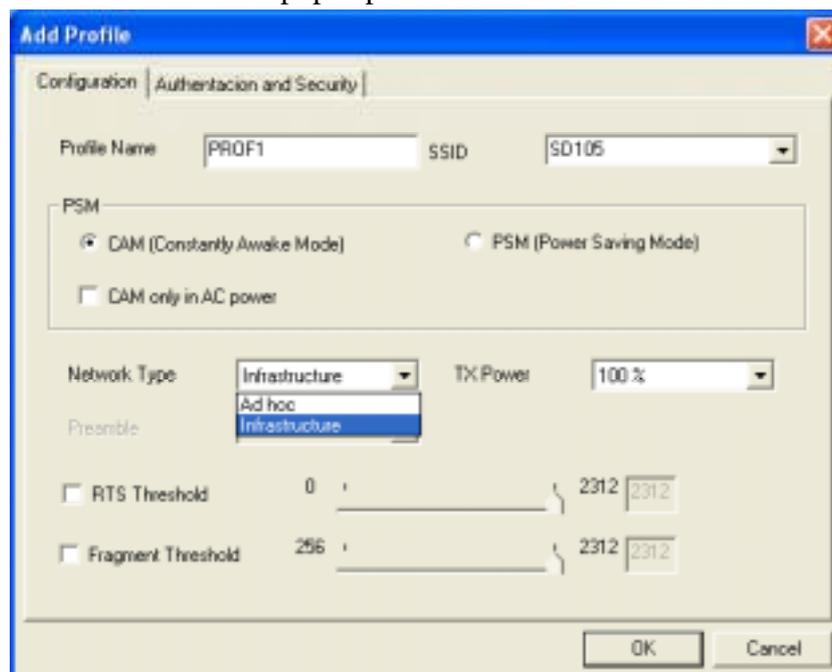
The Configure Profile tab is for you to create and configure the profile (Network) that you frequently use to link per your requirement. The profile records the system Configuration, Authentication and Security.

### 4.4.1 To create a profile

1. Click “Add” button.



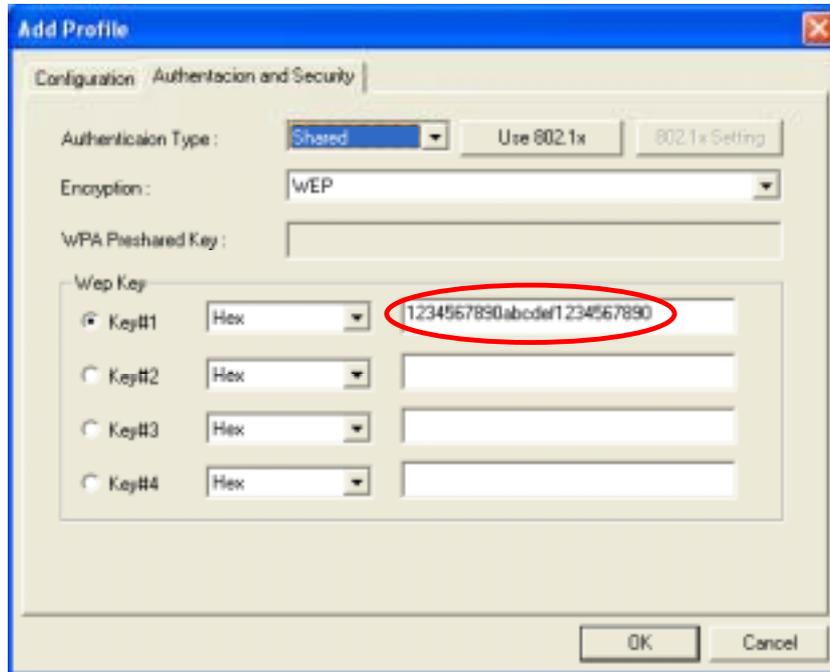
2. Add Profile window pops up. Enter a **Profile Name** and choose a **SSID**.



3. In **Configuration** tab, please choose **CAM** (Constantly Awake Mode) for

**Infrastructure** Network Type. For **802.11 Ad Hoc** Network Type, please activate **PSM** (Power Saving Mode).

4. In **Authentication & Security** tab, please contact the network administrator for WEP Key setting if the chosen AP (SSID) is WEP encrypted.



- **Authentication Type**

Four options are available: None, Shared, WPA and WPA-PSK.

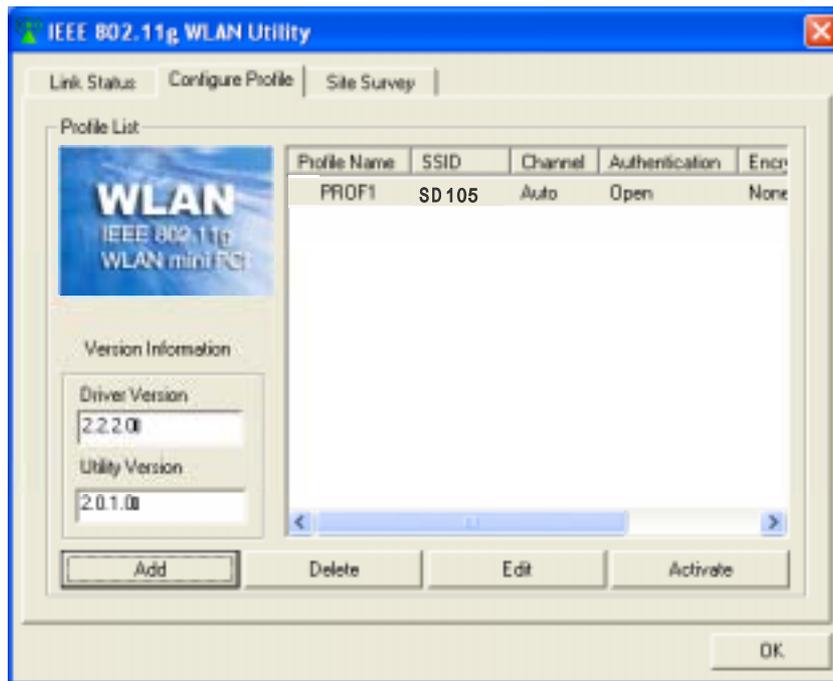
- **802.1x**

If choose to use 802.1x, please click “**802.1x Setting**” button to open 802.1x Setting window. Contact the network administrator for the value of each setting.

- **Wep Key**

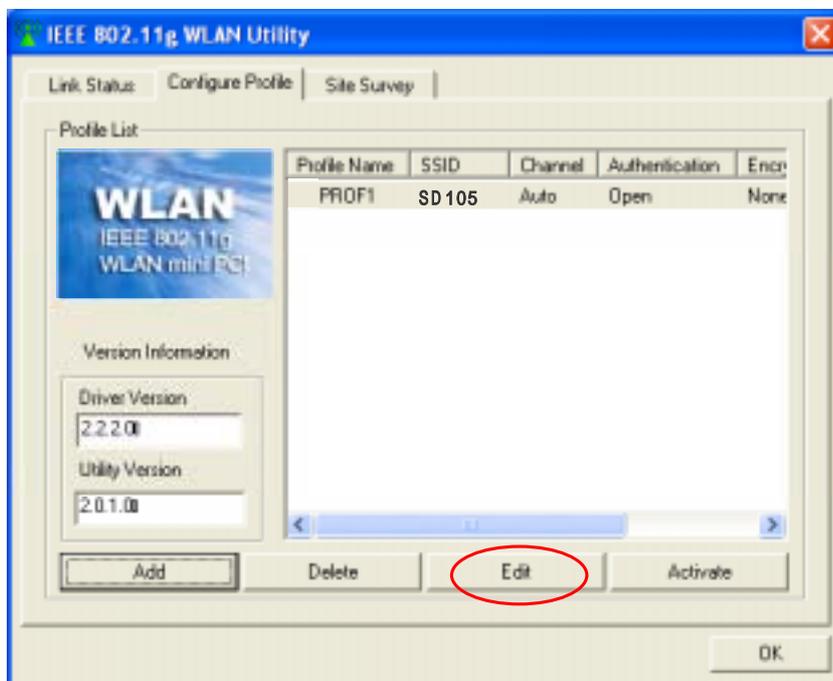
Four Wep Keys are available. Each key can be set as Hex or ASCII. Contact the network administrator for the values of settings.

5. Click “**OK**”. The newly created profile is now listed in **Configure Profile** tab.



#### **4.4.2 To edit a profile**

1. In **Configure Profile** tab, choose the profile (by clicking the profile name from the list) and then click “**Edit**” button.



2. **Add Profile** window pops up. Edit the settings in **Configuration** tab and **Authentication & Security** tab. Click “**OK**” button to save the new settings.

#### **4.4.3 To delete a profile**

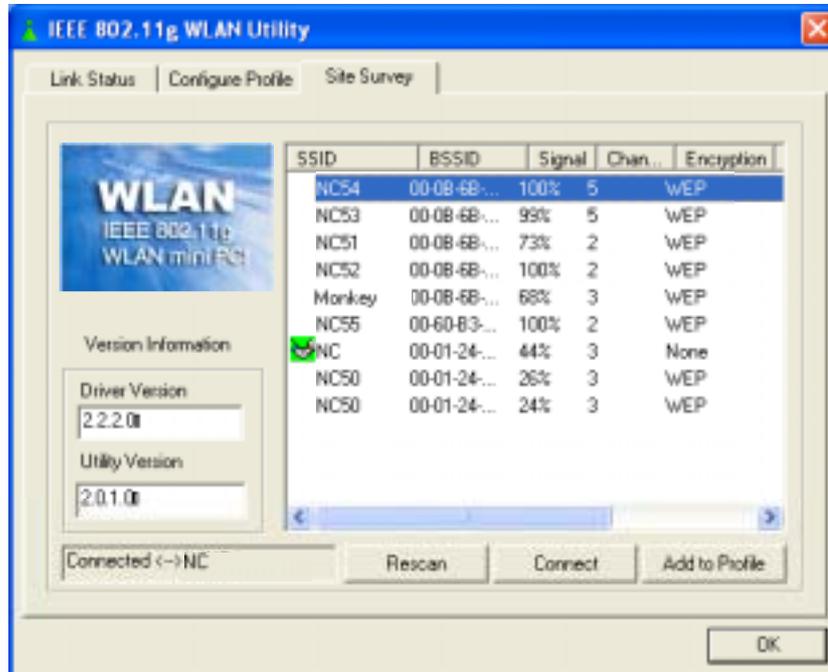
1. In **Configure Profile** tab, choose the profile (by clicking the profile name from the list).
2. Click “**Delete**” button.

#### **4.4.4 To activate a profile**

1. In **Configure Profile** tab, choose the profile (by clicking the profile name from the list).
2. Click “**Activate**” button.
3. An activate icon  will appear in front of the profile name. Green icon  indicates connected, and red one  indicates disconnected.

## 4.5 Site Survey

This tab gives you the information of all the available networks in vicinity, such as SSID, BSSID, Signal, Channel, Encryption, Authentication and Network Type, so that you can select a network with better signal for better performance.



### 4.5.1 To rescan available networks

Click “**Rescan**” button to find all available networks in vicinity.

### 4.5.2 To join a network

1. Choose a network (by clicking the **SSID** from the list).
2. Click “**Connect**” button.
3. An icon , indicates connected, will appear in front of the SSID.

### 4.5.3 To create a new profile

1. Choose a network (by clicking the **SSID** from the list).
2. Click “**Add to Profile**” button.
3. **Add Profile** window pops up. Edit the settings in **Configuration** and **Authentication & Security** tabs, and then click “**OK**” button.

## Appendix A: Glossary

**802.11b** – One of the IEEE standards of wireless networking hardware. Products that adhere to a specific IEEE standard will work with each other, even if they are manufactured by different companies. The 802.11b standard specifies a maximum data transfer rate of 11Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

**802.11g** – Refers to the proposed extension of the IEEE 802.11 standard for wireless networking, which has not been ratified by IEEE. The 802.11g specifications specify a maximum data transfer rate of 54Mbps using OFDM modulation, an operating frequency of 2.4GHz, backward compatibility with IEEE 802.11b devices and WEP encryption for security.

**Ad-Hoc Network** - An Ad-Hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-Hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-Hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

**CTS (Clear To Send)** – An RS-232 signal sent from the receiving station to the transmitting station that indicates it is ready to accept data.

**Default Gateway** - The router used to forward all traffic that is not addressed to a station within the local subnet.

**DHCP (Dynamic Host Configuration Protocol)**- A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, new IP address must be entered. DHCP lets a network administrator supervise and distribute IP address from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a “lease” or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It’s especially useful in education and other environments where users change frequently. Using very short lease, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP address.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

**DNS** – The domain name system (DNS) is the way that Internet domain name are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address.

**DSSS (Direct-Sequence Spread Spectrum)** – DSSS generates a redundant bit pattern for all transmitted data. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected(ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

**Dynamic IP Address** – An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

**ESS (Extended Service Set)** – A set of more than two or more BSSs (multiple access points) forming a single network.

**Firmware** – Code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

**IEEE** – The Institute of Electrical and Electronics Engineers. The IEEE describes itself as “the world’s largest technical professional society – promoting the development and application of electro-technology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.” The IEEE fosters the development of standards that often become national and

international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society.

**Infrastructure Network** – An Infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

**IP Address** – In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32 – binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message ( actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requester or the e-mail sender and can respond by sending another message using the IP address it received.

**IPCONFIG** – A utility that provides for querying, defining and managing IP addresses within a network. A commonly used utility, under Windows NT and 2000, for configuring networks with static IP addresses.

**ISP** – An ISP (Internet service provider) is a company that provides individuals and companies access to the Internet and other related services such as Web site building and virtual hosting.

**LAN** – A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resource of a single processor or server within a small geographic area ( for example, within an office building).

**MAC Address** – The MAC (Media Access Control) address is your computer's

unique hardware number.

**mIRC** – mIRC runs under Windows and provides a graphical interface for logging onto IRC servers and listing, joining and leaving channels.

**Network Mask** – also known as the “Subnet Mask”.

**OFDM** – Developed for wireless applications, Orthogonal Frequency Division Multiplexing (OFDM) technology offers superior performance-increased data rates and more reliable transmissions- than previous technologies, such as DSSS. OFDM is a scheme in which numerous signals of different frequencies are combined to form a single signal for transmission on the medium. OFDM works by breaking one high-speed data stream into a number of lower-speed data streams, which are then transmitted in parallel. Each lower speed stream is used to modulate a sub-carrier. Essentially, this creates a multi-carrier transmission by dividing a wide frequency band or channel into a number of narrower frequency bands or sub-channels. OFDM is also used for other applications, including power line networking.

**Roaming** - In an infrastructure mode wireless network, this refers to the ability to move out of one access point's range and into another and transparently reassociate and reauthenticate to the new access point. This reassociation and reauthentication should occur without user intervention and ideally without interruption to network connectivity. A typical scenario would be a location with multiple access points, where users can physically relocate from one area to another and easily maintain connectivity.

**SSID (Service Set Identifier)** - An identification name that wireless devices use to make connections. In order for wireless devices to communicate, they must all be set to the same channel and they all must use the same SSID. For instance, if you are using an access point to connect two computers using wireless devices, the access point and each of the wireless devices must use the same SSID. Even if they are set to the same channel, they cannot communicate unless the SSID is the same.

**Static IP Address** - A permanent IP address that is assigned to a node in a TCP/IP network.

**Subnet Mask** - The method used for splitting IP networks into a series of subgroups,

or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

**TCP (Transmission Control Protocol)** - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (data gram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a "connection oriented" protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

**UDP (User Datagram Protocol)** - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connection-less" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP). **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11b standard. **WINIPCFG** - Configuration utility based on the Win32 API for querying, defining and managing IP addresses within a network. A commonly used utility under Windows 95, 98SE, and Me.

**WLAN (Wireless Local Area Network)** - A group of computers and associated devices that communicate with each other wirelessly.