

# PROWARE®

## User Guide

**PW-MN421**

**Wireless Lite-N USB Module**



## **COPYRIGHT & TRADEMARKS**

Specifications are subject to change without notice. **PROWARE**<sup>®</sup> is a registered trademark of PROWARE TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from PROWARE TECHNOLOGIES CO., LTD. Copyright © 2010 PROWARE TECHNOLOGIES CO., LTD. All rights reserved.

<http://www.proware.com.cn>

## FCC 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 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.

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.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

“To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas 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.”

## CE Mark Warning



This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

# National Restrictions

## 2400.0-2483.5 MHz

Country	Restriction	Reason/remark
Bulgaria		General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy		If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation		Only for indoor applications

Note: Please don't use the product outdoors in France.

# CONTENTS

<b>Package Contents .....</b>	<b>1</b>
<b>Chapter 1 Introduction .....</b>	<b>2</b>
1.1 Overview of the Product .....	2
1.2 Features .....	2
<b>Chapter 2 Installation Guide .....</b>	<b>3</b>
2.1 Hardware Installation .....	3
2.2 Software Installation .....	3
<b>Appendix A: Specifications .....</b>	<b>8</b>
<b>Appendix B: Glossary .....</b>	<b>9</b>

## Package Contents

The following items should be found in your package:

- PW-MN421 Wireless Lite-N USB Module

### **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

### **Conventions:**

The 'Module' mentioned in this user guide stands for PW-MN421 Wireless Lite-N USB Module without any explanations.

# Chapter 1 Introduction

Thank you for choosing the **PW-MN421 Wireless Lite-N USB Module!**

## 1.1 Overview of the Product

The module is an 802.11n client device. It is mainly designed to provide a high-speed and unrivaled wireless performance for wireless embedded system application. With a faster wireless connection, you can get a better Internet experience without the cost of running network cables.

With the 802.11n technology, the PW-MN421's auto-sensing capability allows high packet transfer rate of up to 150Mbps for maximum throughput. It has good capability on anti-jamming, and it can also interoperate with other wireless (802.11b/g/n) products. The module supports WEP, WPA and WPA2 encryption to prevent outside intrusion and protect your personal information from being exposed.

With unmatched wireless performance, reception, and security protection, it is easily to be used in different kinds of wireless embedded system for its size and portable.

## 1.2 Features

- Complies with IEEE802.11n, IEEE802.11g, IEEE802.11b standards
- Supports WPA/WPA2 data security, IEEE802.1x authentication, TKIP/AES encryption, 64/128/152-bit WEP encryption
- Supports high rate of up to 150Mbps for maximum throughput, supports automatically adjust to lower speeds due to distance or other operating limitations
- Provides USB interface
- Supports Ad-Hoc and Infrastructure modes
- Good capability on anti-jamming
- Supports roaming between access points when configured in Infrastructure mode
- Ease to configure and provides monitoring information
- Supports Windows XP, Vista, 7

## Chapter 2 Installation Guide

### 2.1 Hardware Installation

PW-MN421 has USB interface, and it is mainly designed to provide stability wireless function and performance for your system.

For installation, you must be sure to connect this module to your device or system with a connecting wire first. Then, the promoted Found New Hardware Wizard will pop up if the Module is installed correctly.

### 2.2 Software Installation

Windows XP, Vista, 7 are supported. This user guide takes Windows XP for example.

1. Please run the **Setup** program of the module. Then you will see Figure 2-1.

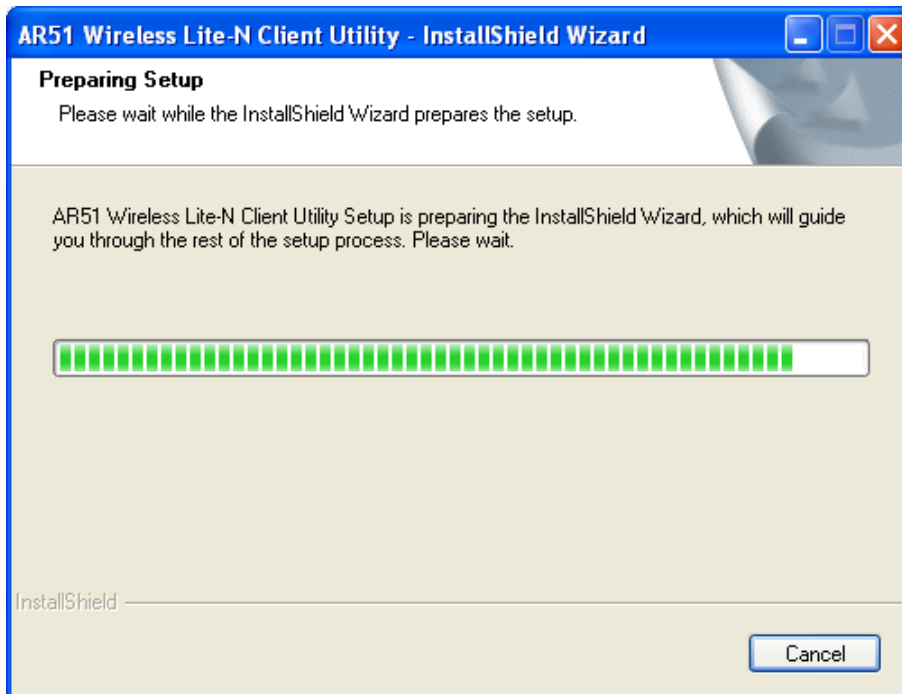


Figure 2-1

2. Soon, Figure 2-2 will display after a moment. Click **Next** to continue.



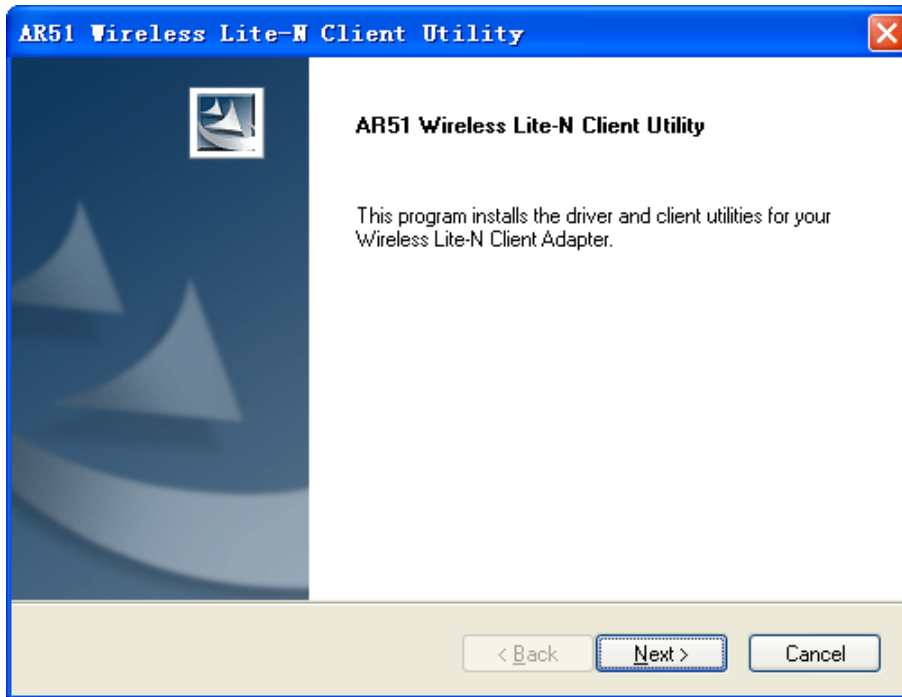


Figure 2-2

3. After that, you should choose a Setup type. It is recommended that you select **Install Client Utilities and Driver**. Select **Install Driver Only** to install driver only, select **Make Driver Installation Diskette(s)** to make the diskette(s) as the installation driver (shown in Figure 2-3). Click **Next** to continue.

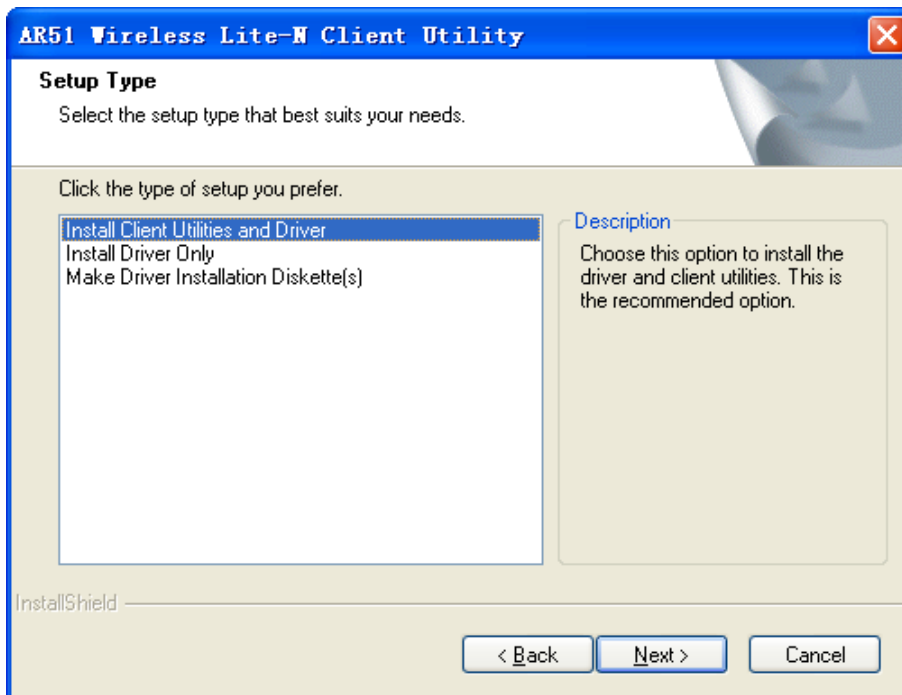


Figure 2-3

4. Click **Browse...** to change the destination location for the software, then click **Next** in the screen below (shown in Figure 2-4).

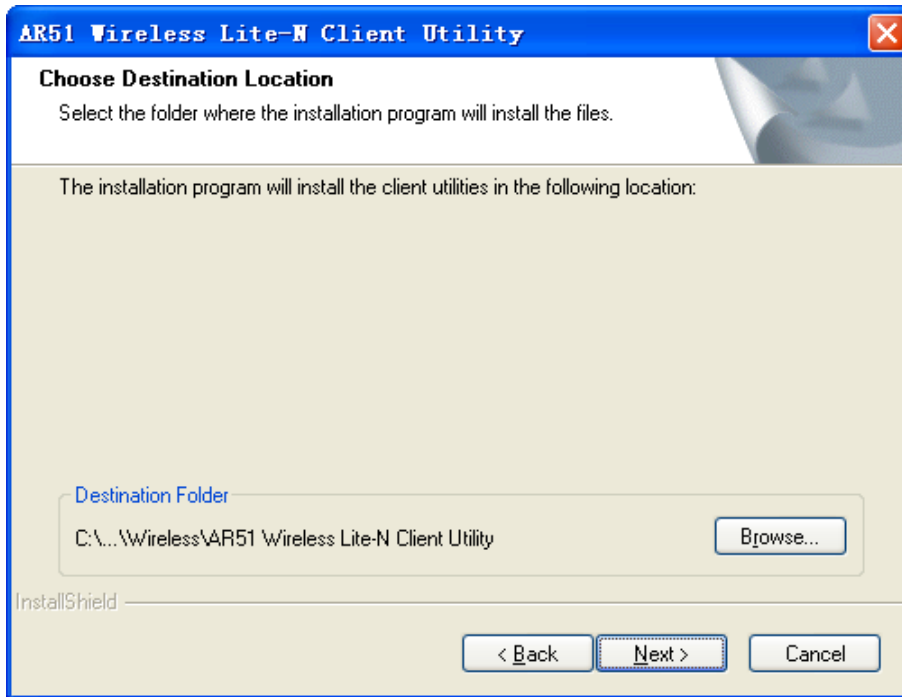


Figure 2-4

5. After that, select the program folder, you should create a new folder name or select one from the **Existing Folders** list. It is recommended that you keep the default setting. Click **Next** to continue the installation.

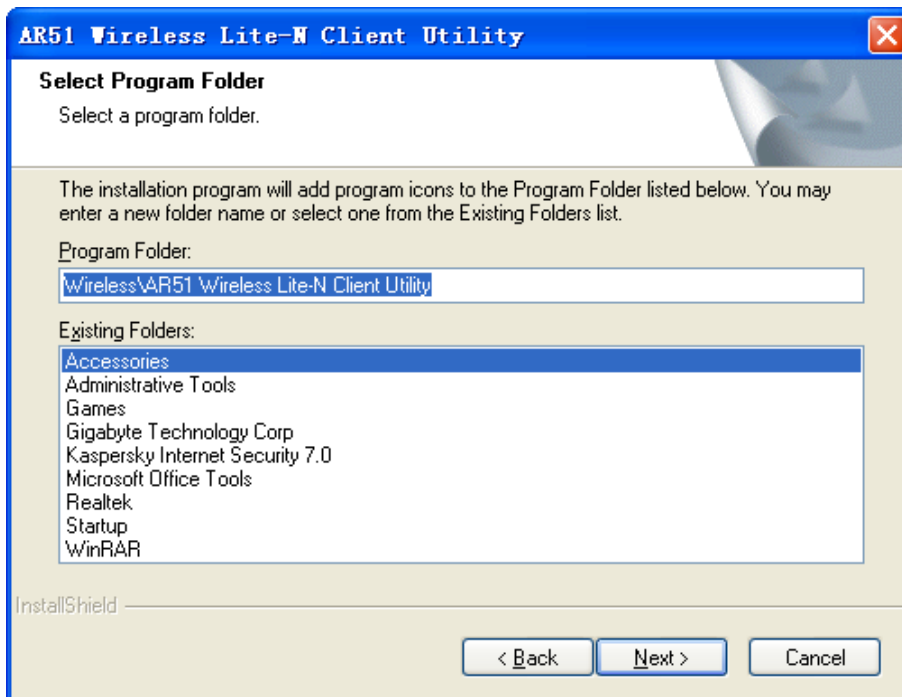


Figure 2-5

6. Choose configuration tool, if you are not sure, please leave it default. Then click **Next** to continue.

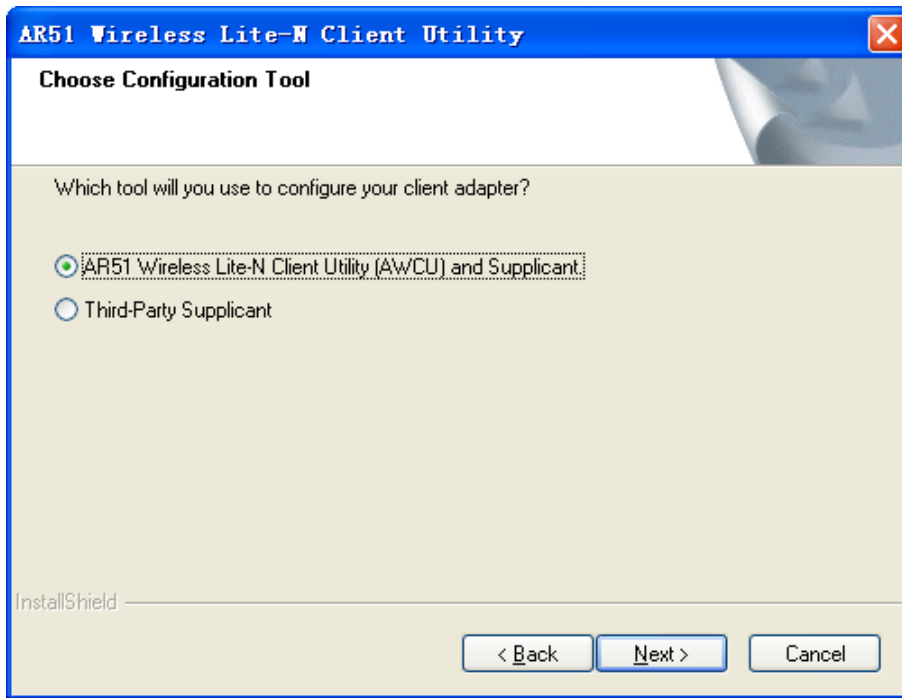


Figure 2-6

7. Click **OK** to continue the Installation. Wait a while for the setup as shown in Figure 2-7.

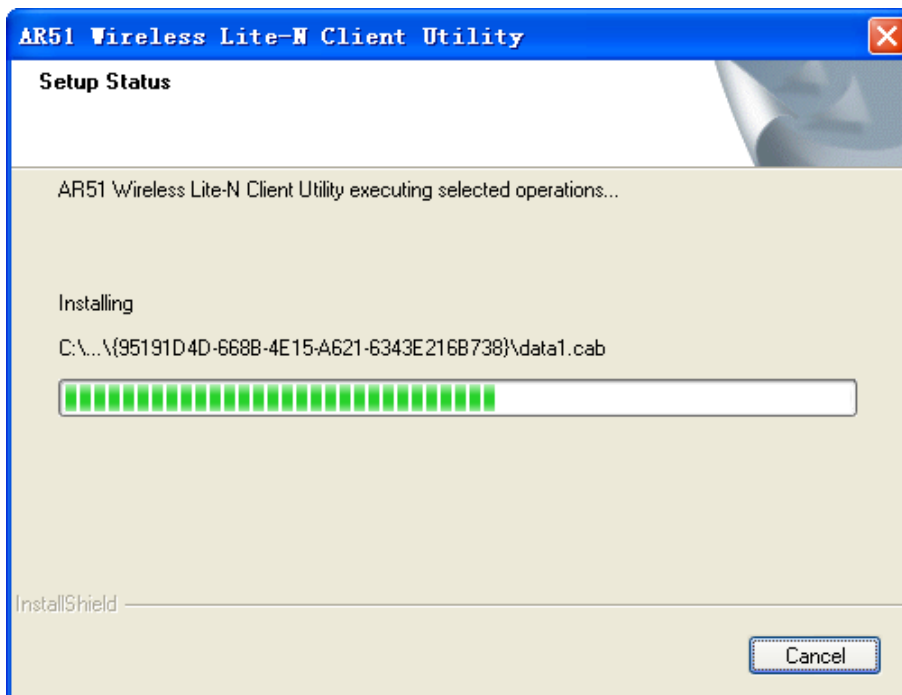


Figure 2-7

 **Note:**

For Windows XP, the Setup Wizard will notify you of how to proceed with the installation during these steps (shown in Figure 2-8). Our drivers have been tested thoroughly, and are able to work with the operating system. Click **Continue Anyway** to continue the Installation.



Figure 2-8

8. After all the steps above, you will see the screen below, click **Finish** to reboot the system.

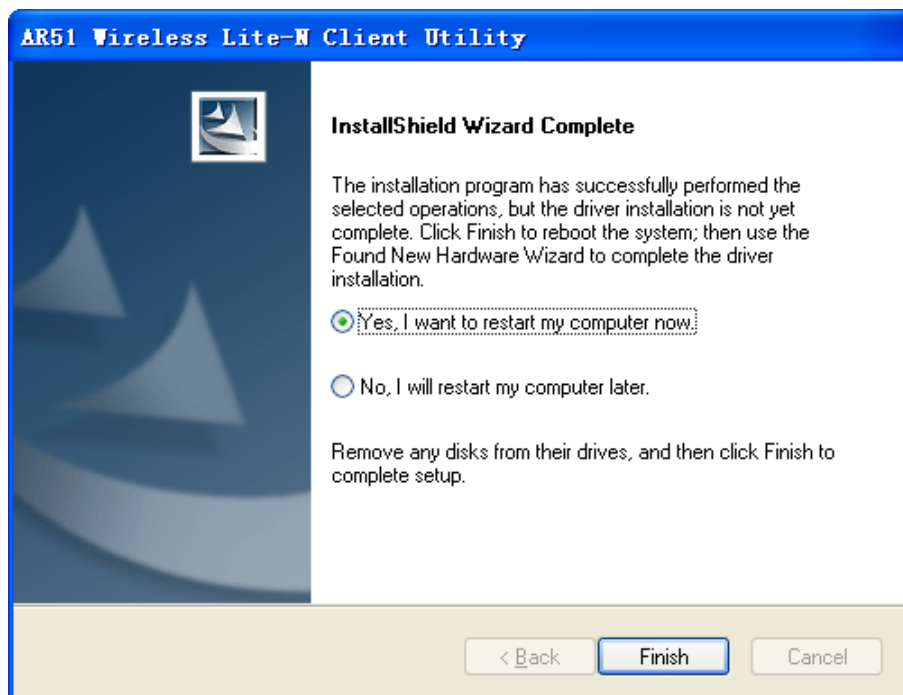


Figure 2-9

## Appendix A: Specifications

<b>Normal</b>	
Interface	USB 2.0 Interface
Standards	IEEE802.11n; IEEE802.11g; IEEE802.11b;
Operating System	Windows XP, Vista, 7
Throughput	150Mbps (Maximal)
Radio Data Rate	11b: 11/5.5/2/1Mbps (Dynamic) 11g: 54/48/36/24/18/12/9/6Mbps (Dynamic) 11n: up to 150Mbps (Dynamic)
Modulation	BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, DQPSK, and CCK
Media Access Protocol	CSMA/CA with ACK
Data Security	WPA/WPA2; 64/128/152-bit WEP; TKIP/AES
Frequency	2.4 ~ 2.4835GHz
Spread Spectrum	Direct Sequence Spread Spectrum (DSSS)
Safety & Emissions	FCC, CE

<b>Environmental and Physical</b>	
Operating Temp.	0°C~60°C (32°F~140°F)
Storage Temp.	-40°C~ 80°C (-40°F~176°F)
Humidity	10% ~ 90% RH, Non-condensing
Size	35 * 17 * 1.0 mm(1.38 * 0.67 * 0.04 in)
Weight	2.7g

## Appendix B: Glossary

- **802.11b** - The 802.11b standard specifies a wireless product networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC)<sup>[3]</sup> was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **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.
- **DSSS - (Direct-Sequence Spread Spectrum)** - DSSS generates a redundant bit pattern for all data transmitted. 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 of 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).
- **FHSS - (Frequency Hopping Spread Spectrum)** - FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.
- **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.
- **Spread Spectrum** - Spread Spectrum technology is a wideband radio frequency technique

developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

- **WEP - (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.
- **Wi-Fi** - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN - (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
- **WPA - (Wi-Fi Protected Access)** - A wireless security protocol uses TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.