EZ Connect™ N Draft 11n Wireless USB 2.0 Adapter User Guide

The easy way to make all your network connections

SMC®
Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

July 2009
Rev: 1.0.0
1910020176

Copyright

Trademarks:
SMC is a registered trademark; and EZ Connect N and EZ Switch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Warranty and Product Registration

To register SMC products and to review the detailed warranty statement, please refer to the Support Section of the SMC Website at http://www.smc.com

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.

Changes or modifications to this unit 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, 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”.

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

Package Contents

The Wireless USB Adapter package contains:

- 1 EZ Connect™ N 802.11n Wireless USB 2.0 Adapter (SMCWUSB-N2)
- 1 USB extension cable
- Warranty Information Card
- Quick Installation Guide
- 1 EZ Installation and Documentation CD, including:
  - SMCWUSB-N2 Wireless Utility and Drivers
  - User Manual

☞ **Note:**

Please register this product and upgrade the product warranty at http://www.smc.com

Please inform your distributor if there are any incorrect, damaged, or missing parts. If possible, retain the carton and the original package materials, in case there is a need to return the product.

Chapter 1. Introduction

1.1 Product Overview

Thank you for purchasing the EZ Connect™ N Draft 11n Wireless USB2.0 Adapter (SMCWUSB-N2). Designed for both the home and office, this wireless USB2.0 adapter provides the speed, coverage and security expected by today's wireless users. The SMCWUSB-N2 is 802.11n draft v2.0 compliant while maintaining full backwards compatibility with the Wireless-G (802.11g) and Wireless-B (802.11b) standards. This next generation standard utilizes advanced MIMO (Multiple-In, Multiple-Out) technology to deliver incredible speed and range. With wireless speeds up to 300Mbps and extended coverage, there is enough bandwidth to simultaneously stream video and audio, play online games, transfer large files, make VoIP calls and surf the Internet. With security being a key consideration, SMCWUSB-N2 supports the latest WPA and WPA2 wireless encryption standards, which prevent unauthorized access to wireless networks and ensure data is secure. Wireless security can also be set up easily using Wi-Fi Protected Setup™ (WPS) that enables push button or PIN configuration. The SMCWUSB-N2 includes an easy installation wizard which guides you step-by-step through the process. Once installed the WLAN utility allows you to scan for available wireless networks and manage multiple network profiles so connecting becomes instantaneous.

1.2 Features

- IEEE802.11n draft v2.0 compliant
- Wireless speeds up to 300Mbps
- Increased speeds & coverage - up to 5x the speed of 802.11g
- Fully backwards compatible with 802.11b/g wireless networks
- Stream HD video, Listen to digital music, Play online games, Transfer large files, Make VoIP calls & Surf the Internet simultaneously
- WEP 64-/128-Bit, WPA & WPA2 wireless encryption
- EZ Installation Wizard for easy installation
- Supports Windows 2000/XP/Vista
- WLAN management utility
- Two internal antennas (two receivers and two transmitters)

1.3 LED Status

LED Indications	Status	Working Status
Status Blue	Flashing Alternately	The adapter is scanning for a networking connection.
Activity Blue		
Status Blue	Intermittently	The adapter is connected but is not transmitting or receiving data.
Activity Blue		
Status Blue	Flashing	The adapter is transmitting or receiving data.
Activity Blue		

Chapter 2. Installation Guide

2.1 Hardware Installation

There are two options for installing the SMC Adapter:

Option 1: Plug the Adapter directly into the USB port on your computer.

Option 2: Connect the Adapter and your computer through the USB extension cable in the package.

The LED will light up when the Adapter is installed successfully and the PC is switched on.

2.2 Software Installation

2.2.1 Overview

The SMCWUSB-N2 EZ Installation Wizard will guide you through the Installation procedure for Windows XP. The Setup Wizard will install the SMCWUSB-N2 Wireless Utility and drivers.

When you install the hardware prior to before installing the software, the system will prompt "Found New Hardware Wizard", click **Cancel**, and run the Setup Wizard program on the CD-ROM.

The Setup steps for Windows 2000 and XP are similar. The next section of this manual uses Windows XP as an example.

For the Setup steps in Windows Vista, please follow the onscreen instructions.

2.2.2 Software Installation for Windows XP

1. Insert the EZ Installation & Documentation CD into your CD-ROM drive. The CD will auto run. Click **Install/Remove Driver and Utility** and follow the on-screen instructions.

☞ **Note:**

If a "Software Installation" warning appears during installation, click **Continue Anyway**.

Figure 2-1

2. The InstallShield Wizard prompts you for confirmation. Click **Next** to continue.

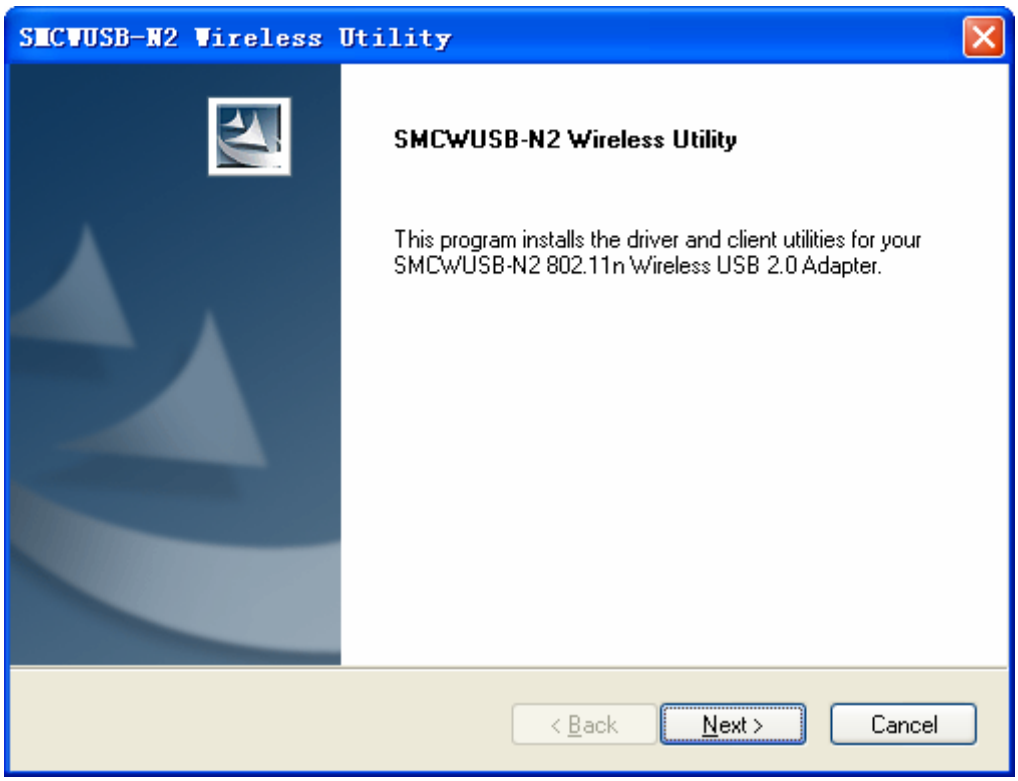

Figure 2-2

3. Choose the Setup type. It is recommended that you select **Install SMC Wireless Utility and Drivers**. Select **Install Drivers only** if you prefer to use Windows to configure and manage your wireless network connections. Click **Next** to continue.

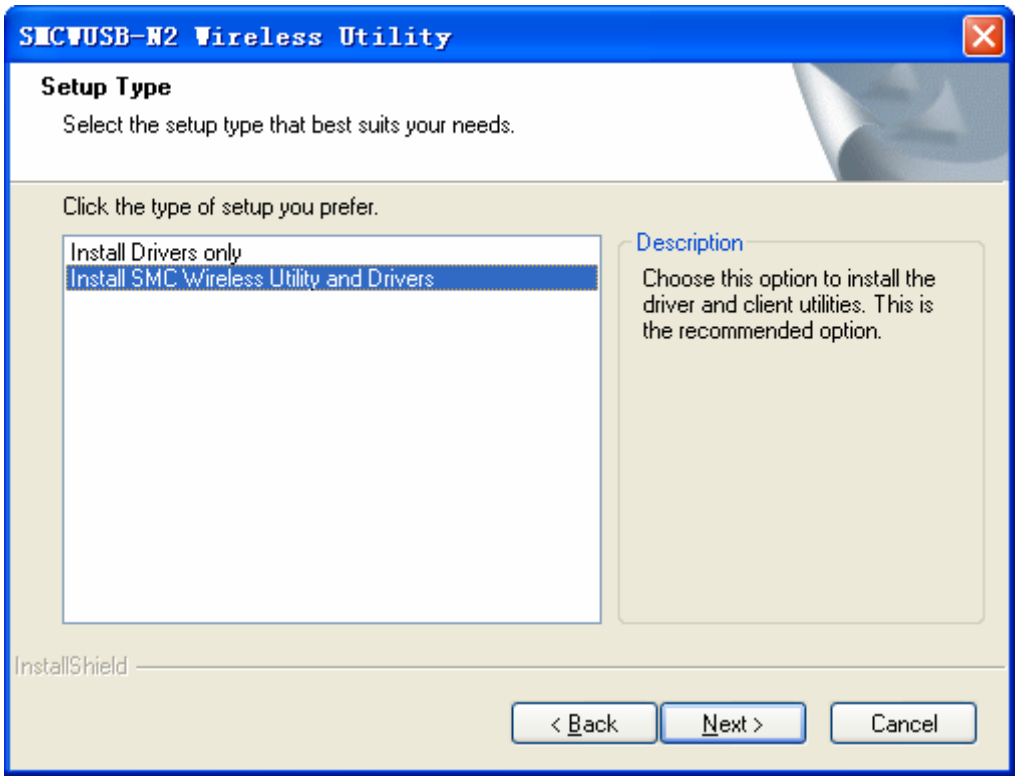

Figure 2-3

4. In the Destination Folder screen you are asked to confirm the Destination Folder for the application software. You may change the destination folder to another location. Click **Browse** to change the destination location for the software and click **Next**.

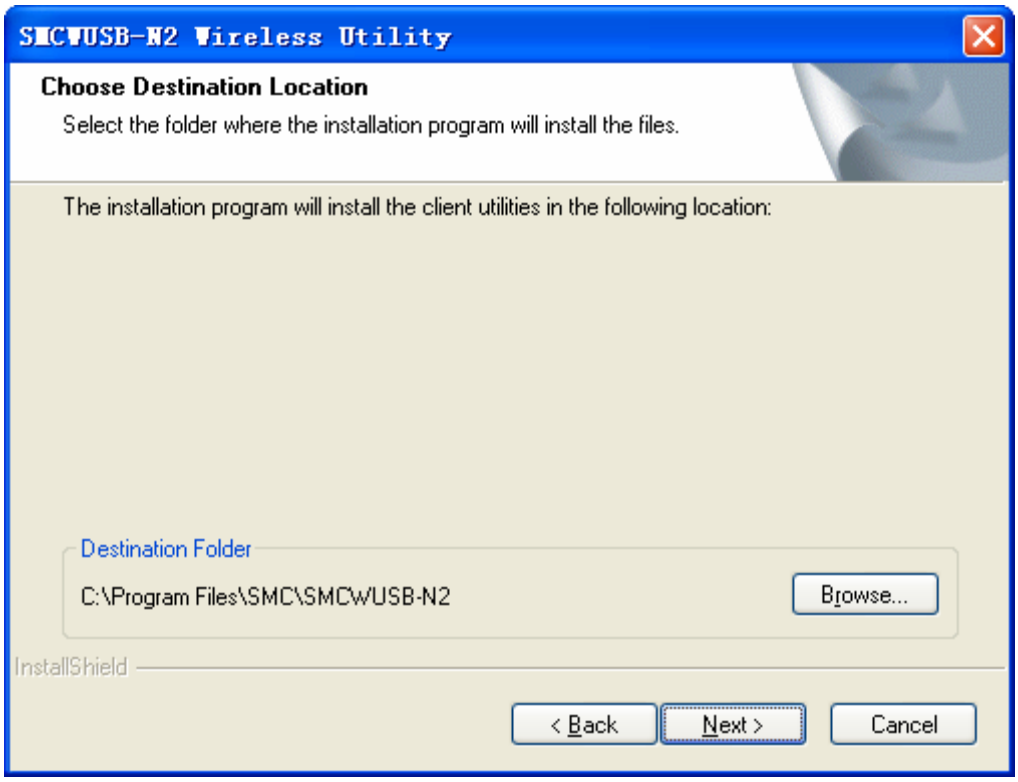

Figure 2-4

5. In the Program Folder screen you may create a new folder name for the software or select one from the **Existing Folders** list. It is recommended that you keep the default setting. Click **Next** to continue the installation.

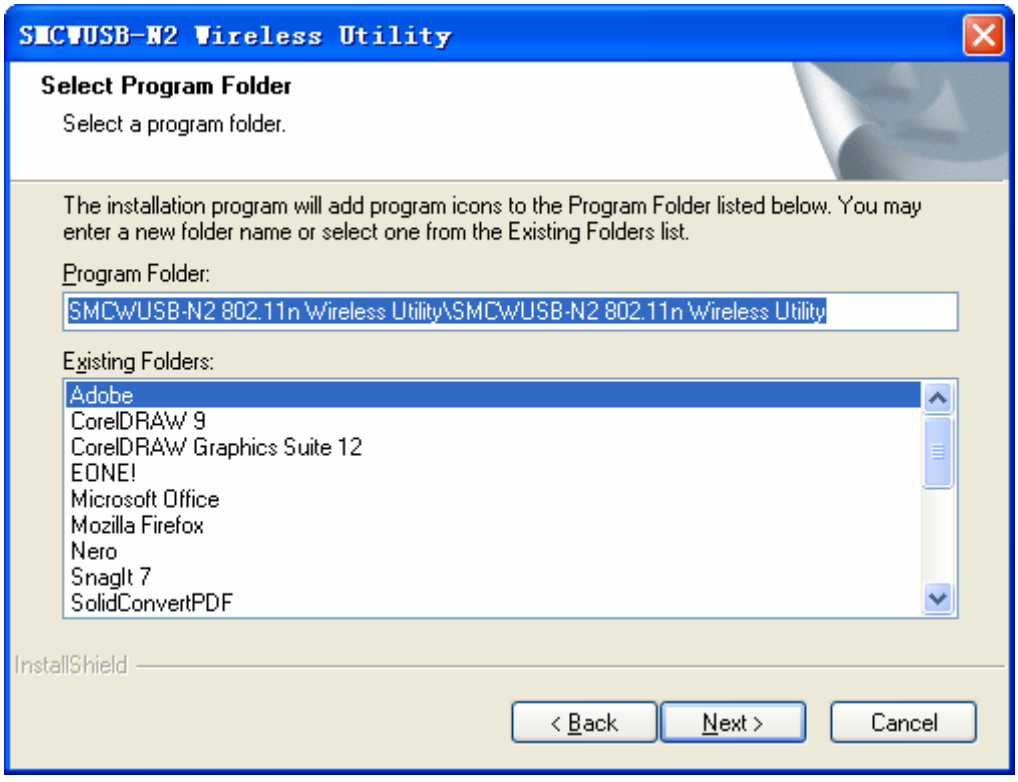

Figure 2-5

6. The following screen appears. Click **OK** to continue the Installation.

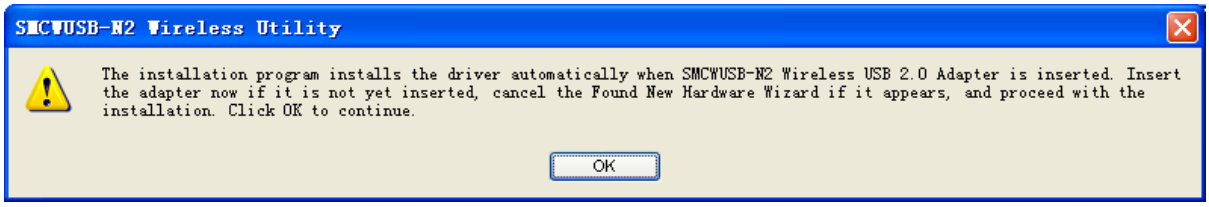

Figure 2-6

7. The wizard now begins installation.

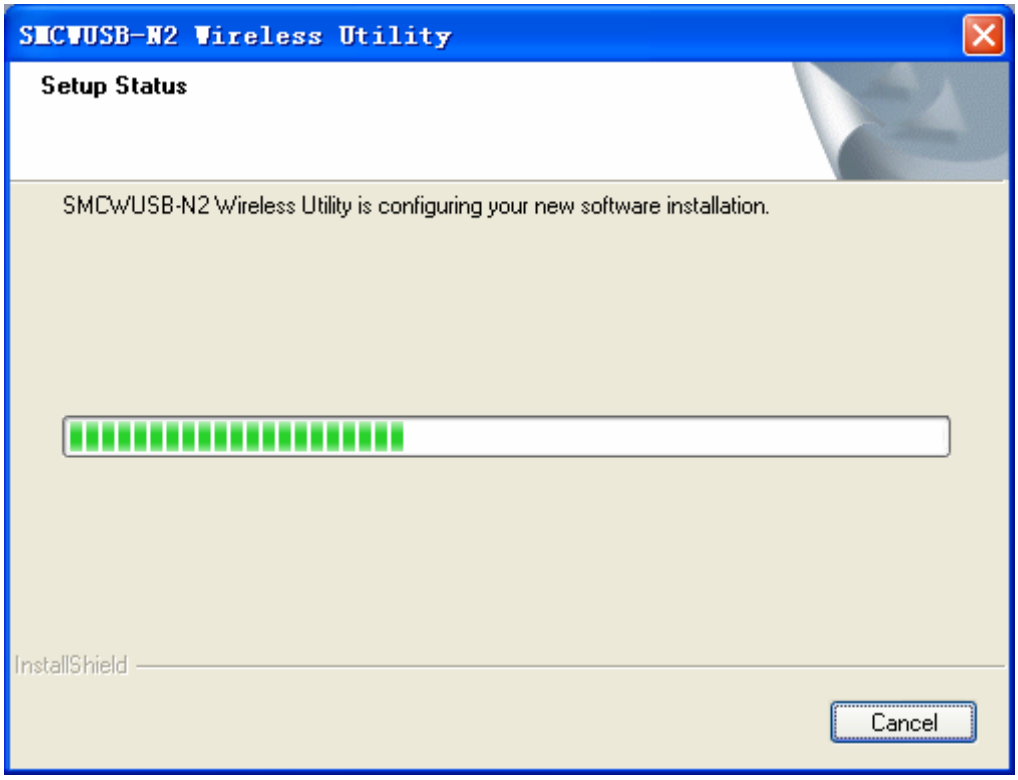

Figure 2-7

Note:

1) In Windows XP, if the following warning appears (Figure 2-8), click **Continue Anyway** to continue the installation. The SMC drivers have been tested thoroughly and are able to work with the Windows operating system.

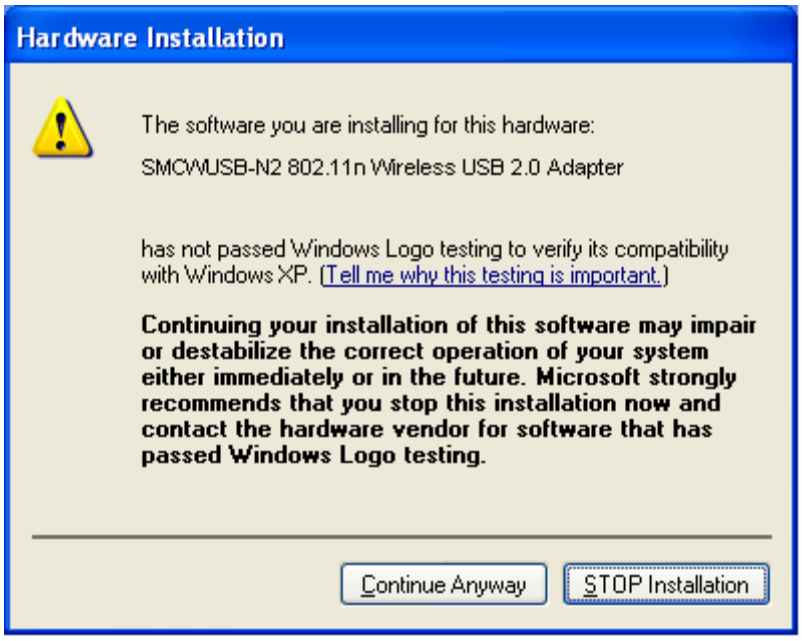

Figure 2-8

8. Click **Finish** to complete the installation and exit the Wizard.

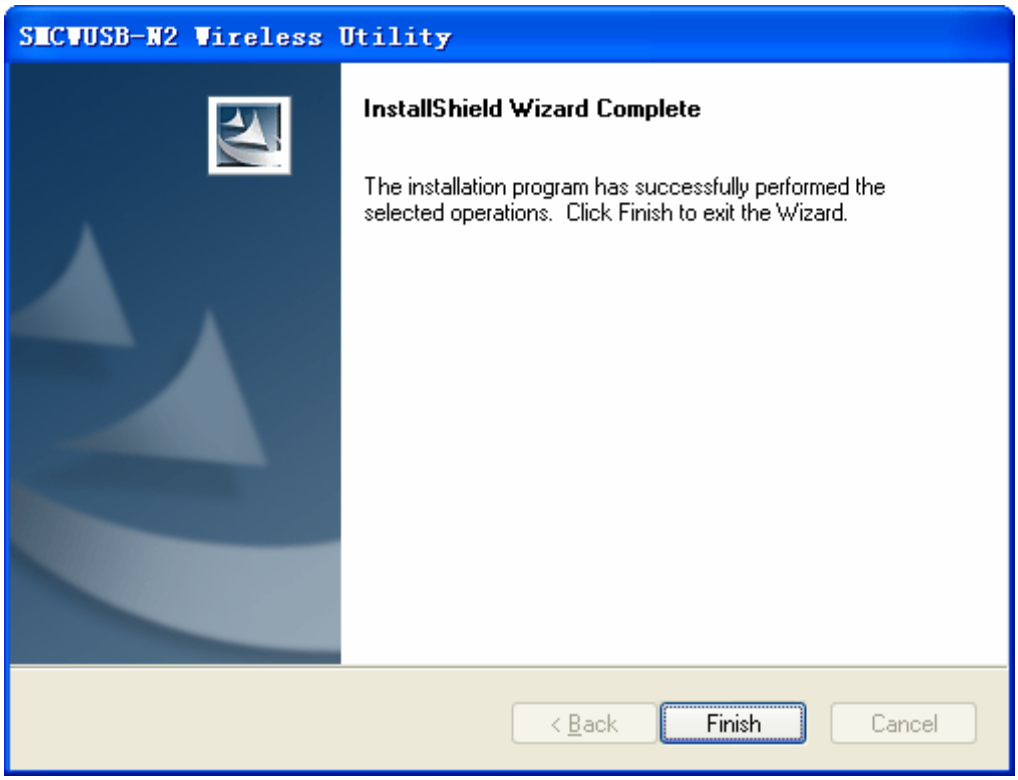

Figure 2-9

Chapter 3. Configuration for Windows XP

The EZ Connect™ N 802.11n Wireless USB 2.0 Adapter can be configured by the SMCWUSB-N2 Wireless Utility in Windows 2000 and XP. This chapter explains how to configure and use the SMC Wireless Utility program.

For the configuration in Windows Vista, please refer to Chapter 4.

After completing the installation procedure, the Adapter's tray icon  will appear in the lower right tray bar on your PC. .

 If the icon is gray, there is no connection.

 If the icon is red, there is poor signal strength and the RSSI is less than 5dB.

 If the icon is yellow, there is poor signal strength and the RSSI is between 5dB and 10dB.

 If the icon is green, there is good signal strength and the RSSI is between 10dB and 20dB.

 If the icon is green (full bar), there is excellent signal strength and the RSSI is more than 20dB.

Double-click the icon and the **SMCWUSB-N2 Wireless Utility** will run. You can also run the utility by clicking the **Start → Programs → SMCWUSB-N2 802.11n Wireless Utility → SMCWUSB-N2 802.11n Wireless Utility**. The SMCWUSB-N2 Wireless Utility provides some integrated and easy tools to:

- Display current status information
- Edit and add configuration profiles
- Display current diagnostics information

The section below introduces the above capabilities.

3.1 Current Status

The Current Status tab contains general information about the program and its operations. The Current Status tab does not need any configurations.

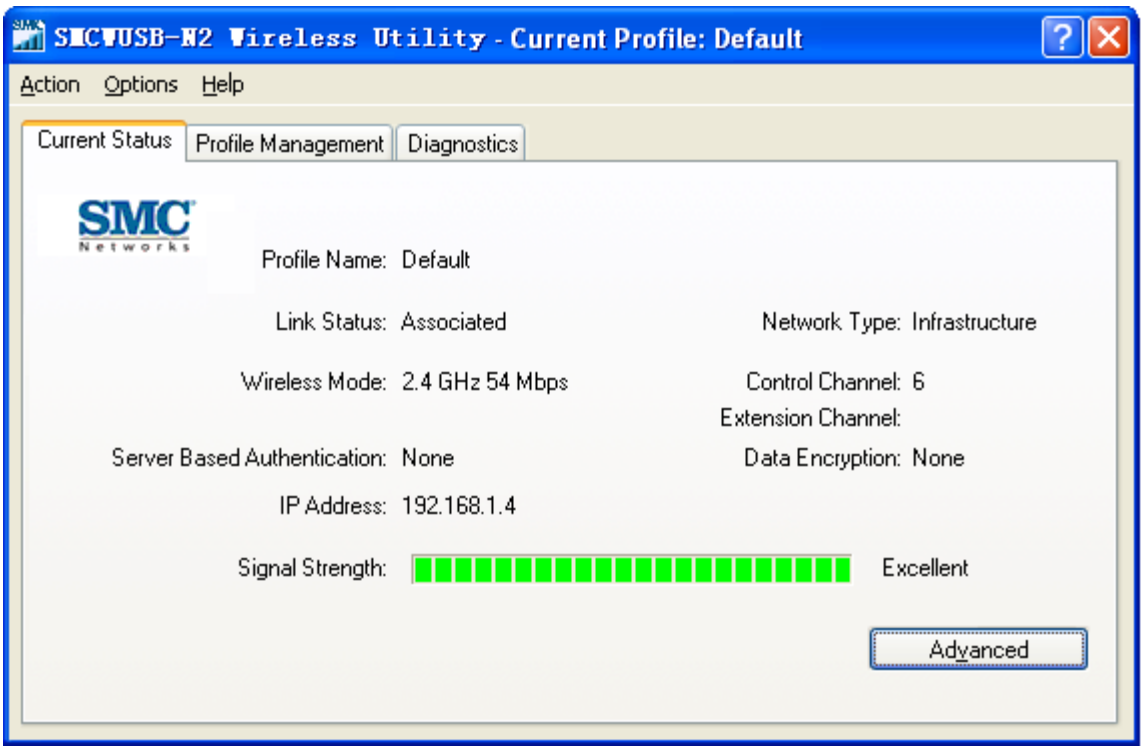

Figure 3-1

The following table describes the items on the Current Status screen.

- **Profile Name -** This shows the name of current selected configuration profile. The configuration of Profile name will be described on the **General** tab of **Profile Management**.
- **Link Status -** This shows whether the station is associated to the wireless network.
- **Wireless Mode -** This displays the wireless mode of the connected network.
- **Network Type -** The type of network and the station currently connected are shown here. The options include:
  - Infrastructure (access point)
  - Ad Hoc

☞ **Note:**

You can configure the network type and wireless mode on the **Advanced** tab of **Profile Management**.

- **IP Address -** This displays the IP address of your computer.
- **Control Channel -** This indicates the channel that the network uses.
- **Data Encryption -** This indicates the encryption type the driver is using. You can configure it on the **Security** tab of **Profile Management**.
- **Server Based Authentication -** This indicates whether the server based authentication is used.

- **Signal Strength -** This indicates the strength of the signal.

Click **Advanced** on the screen above to view other detailed information about the program and its operations.

3.2 Profile Management

Click the Profile Management tab of the **SMCWUSB-N2 Wireless Utility** to configure your wireless network connection. The Profile Management screen provides tools to:

- Add a new Profile
- Modify a Profile
- Remove a Profile
- Activate a Profile
- Import a Profile
- Export a Profile
- Scan Available Networks
- Order profiles

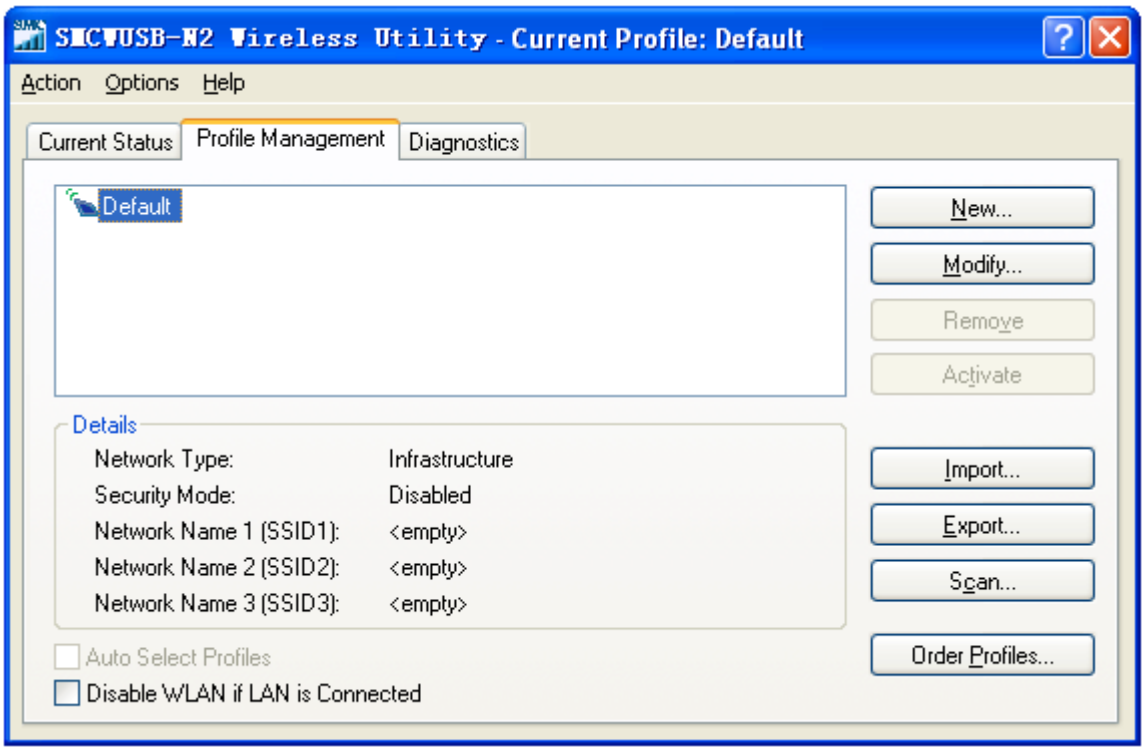

Figure 3-2

3.2.1 Add or Modify a Configuration Profile

To add a new configuration profile, click **New** on the Profile Management tab. To modify a configuration profile, select the configuration profile from the Profile list and click **Modify**. Then

you will see the Management dialog box (Figure 3-3).

1. Configure the General tab

- **Profile Name -** Enter the Profile name which identifies the configuration profile. This name must be unique. Note that the profile names are not case-sensitive.
- **Client Name -** Enter the Profile name which identifies the client machine.
- **Network Names (SSIDs) -** Enter the SSID or the name of the Wireless Network you wish to connect to. This field allows a maximum limit of 32 characters.

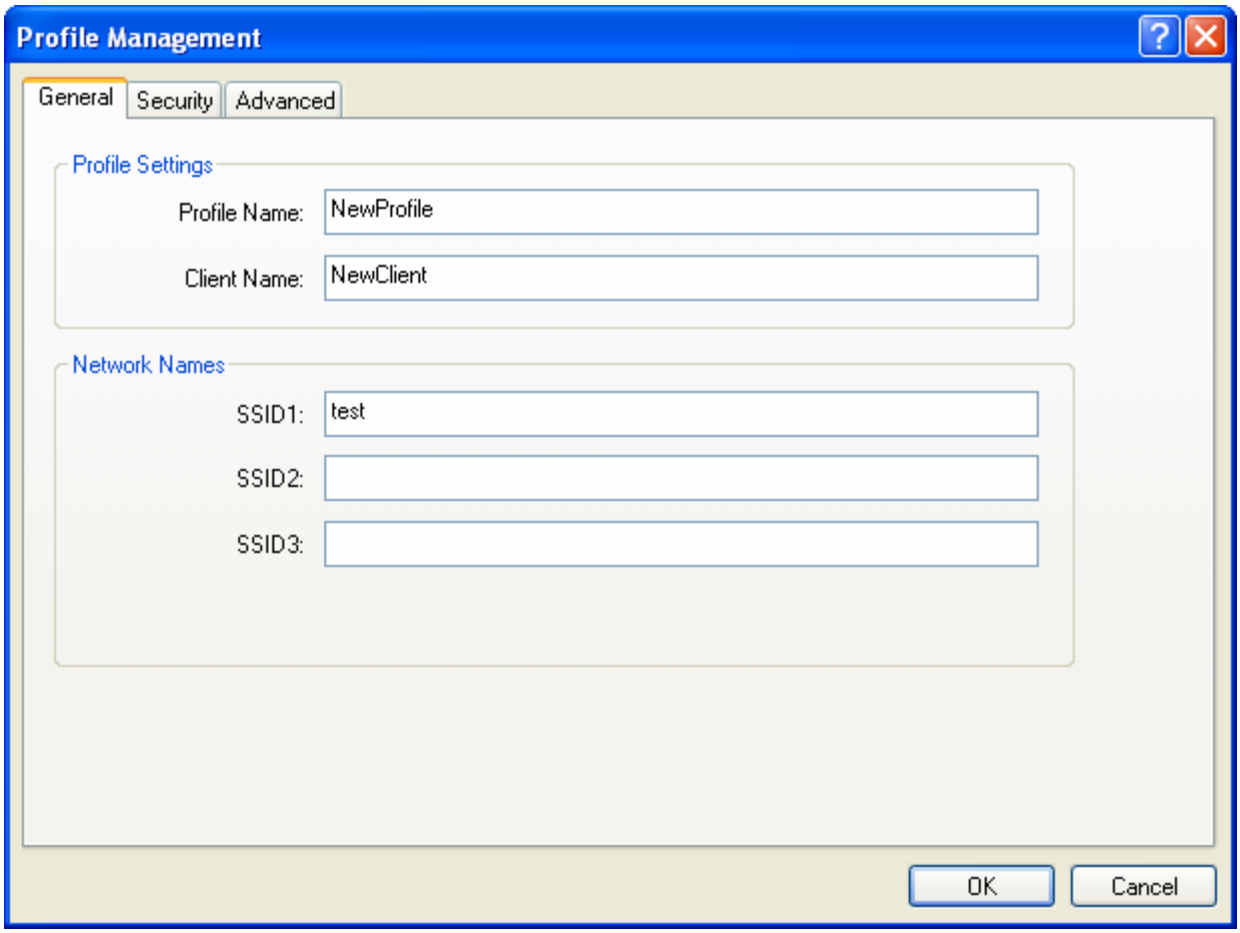

Figure 3-3

2. Configure the Security tab

Click the Security tab to configure the security settings of the profile. To define the security mode, select the radio button of the desired security mode as follows.

☞ **Note:**

You must configure the security type and password to be the same as what is set up on your wireless router or access point. If you wish to connect to a wireless network that is secured (with password), please first gather the security type and password set up on your wireless router or access point.

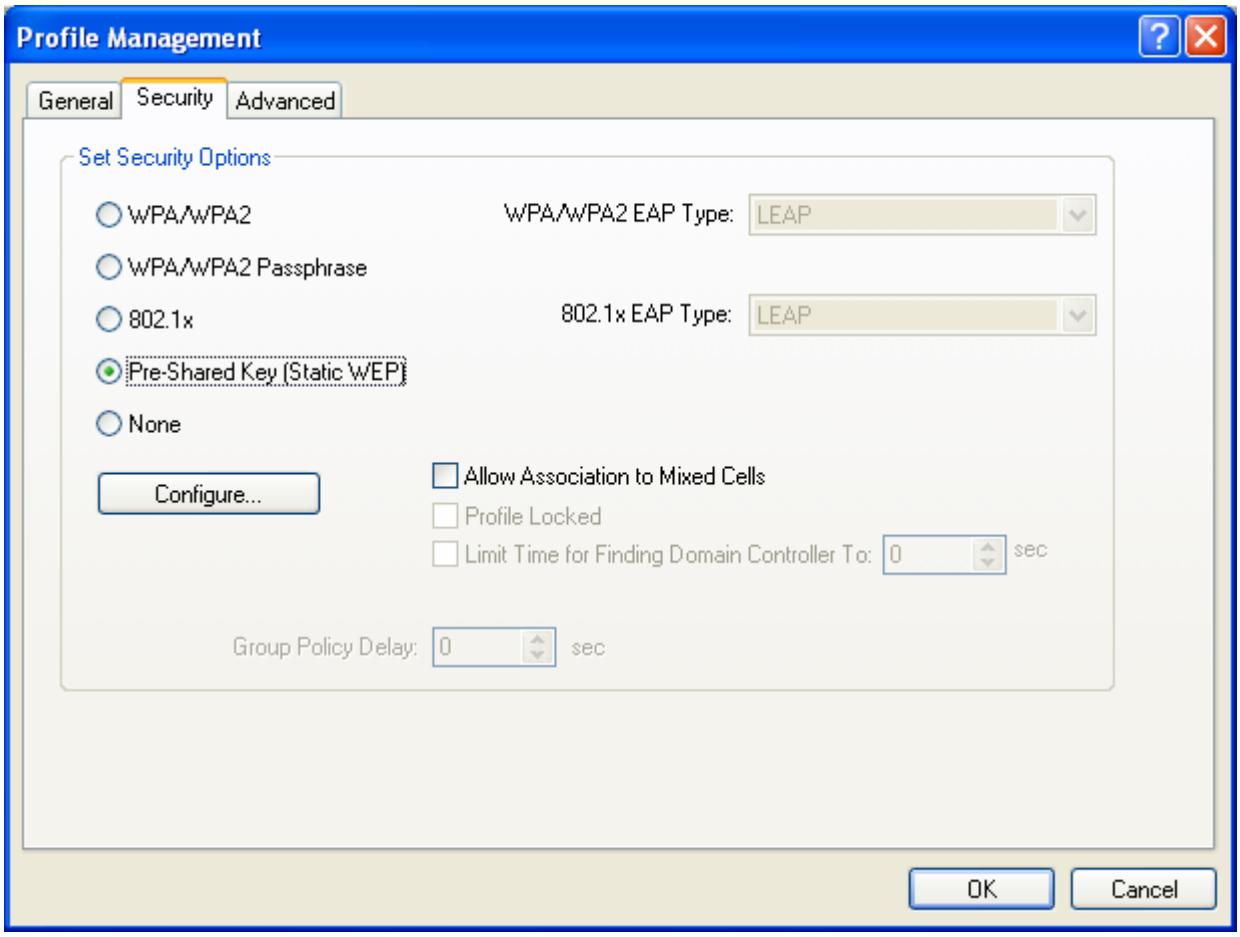

Figure 3-4

- **WPA/WPA2:** Wi-Fi Protected Access
- **WPA/WPA2 Passphrase:** Wi-Fi Protected Access Passphrase (Recommended for maximum security)
- **802.1x:** Enables 802.1x security.
- **Pre-Shared Key (Static WEP):** Enables the use of shared keys that are defined on both the access point and the station. To define shared encryption keys, choose the Shared Key radio button and click **Configure** to fill in the Define Shared Keys window (shown in Figure 3-5).
- **None:** No security (not recommended).

☞ **Note:**

1. The **WEP** security mode is not available for 802.11n.
2. If the access point which the Adapter is associated has WEP set and the client has WEP enabled, make sure that **Allow Association to Mixed Cells** is checked on the Security tab to allow association. To complete WEP encryption configuration, you must select the 802.11 Authentication Mode as appropriate on the **Advanced** tab of this **Profile Management** dialog.

To configure the Encryption Keys under the Pre-Shared keys (Static WEP) Security mode:

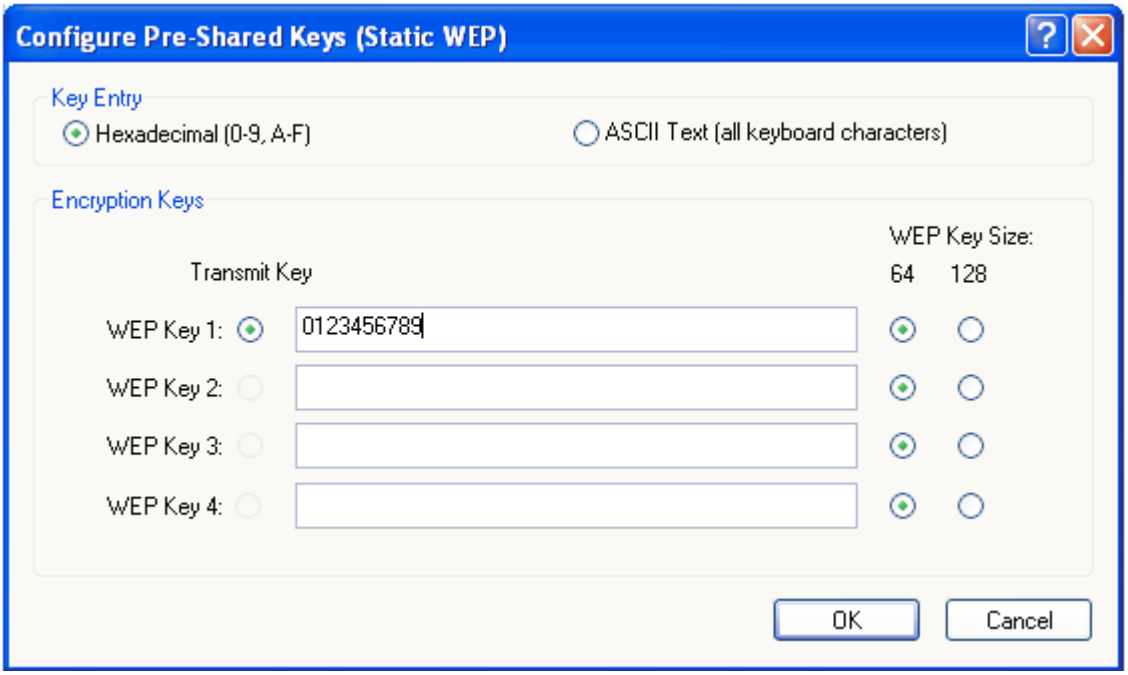

Figure 3-5

Note:

Select different **Security Options**, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

3. Configure the Advanced tab

This screen below allows you to make advanced configuration for the profile.

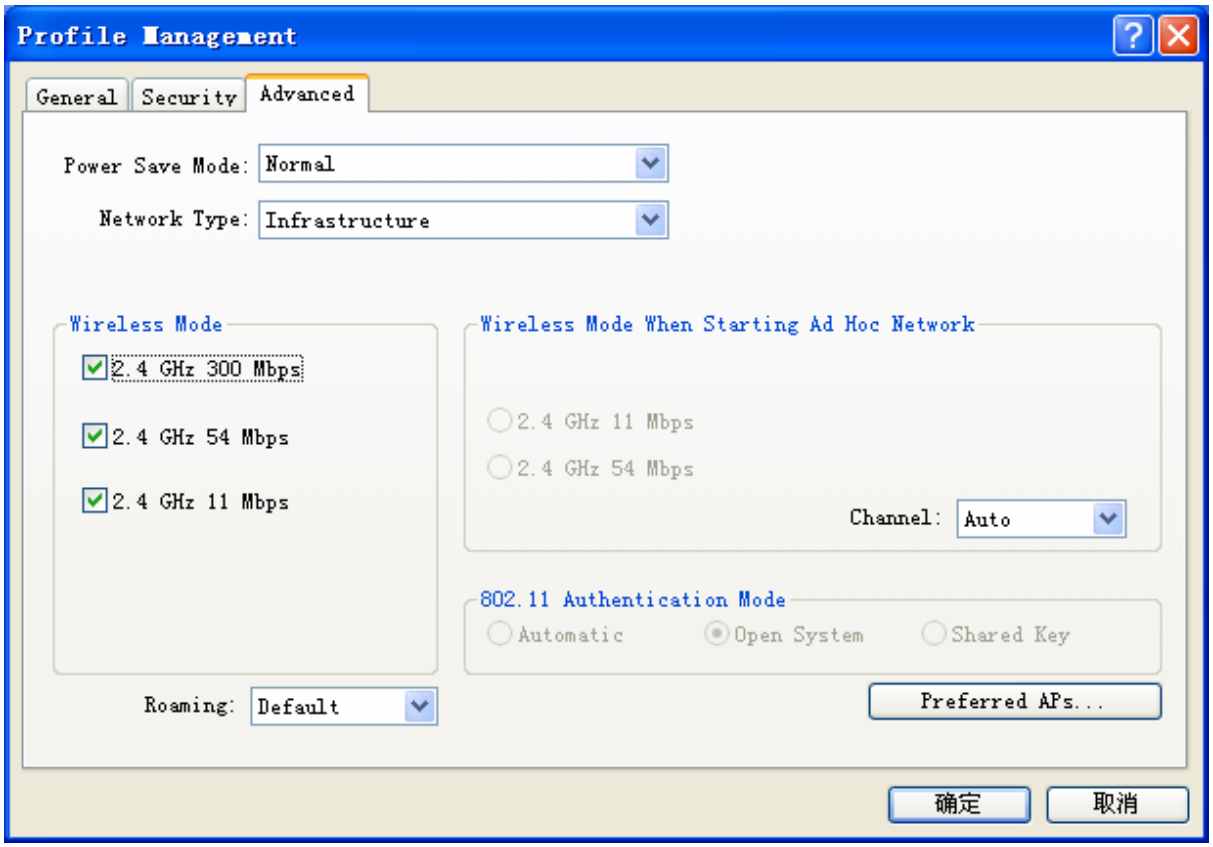

Figure 3-6

- **Power Save Mode -** Please select the power save mode from the drop-down list.
  - **Maximum -** Selects maximum mode to let the access point buffer incoming messages for the Adapter. The Adapter will detect the access point if any messages are waiting periodically.
  - **Normal (Default) -** Normal mode uses maximum when retrieving a large number of packets and switches back to Power Save mode after retrieving the packets.
  - **Off -** Powers up the Wireless USB Adapter continuously for a short message response time.
- **Network Type:**
  - **Infrastructure -** All wireless clients connect to a single access point or wireless router.
  - **Ad-Hoc -** Two or more wireless clients communicate directly to each other. Ad-hoc mode is also known as peer-to-peer communication. To set up an ad-hoc network, configure all the clients (such as two or more SMCWUSB-N2) in ad-hoc mode. Use the same SSID and channel for each other.

Note:

1) An Infrastructure network contains an Access Point or wireless router. All the wireless devices or clients will connect to the wireless router or access point.

2) An Ad-Hoc network contains only clients, such as laptops with wireless desktop adapters. All

the adapters must be in Ad-Hoc mode to communicate.

- **Wireless Mode**: Specifies 2.4 GHz 300 Mbps, 2.4 GHz 54 Mbps or 2.4 GHz 11 Mbps operation in an access point network. The Wireless adapter must match the wireless mode of the access point with which it associates.
- **Wireless Mode when Starting an Ad Hoc Network**: Specifies 2.4 GHz 300/54/11 Mbps to start an Ad Hoc network if no matching network name is found after scanning all available modes. This mode also allows the selection of the channel that the Wireless Adapter uses. The channels available depend on the regulatory domain. If the adapter finds no other ad hoc adapters, the channel that the adapter starts the ad hoc network with will be selected automatically. The Adapter must match the wireless mode and channel of the clients it associates.
- **802.11 Authentication Mode**: Select which mode the Adapter uses to authenticate to an access point:
  - **Automatic** causes the adapter to attempt authentication using shared, but switches it to open authentication if shared fails.
  - **Open System** enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match.
  - **Shared-key** only allows the adapter to associate with access points that have the same WEP key.

For infrastructure (access point) networks, click **Preferred APs…** to specify up to four access points for the client adapter. Enter the MAC Addresses for the preferred access points. The four access points have different priorities; the frontal has the higher priority.

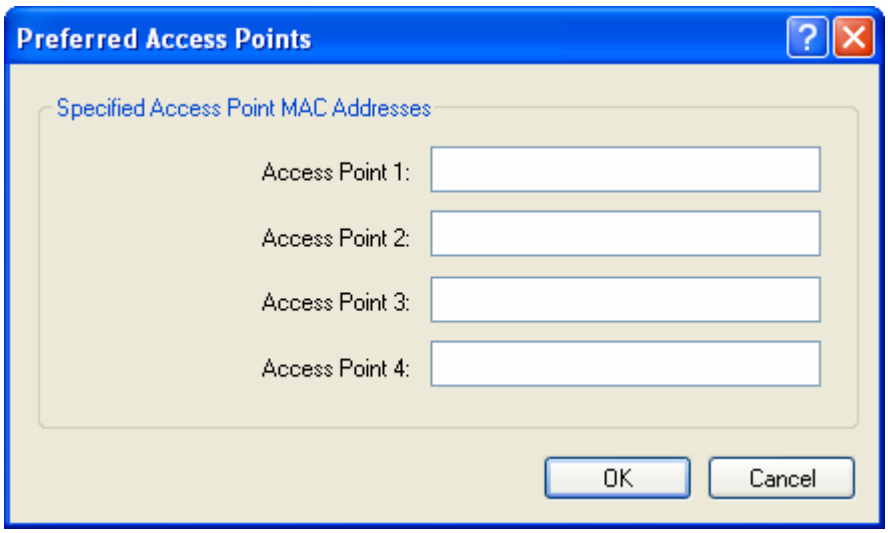

Figure 3-7

3.2.2 Remove a profile

1. Go to the Profile Management tab (shown in Figure 3-2).
2. Select the profile name in the Profiles List.
3. Click **Remove**.

☞ **Note:**

The profile being used cannot be removed.

3.2.3 Switch to another Profile

1. Go to the Profile Management tab (shown in Figure 3-2).
2. Select the profile name required in the Profiles List.
3. Click **Activate**.

3.2.4 Export a Profile

1. On the Profile Management tab (shown in Figure 3-2), highlight the profile to export.
2. Click **Export…**, the Export Profile window will appear as below.
3. Browse the directory to export the profile to.
4. Click **Save**. The profile should then be exported to the specified location.

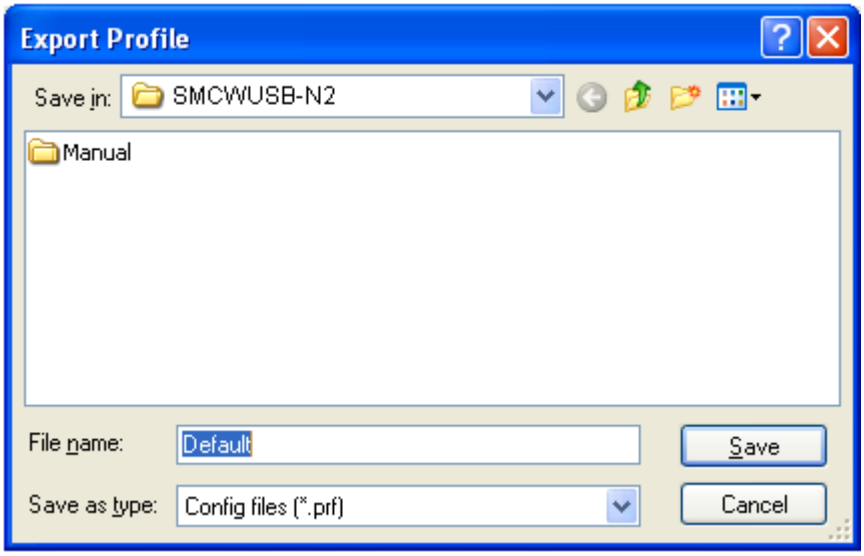

Figure 3-8

3.2.5 Import a Profile

1. From the Profile Management screen (shown in Figure 3-2), click **Import…**. The Import Profile will appear as below.
2. Browse to the directory where the profile is located.
3. Highlight the profile name.

4. Click **Open**, the imported profile will then appear in the Profiles List.

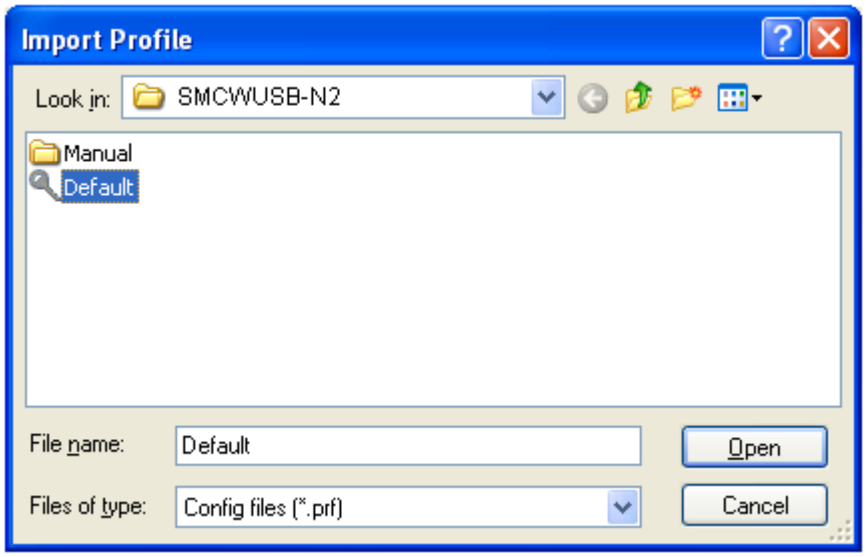

Figure 3-9

3.2.6 Scan Available Networks

1. Click **Scan** on the Profile Management tab (Figure 3-2), the Available Infrastructure and Ad Hoc Networks window will appear as below.

2. Click **Refresh** to refresh the list at any time.

3. Highlight a Network Name (SSID) and click **Activate** to connect to the network. If no configuration profile exists for that network, the Profile Management window will open the **General** tab. Fill in the Profile name and click **OK** to create the configuration profile for the network.

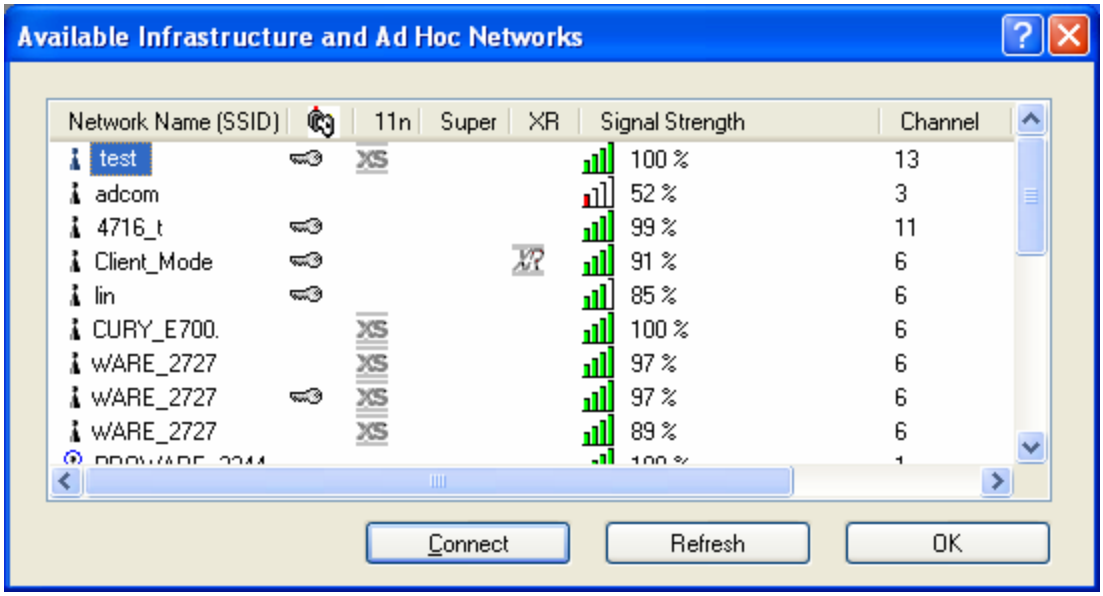

Figure 3-10

3.2.7 Auto Profile Selection Management

The auto selection feature allows the adapter to automatically select a profile from the list of profiles and use it to connect to the network. To add a new profile into the Auto Selected Profiles list, please follow these steps.

1. On the Profile Management screen (Figure 3-2), click **Order Profiles…**.
2. The Auto Profiles Selection Management window will appear (Figure 3-11) with a list of created profiles in the Available Profiles section.

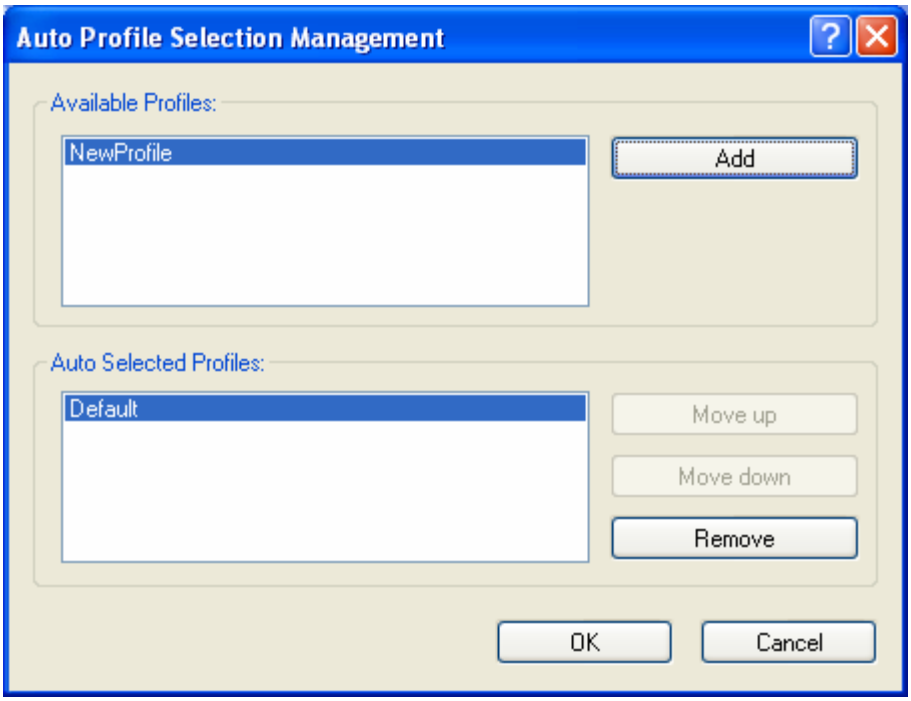

Figure 3-11

3. Highlight the profile to add to Auto Selected Profiles and click **Add**. The profile will appear in the Auto Selected Profiles box.
4. Highlight a profile in the Auto Selected Profiles box.
5. Click **Move Up** or **Move Down** as appropriate.

☞ **Note:**

The first profile in the Auto Selected Profiles box has highest priority, while the last profile has the lowest priority.

6. Click **OK**.
7. Check the **Auto Select Profiles** checkbox on the **Profile Management** tab (Figure 3-2).

☞ **Note:**

When auto profile selection is enabled by checking **Auto Select Profiles** on the **Profile Management** tab, the adapter will scan for an available network. The profile with the highest

priority and the same SSID as one of the found networks will be selected for network connection. If the connection fails, the client adapter will try the next highest priority profile that matches the SSID until a successful network connection is built.

3.3 Diagnostics

The **Diagnostics** tab of the SMCWUSB-N2 Wireless Utility provides tools to retrieve receiving and transmitting statistics. The Diagnostics tab does not require any configuration.

The Diagnostics tab lists the following receiving and transmitting diagnostics for frames received or transmitted by the SMCWUSB-N2 adapter:

- Multicast frames transmitted and received
- Broadcast frames transmitted and received
- Unicast frames transmitted and received
- Total bytes transmitted and received

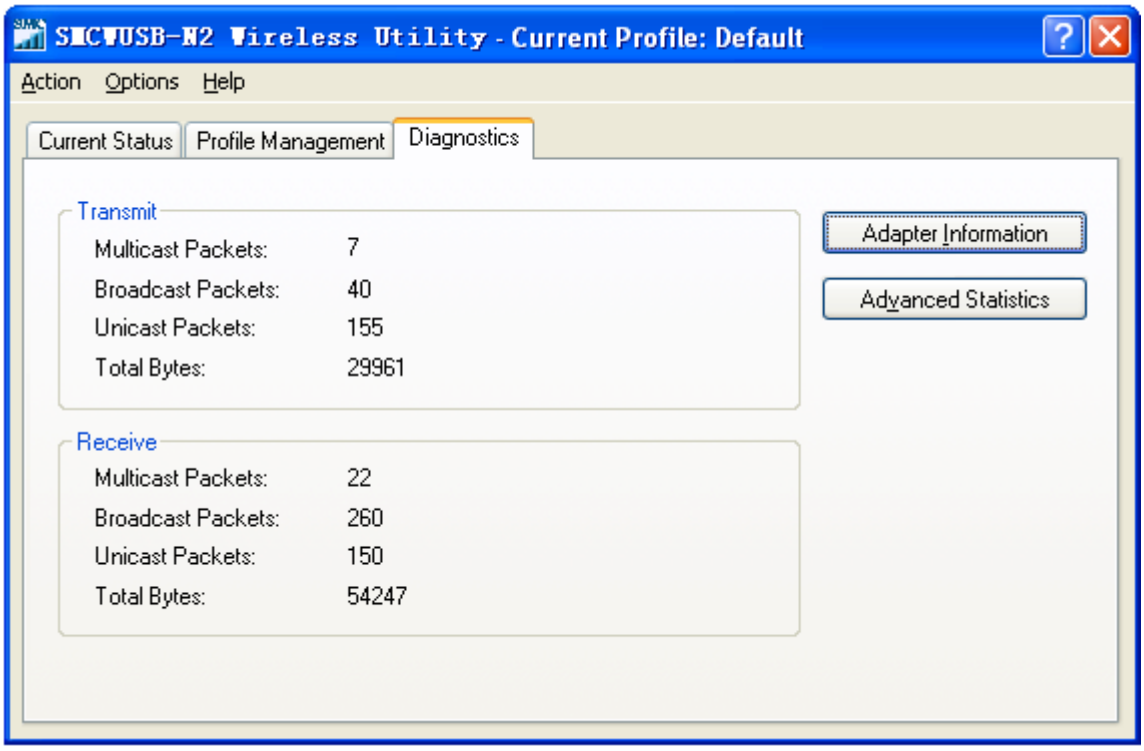

Figure 3-12

3.3.1 Check Driver Information

Click the **Adapter Information** button in the screen above to view the adapter information, including general information about the wireless network adapter and the Network Driver Interface Specification (NDIS) driver. Access the adapter information from the Diagnostics tab.

- **Card Name -** The name of the wireless network adapter.

- **MAC Address -** The MAC address of the wireless network adapter.
- **Driver -** The driver name and path of the wireless network adapter driver.
- **Driver Version -** The version of the wireless network adapter driver.
- **Driver Date -** The creation date of the wireless network adapter driver.
- **Client Name -** The name of the client computer.

3.3.2 Check Receive and Transmit Statistical Information

The **Advanced Statistics** screen shows detailed receiving and transmitting diagnostics for the SMCWUSB-N2 adapter.

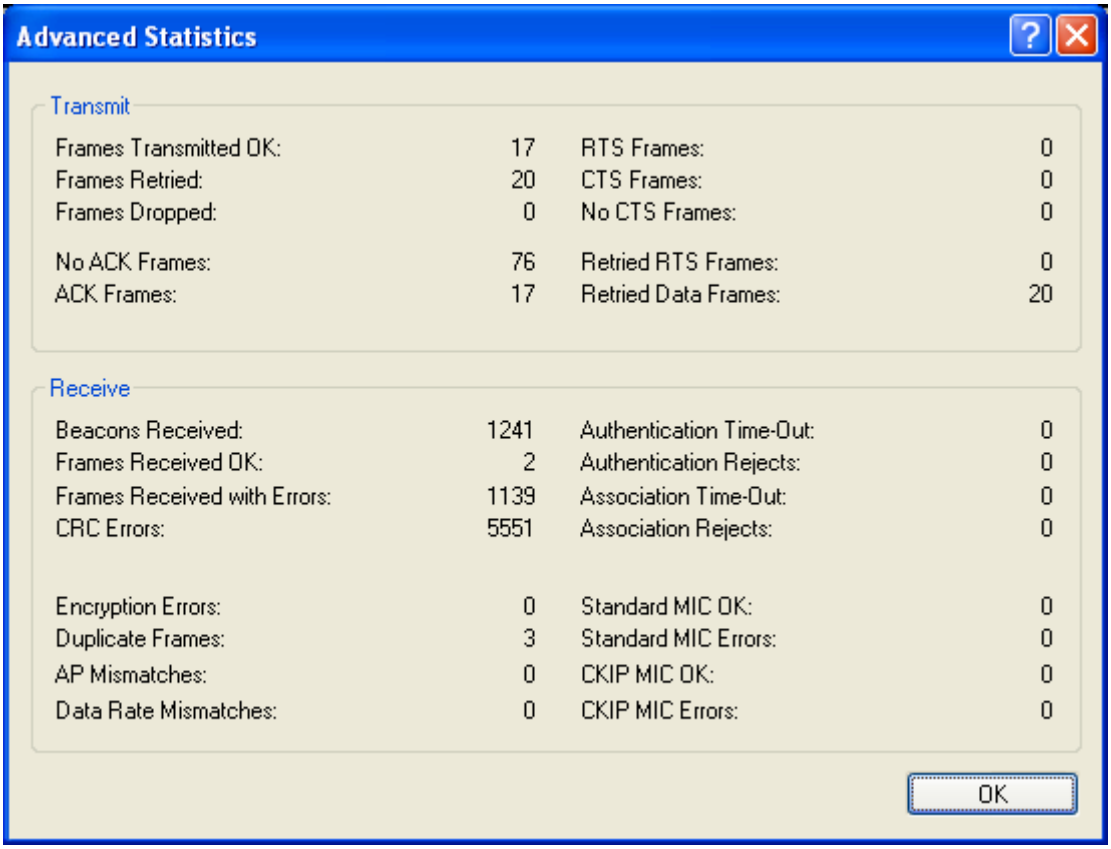

Figure 3-13

Chapter 4. Configuration for Windows Vista

After installing the SMCWUSB-N2 adapter on Windows Vista, the Wireless Network Connection message box appears.

Figure 4-1

A green icon indicates that the connection has been established. A gray icon indicates no connection.

If the icon does not appear, please follow the steps below. If the icon still does not appear, the driver may be installed incorrectly or the adapter is unplugged, please try again.

1. Right-click the icon in your system tray, then click **Connect to a network**.

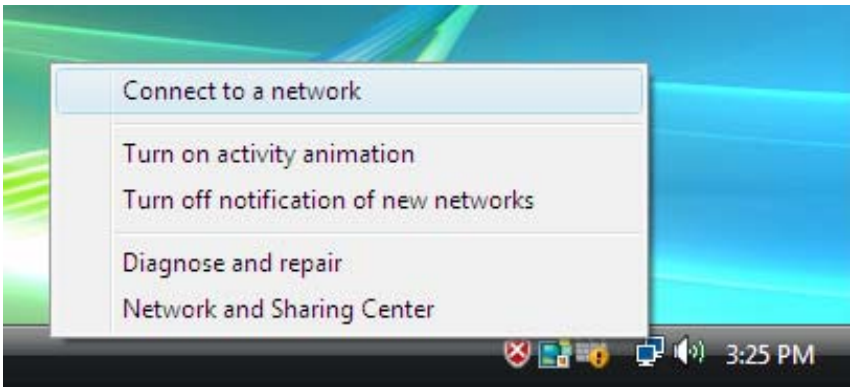

Figure 4-2

2. The screen that appears displays available wireless networks. Highlight the network that you wish to connect to and click **Connect**.

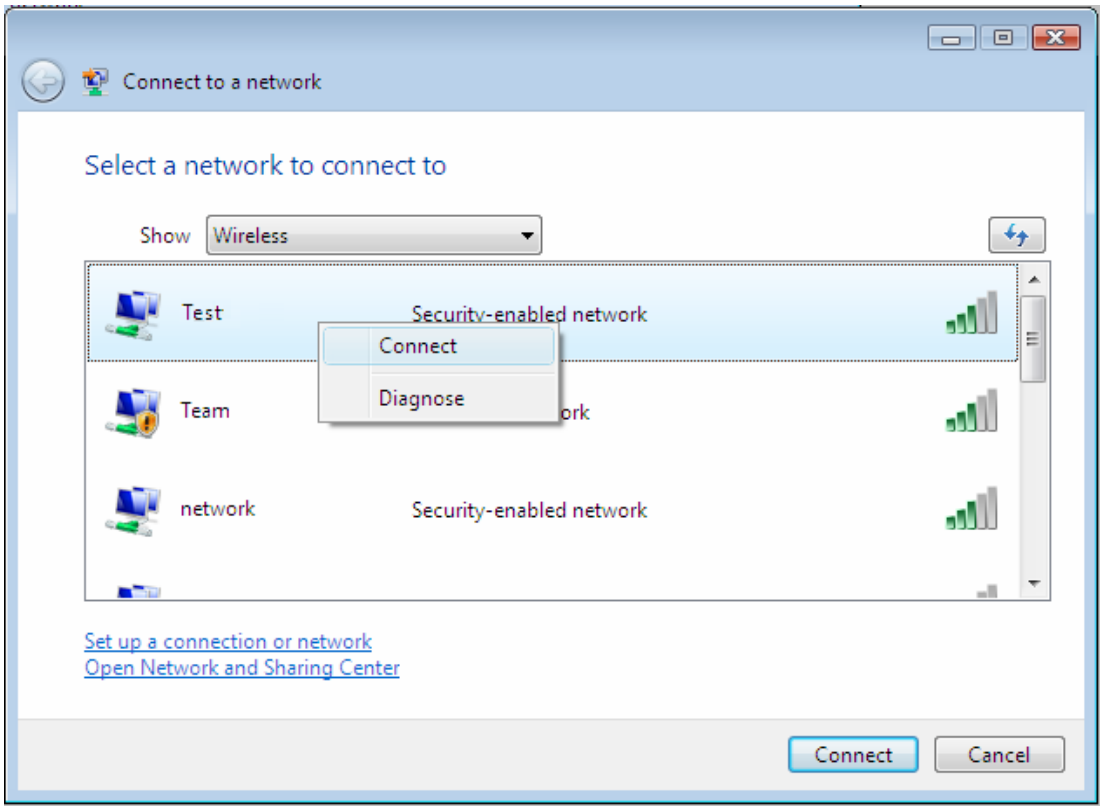

Figure 4-3

3. To continue, click **Connect Anyway**. Click the **Cancel** button to end the Installation.

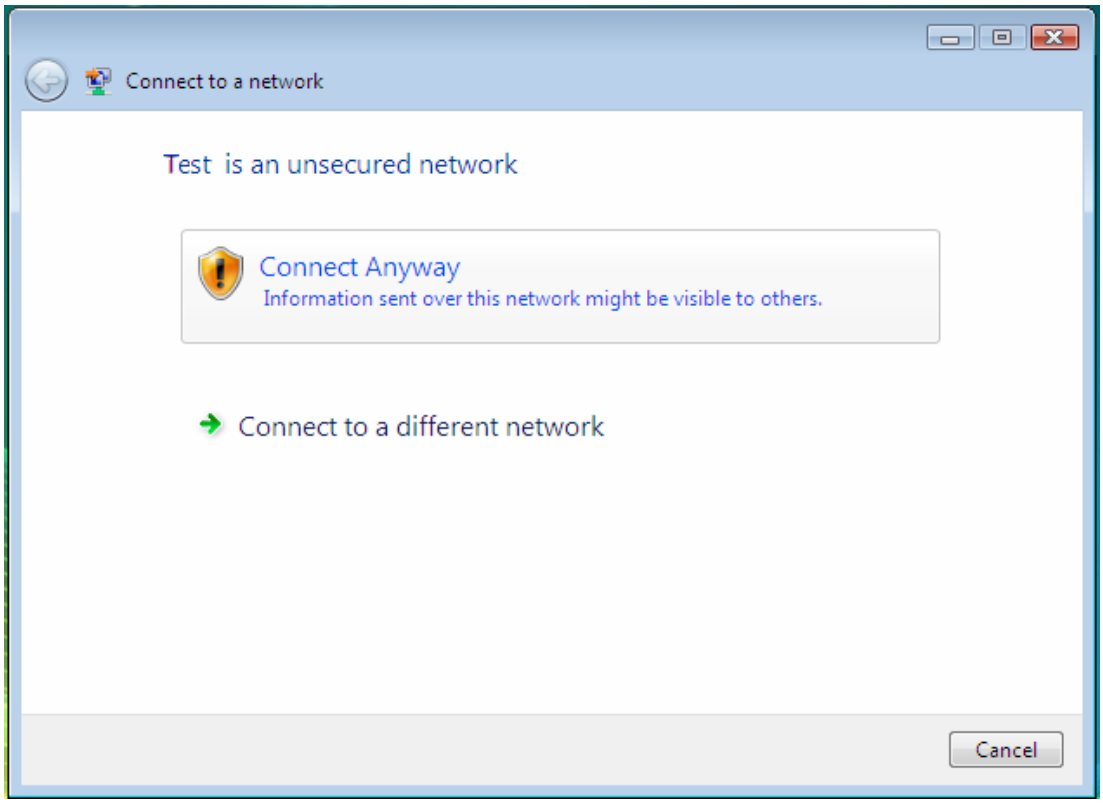

Figure 4-4

4. Click **close** to exit.

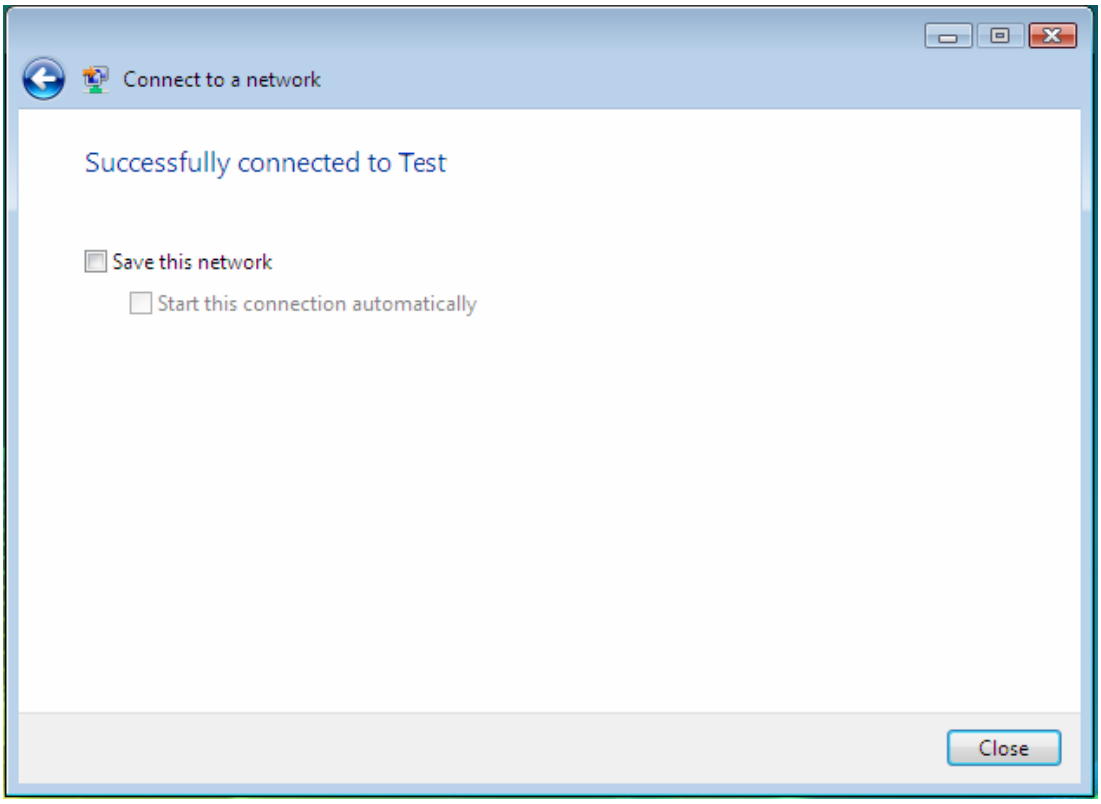

Figure 4-5

5. The screen below will appear if the connection is successful.

Figure 4-6

Chapter 5. WPS configuration

The Wi-Fi Protected Setup (WPS) function allows you to establish a wireless connection with your WPS-enabled wireless router or access point easily, using either Push Button Configuration (PBC) method or PIN method.

Install the WPS software on your computer. Insert the EZ Installation & Documentation CD into your CD-ROM drive. The CD will auto run. Click **Install/Remove WPS (WiFi Protected Setup)**.

Figure 5-1

Follow the on-screen instructions to complete the WPS installation. After that, the WPS function can be enabled. The following section introduces two ways to configure WPS.

5.1 PBC (Push Button Configuration) method

1. On the management interface of your wireless router/AP, make sure WPS is enabled.

   Press the WPS button on your WPS-enabled wireless router or access point for 4 seconds.

   Within two minutes, press the WPS button on the SMCWUSB-N2 adapter to join the wireless network.

2. Double click the WPS icon on the desktop to start the WPS Utility. Click **Next** to continue.

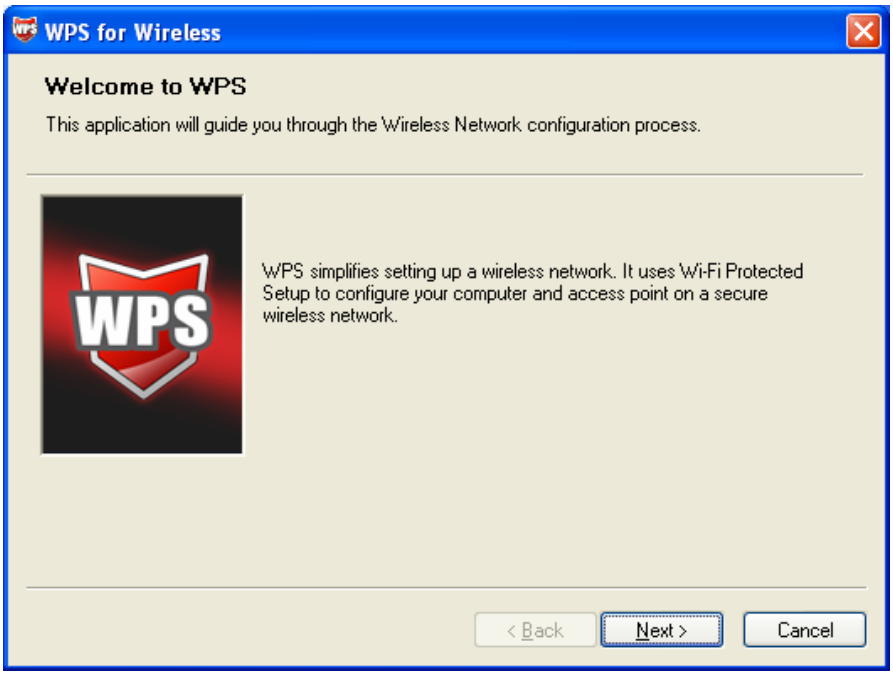

Figure 5-2

3. Select **Push the button on my access point** and click **Next**.

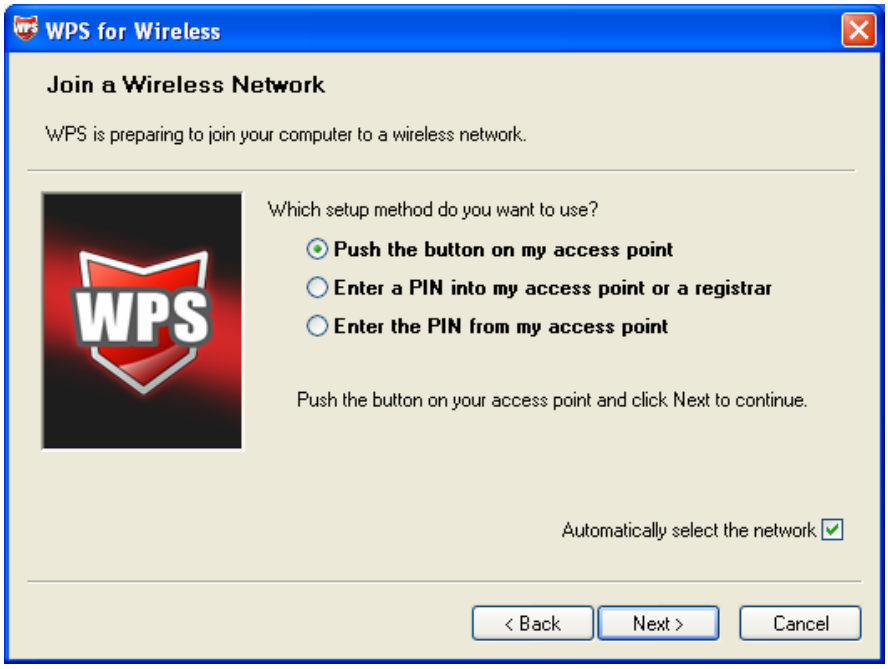

Figure 5-3

4. Wait for the following screen to appear. Click **Finish** to complete the WPS configuration.

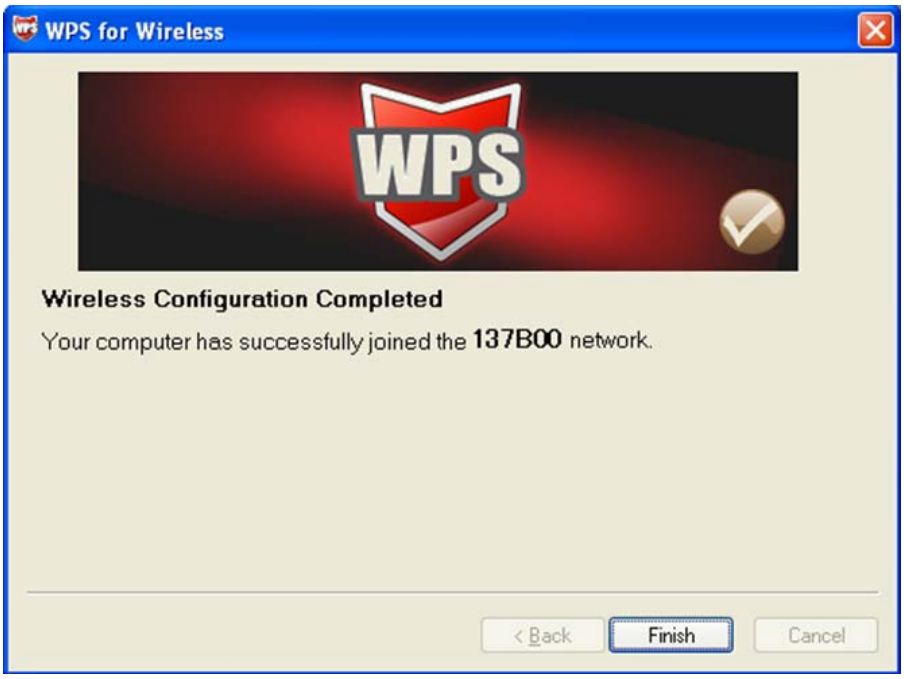

Figure 5-4

5.2 PIN method

There are two ways to configure the WPS by **PIN method**:

1) Enter the PIN for SMCWUSB-N2 into your AP device

2) Enter the PIN from your AP device into the SMCWUSB-N2 Wireless Utility.

Following are the detailed configuration procedure of each way.

5.2.1 Enter a PIN into your AP device

1. Double click the icon  on the desktop to open the WPS Utility. Click **Next** to continue.

   Select the second option **Enter a PIN into my access point or a registrar**. Remember the PIN displayed in the screen and click **Next**.

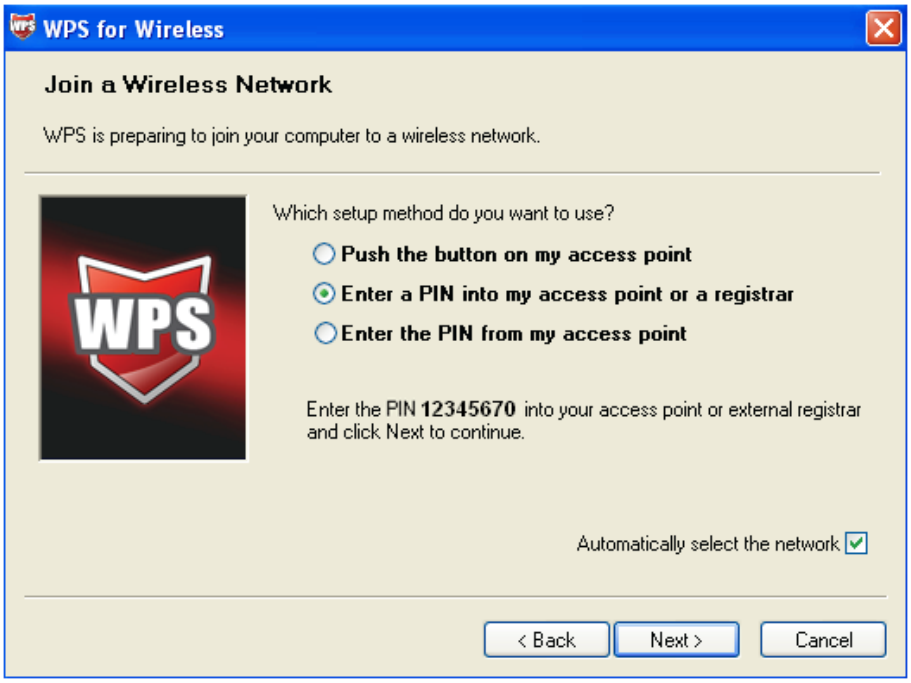

Figure 5-5

2. On the management interface of your wireless router/AP, select **PIN** as the WPS method. **Enter** the PIN value shown in Figure 5-5 and connect.

5.2.2 Enter the PIN from your AP device

1. Open the WPS Utility and click **Next** to continue. Select the third option **Enter the PIN from my access point**. Enter the PIN value of your router or access point. The PIN value can usually be found on the bottom of the device or from the management interface of your router/AP. Click **Next**.

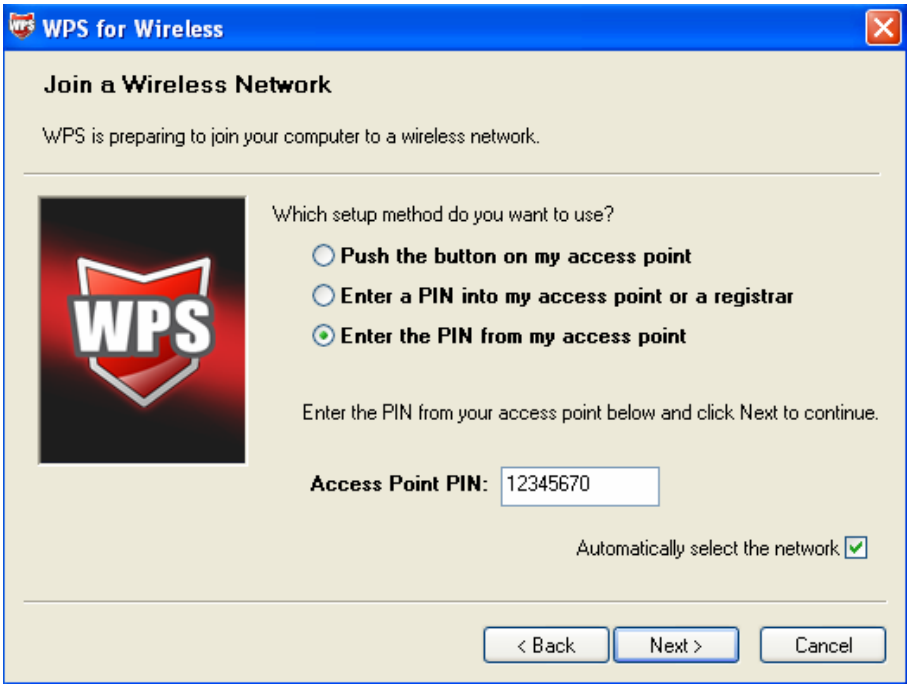

Figure 5-6

2. When Figure 5-4 appears, the WPS configuration is complete.

☞ **Note:**

If you generate a new PIN code for your router or access point, please enter the new one instead.

Appendix A: Specifications

General Specifications	
Interface	USB 2.0 Interface
Standards	IEEE802.11n (draft); IEEE802.11g; IEEE802.11b
Operating System	Windows 2000, XP and Vista
Radio Data Rate	11b：1/2/5.5/11Mbps 11g：6/9/12/18/24/36/48/54Mbps 11n：Up to 300Mbps
Modulation	11b: CCK,QPSK,BPSK; 11g: OFDM; 11n: QPSK,BPSK,16-QAM,64-QAM
Media Access Protocol	CSMA/CA with ACK
Data Security	WPA/WPA2; 64/128-bit WEP; TKIP/AES
Frequency	2.4 ~ 2.4835GHz
Spread Spectrum	Direct Sequence Spread Spectrum (DSSS)
Safety & Emissions	FCC, CE

Environmental and Physical Specifications	
Operating Temp.	0 ~40°C (32 ~104°F)
Storage Temp.	-20 ~ 70°C (-4 ~158°F)
Humidity	10% ~ 95% RH, Non-condensing

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)[3] 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 -** (**D**irect-**S**equence **S**pread **S**pectrum) **-** 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 -** (**F**requency **H**opping **S**pread **S**pectrum) **-** 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).

- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

- **WEP -** (**W**ired **E**quivalent **P**rivacy) **-** 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 -** (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

- **WPA -** (**W**i-Fi **P**rotected **A**ccess) **-** A wireless security protocol that uses TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.