

# **2.4GHz Wireless 802.11n (DRAFT) CardBus Card**

## **User's Guide**

**Version 0.9**

## **Copyright**

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Copyright 2006

Version 1.0 (June, 2006)

## **Disclaimer**

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

## **Trademark recognition**

All product names used in this manual are the properties of their respective owners and are acknowledged.

## 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.

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

### IMPORTANT NOTE:

#### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

End users must follow the specific operating instructions for satisfying RF exposure compliance.

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

SAR compliance has been established in typical laptop computer(s) with CardBus  slot, and product could be used in typical laptop computer with CardBus slot. Other  application like handheld PC or similar device has not been verified and may not  compliance with related RF exposure rule and such use shall be prohibited.

U-MEDIA declares that US model of WCB-370A (FCC ID: SI5WCB370A) is limited  in CH1-CH11 for 2.4G band by specific firmware controlled by the manufacturer and  is not user changeable.

## **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.

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

# Table of Contents

Federal Communications Commission (FCC) Interference statement	3
CE Mark Warning	4
<b>Chapter 1 – Wireless LAN Networking</b>	
Transmission Rate	6
Type of Wireless Networks	6
Ad-Hoc (IBSS) Network	6
Infrastructure (BSS) Network	7
Wireless LAN Security	11
Data Encryption with WEP	11
<b>Chapter 2 - Getting Started</b>	
About Your Card	12
Package Content	12
System Requirement	12
LED Definition	12
Wireless Utility and Card Hardware Installation	13
Using the Utility to Configure Your Network	17
Link Information	17
Site Survey	19
Profile	20
<b>Chapter 3 – Maintenance</b>	
Uninstalling the Driver	25
Uninstall the Client Utility	25
Upgrading the Wireless Utility	25
<b>Glossary</b>	<b>26</b>

# Chapter 1- Wireless LAN Networking

This section provides background information on wireless LAN networking technology.



---

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

---

## Transmission Rate (Transfer Rate)

---

The card provides various transmission (data) rate options for you to select. Options include Fully Auto, 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 22 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps and 108Mbps. In most networking scenarios, the factory default Fully Auto setting proves the most efficient. This setting allows your card to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the card automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the card gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

## Types of Wireless Networks

---

Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

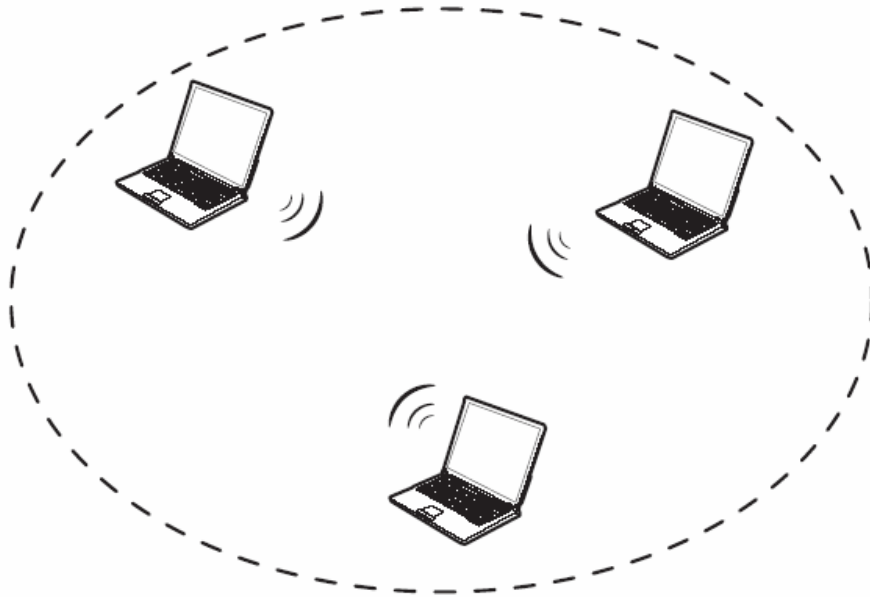
To connect to a wired network within a coverage area using access points, set the card operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

### **AD-HOC (IBSS) NETWORK**

Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each .

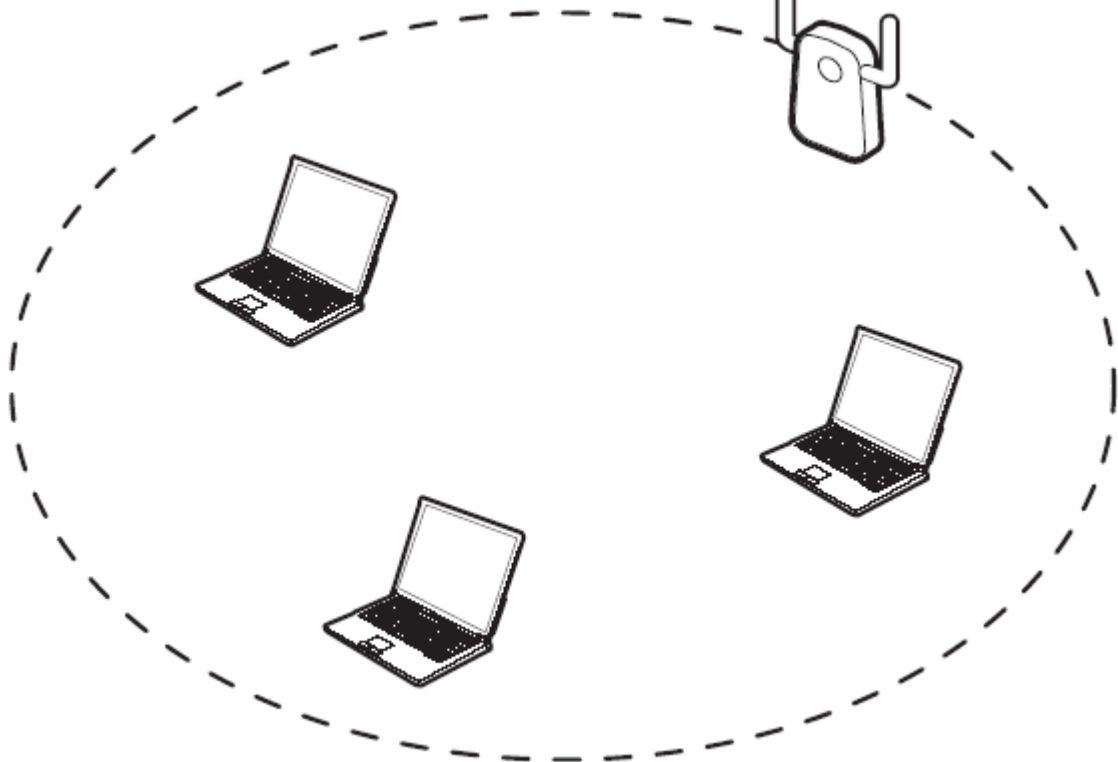
Ad-hoc IBSS



Ad-hoc (also known as peer-to-peer) network diagram

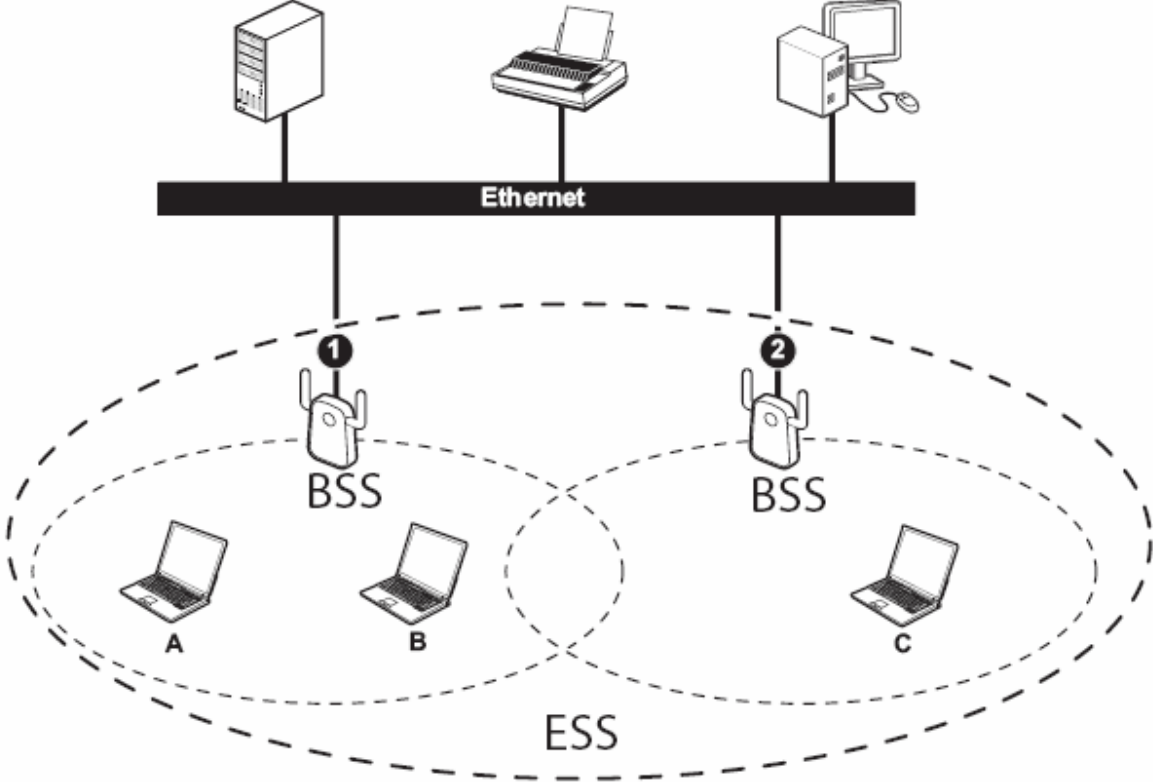
When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).

Infrastructure BSS



Infrastructure (IBSS) network diagram

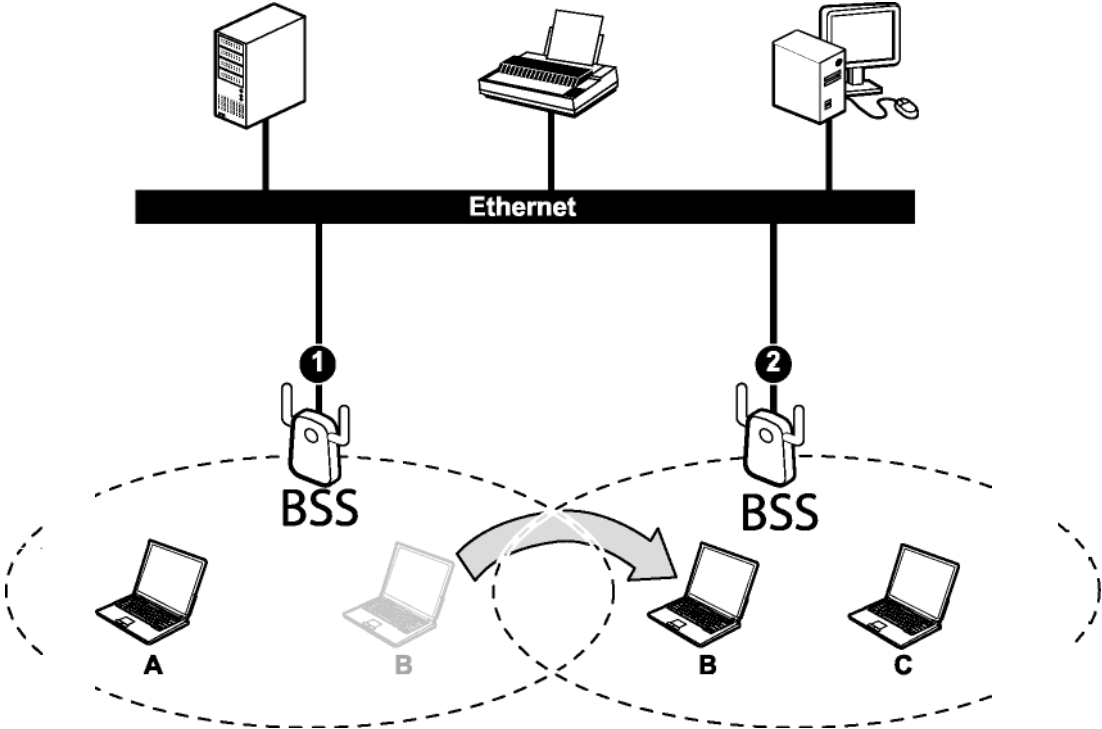
In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.



Infrastructure (ESS) network diagram



In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the card automatically switches to the channel used in BSS (2).



Roaming in an ESS network diagram



## WIRELESS LAN SECURITY

Because wireless networks are not as secure as wired networks, its vital that security settings are clearly understood and applied.



DO NOT ATTEMPT TO CONFIGURE OR CHANGE SECURITY SETTINGS FOR A NETWORK WITHOUT AUTHORIZATION AND WITHOUT CLEARLY UNDERSTANDING THE SETTINGS YOU ARE APPLYING. WITH POOR SECURITY SETTINGS, SENSITIVE DATA YOU SEND CAN BE SEEN BY OTHERS.

---

The list below shows the possible wireless security levels on your card starting with the most secure. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. EAP requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or the LAN to provide authentication service for wireless stations.

1. Wi-Fi Protected Access (WPA)
2. IEEE802.1X EAP with RADIUS Server authentication
3. WEP Encryption
4. Unique ESSID

### DATA ENCRYPTION WITH WEP

The WEP (Wired Equivalent Privacy) security protocol is an encryption method designed to try to make wireless networks as secure as wired networks. WEP encryption scrambles all data packets transmitted between the card and the access point or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your card.

- Automatic WEP key generation based on a password phrase called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN cards with this feature in the same WLAN.
- For WLAN cards without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the wireless utility and entering them manually as the WEP keys in the other WLAN card(s).

The card allows you to configure up to four WEP keys and only one key is used as the default transmit key at any one time.

# Chapter 2 - Getting Started

This chapter introduces the Card and prepares you to use the Wireless Utility.

## 2.1 About Your Card

With the Card, you can enjoy wireless mobility within almost any wireless networking environment.

The following lists the main features of your Card.

- ✓ Automatic rate selection.
- ✓ Data transmission rates up to 300 Mbps
- ✓ Offers 64-bit and 128-bit WEP (Wired Equivalent Privacy) data encryption for network security.
- ✓ Supports IEEE802.1x and WPA (Wi-Fi Protected Access).
- ✓ Multiple antennas design.
- ✓ Driver support for Windows XP/2000.

## 2.2 Package Content

- The WLAN Card
- Installation and Manual CD
- Quick Start Guide
- Warranty/Registration Card

## 2.3 System Requirement

- Pentium class notebook computers with at least one available Type II CardBus slot
- Microsoft Windows XP or 2K
- CD-ROM drive

## 2.4 LED Definition

The following table describes the LED on the Card

STATUS	POWER LED	LINK LED
POWER OFF	OFF	OFF
POWER ON	Slow Blinking	OFF
Radio ON without association	Two LEDs slow blinking mutually	
Associated without traffic	Two LEDs slow blinking together	
Associated with traffic	Two LEDs blinking together per traffic amount	

## 2.5 Wireless Utility & Card Hardware Installation



IF YOU HAVE CONNECTED THE CARD TO YOUR COMPUTER, PLEASE REMOVE IT FIRST.

Follow the instructions below to install the Card and Utility.

### STEP 1

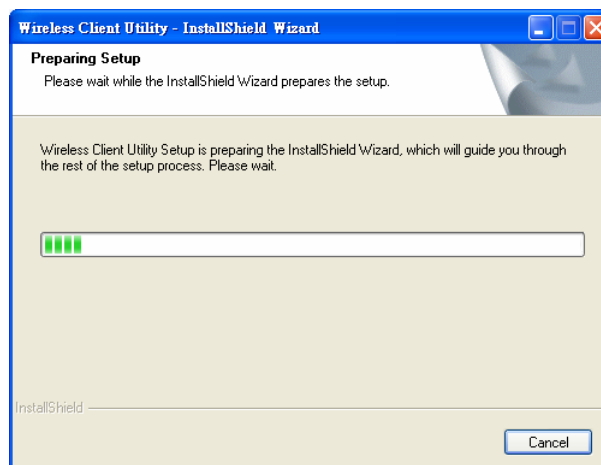
Insert the Driver and Utility CD into CD drive

### STEP 2

If your CD Autorun is enabled, the installation procedures will be started. (Otherwise open your CD folder and double-click on the “setup.exe” file)

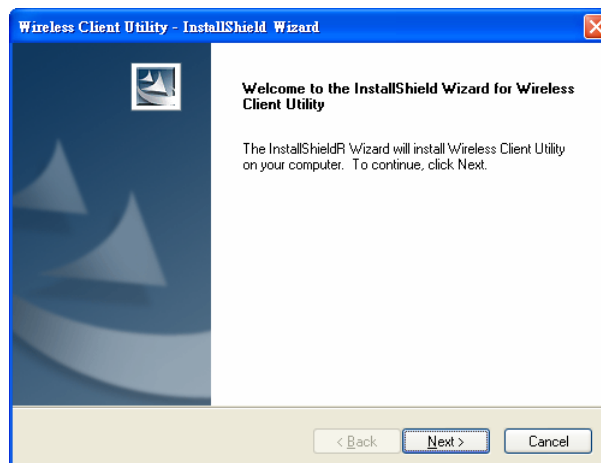
### STEP 3

The InstallShield Wizard prepares for installation.



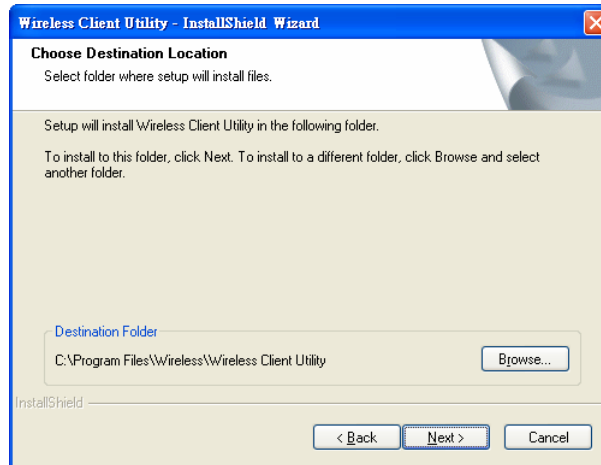
### STEP 4

The InstallShield Wizard prompts you for confirmation. Click **Next** on the following menu.



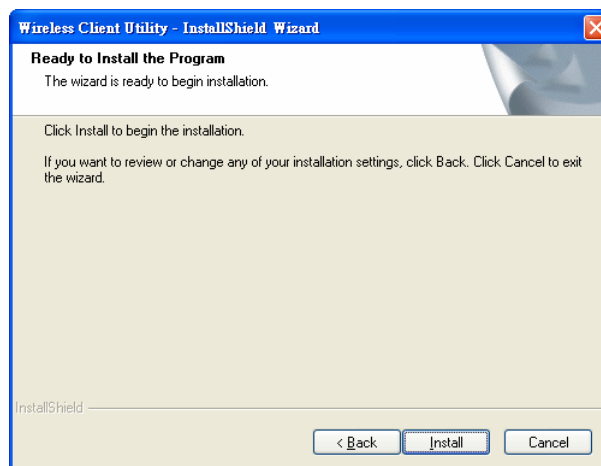
## STEP 5

In the destination Folder screen you are asked to confirm the Destination Folder for the application software. If you would like, you may change the destination folder to another location. Click **Next**



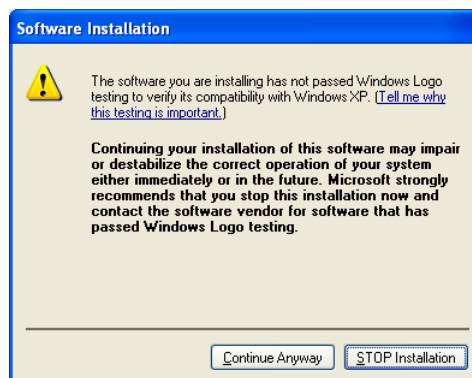
## STEP 6

The wizard is ready to begin installation. Click **Install** on it.



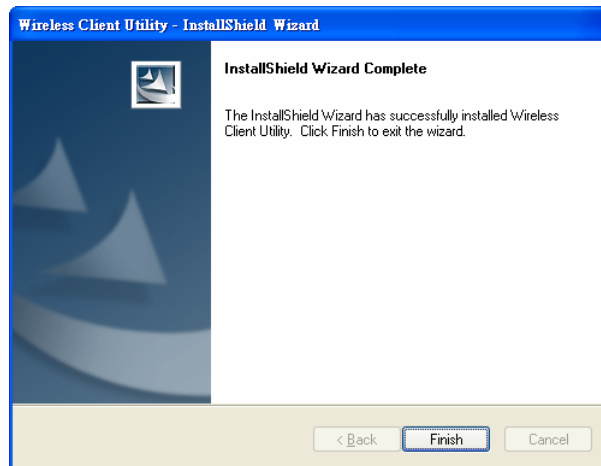
## STEP 7

At the Software Installation menu click **Continue Anyway**.



### STEP 8

Click **Finish** to complete the client utility installation.



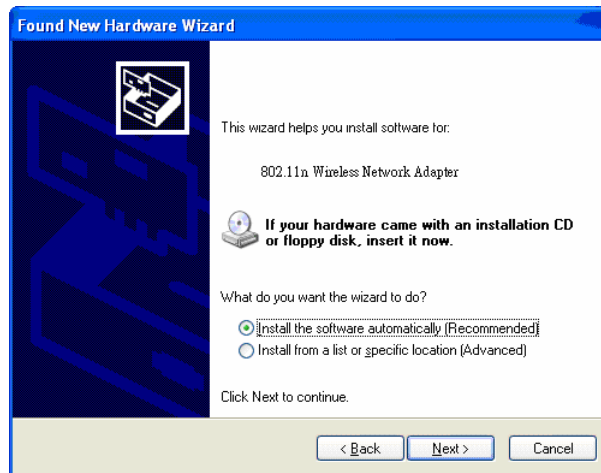
### STEP 9

At this moment please insert your Card to your Laptop, After the following window pop up, click **Next** on the Found New Hardware Wizard



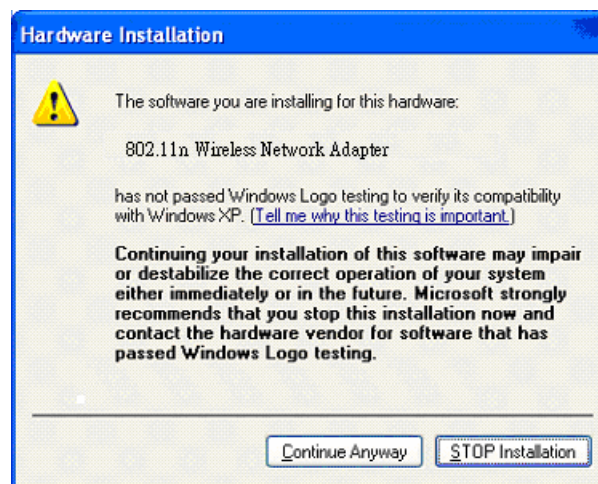
### STEP 10

Choose "Install the software automatically" , and click **Next**.



### STEP 11

Click "Continue Anyway".



### STEP 12

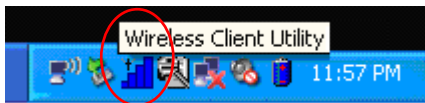
Click Finish to complete the installation.





## 2.6 Using the Utility to Configure Your Network

The following are explanations on how to configure and use the Utility program. After completing the installation procedure, a new icon as shown below will automatically appear in the lower right tray bar.



Hold your mouse pointer over the icon, and double click the left mouse button to open the Wireless Client Utility.

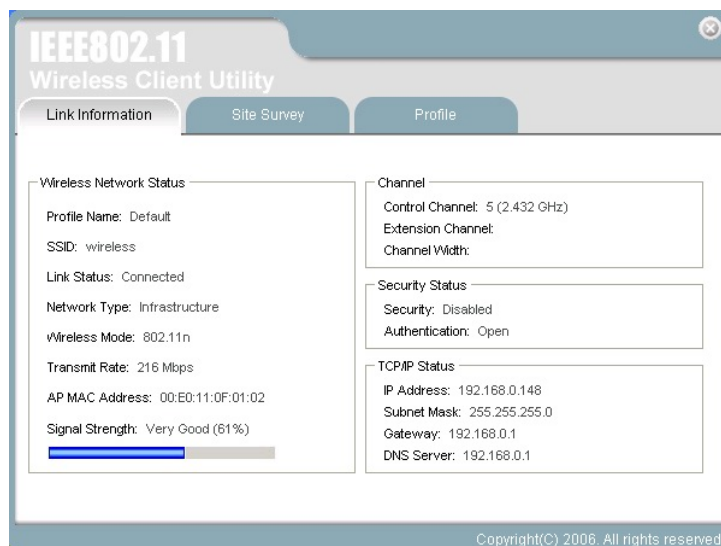
The Wireless Client Utility window as shown below will appear.



The user can now use any of the management functions available in the IEEE 802.11 Wireless Client Utility.

### 2.6.1 Link Information

Click the **Link Information** tab to see general information about the program and its operation.



The following table describes the items found on the Link Information screen.

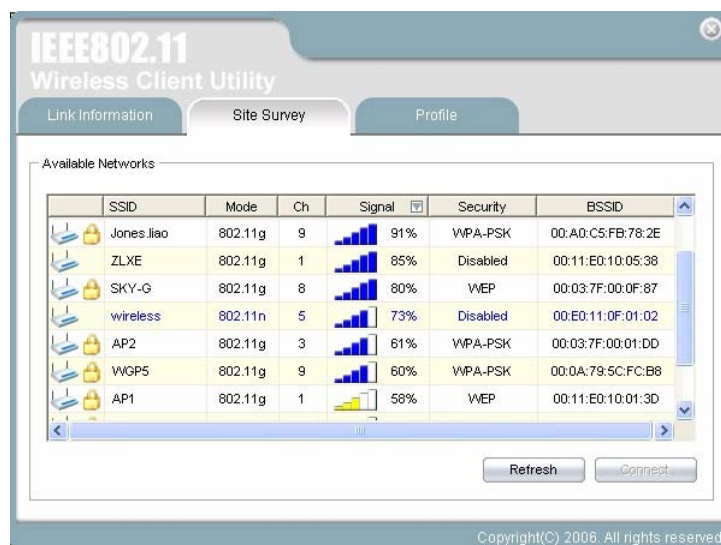
<b>Wireless Network Status</b>	
<b>Profile Name</b>	The name of the current selected configuration profile. Set up the configuration name on the <b>Profile tab</b> .
<b>SSID</b>	Displays the wireless network name.
<b>Link Status</b>	Shows whether the station is associated to the wireless network.
<b>Network Type</b>	The type of network the station is connected to. The options include: <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Infrastructure (access point)</b></li> <li><input type="checkbox"/> <b>Ad Hoc</b></li> </ul>
<b>Wireless Mode</b>	Displays the wireless mode. 802.11g, 11b or 11n
<b>Transmit Rate</b>	Displays the current transmit rate in Mbps.
<b>AP MAC Address</b>	Displays the MAC address of the access point the wireless card is associated to.
<b>Signal Strength</b>	Shows the strength of wireless signal.
<b>Channel</b>	
<b>Control Channel</b>	Channel number of the control 20MHz channel
<b>Extension Channel</b>	To locate the 40MHz channel on combination with the control channel
<b>Channel Width</b>	20MHz only or 40/20MHz channel support

<b>Security Status</b>	
<b>Security</b>	Shows the security type – Disable, WEP, WPA/WPA2, WAP-PSK/WAP2-PSK or 802.1X
<b>Authentication</b>	Displays the authentication mode.
<b>TCP/IP Status</b>	
<b>IP Address</b>	Displays the computer's IP address.
<b>Subnet Mask</b>	Displays subnet mask
<b>Gateway</b>	Displays gateway address
<b>DNS Server</b>	Display DNS server address

## 2.6.2 Site Survey

Click the **Site Survey** tab to see available infrastructure and ad hoc networks.

On this screen, click **Refresh** to refresh the list at any time.



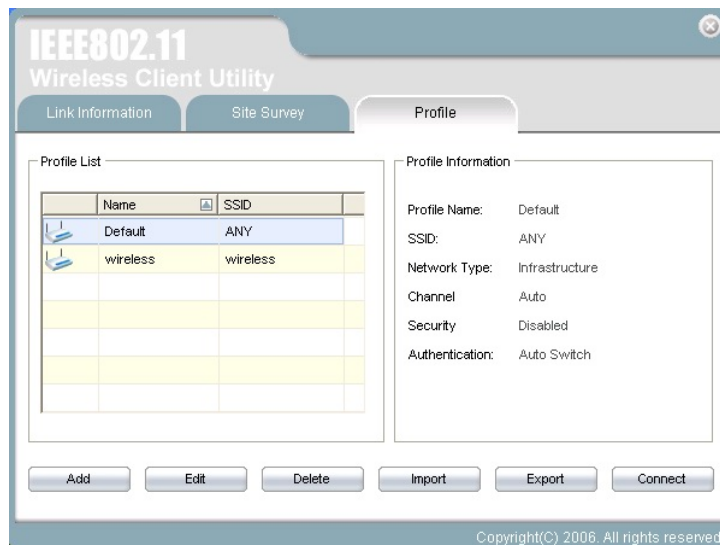
### Connecting to a different network

Hold your mouse pointer over the network icon, and click the right mouse button to select the network.



Click the **Connect** button to connect the available network. If no configuration profile exists for that network, the Profile Settings window opens to ask to create a profile for the network. Follow the procedures to create profile for that network.

### 2.6.3 Profile

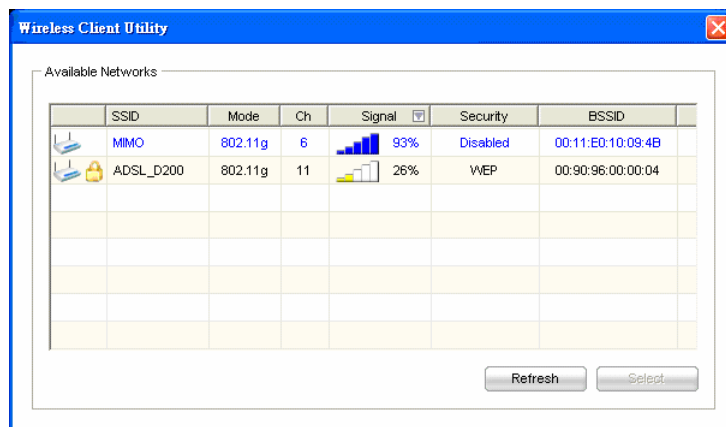


To add a new configuration profile, click **Add** on the Profile tab.  
 To modify a configuration profile, select the configuration from the Profile list and click the **Edit** button.

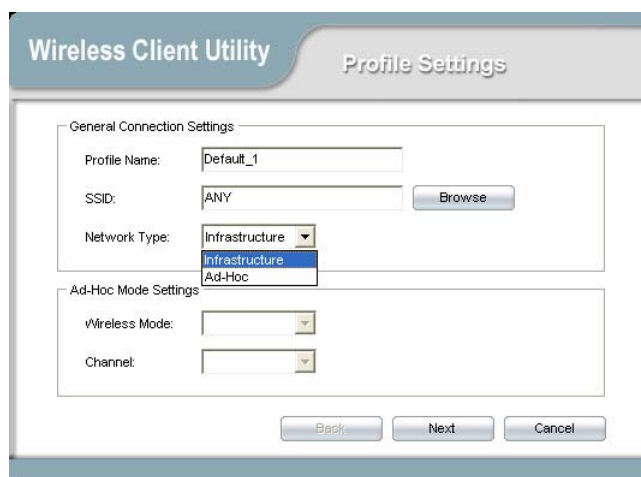


### Scan Available Networks

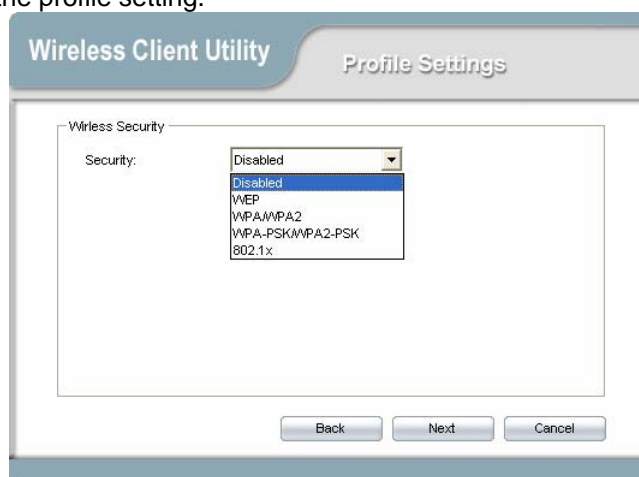
Click the **Browse** button on the Profile Settings screen to scan for available infrastructure and ad hoc networks. On this list, click **Refresh** to refresh the list at any time.



To configure a profile for Ad-Hoc or Infrastructure mode, select the Network Type field on the Profile Settings.



Click **Next** to continue the profile setting.



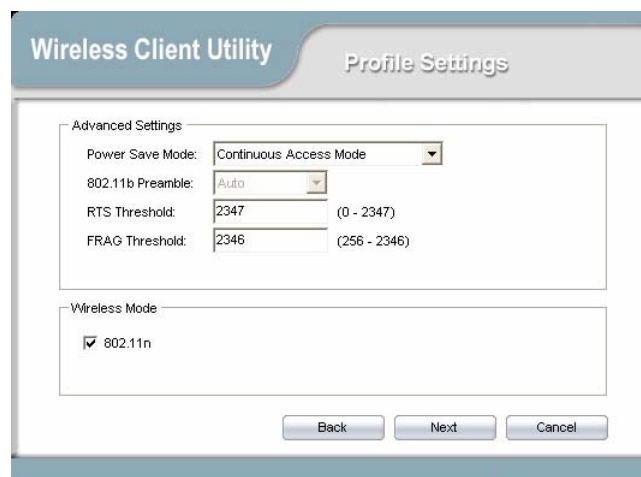
To define the security mode, select the security button of the desired security mode. And then click **Next** to continue. Please see following table for details of security modes.

<p><b>WEP</b></p>	<p>This card support three modes of WEP, include:</p> <ul style="list-style-type: none"> <li>■ <b>64 Bits</b></li> <li>■ <b>128 Bits</b></li> <li>■ <b>152 Bits</b></li> </ul> <p>Except 152-Bit ode, both 64-Bit &amp; 128-Bit modes support Passphrase.</p>
<p><b>WPA/WPA2</b></p>	<p>Enables the use of Wi-Fi Protected Access (WPA).</p> <p>Choosing WPA/WPA2 opens the WPA/WPA2 <b>Security Settings</b> screen. The options include:</p> <ul style="list-style-type: none"> <li>■ <b>TLS (Transport Layer Security)</b> is a Point-to-Point Protocol (PPP) extension supporting additional authentication methods within PPP. Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints.</li> <li>■ <b>PEAP (EAP-GTC) (Protected Extensible Authentication Protocol)</b> authenticates <u>wireless LAN clients</u> using only <u>server-side digital certificates</u> by creating an <u>encrypted SSL/TLS</u> tunnel between the client and the <u>authentication server</u>. The tunnel then protects the subsequent user authentication exchange.</li> <li>■ <b>PEAP (EAP-MSCHAP V2) (Protected Extensible Authentication Protocol) To use PEAP (EAP-MSCHAP V2) security</b>, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager</li> <li>■ <b>TTLS (Tunneled Transport Layer Security)</b> An <u>EAP</u> variant that provides mutual authentication using a certificate for server authentication, and via a secure <u>TLS</u> tunnel for the client</li> <li>■ <b>LEAP (Lightweight and Efficient Application Protocol)</b> is the general framework for a set of high-performance, efficient protocols which are ideal for mobile and wireless applications. LEAP is designed to address all the technical requirements of the wireless data communications industry, and is oriented towards providing the greatest benefit to the</li> </ul>

	industry and the consumer
<b>WPA-PSK/WPA2-PSK</b>	Enables WPA/WPA2 Passphrase security. Fill in the WPA/WPA2 Passphrase on <b>Security Settings</b> screen.
<b>802.1x</b>	Enables 802.1x security. This option requires IT administration. Choosing 802.1x opens the 802.1x <b>Security Settings</b> screen. The options include: <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>TLS</b></li> <li><input type="checkbox"/> <b>PEAP</b></li> <li><input type="checkbox"/> <b>TTLS</b></li> <li><input type="checkbox"/> <b>LEAP</b></li> </ul>

### Advanced Settings

After Security Settings finished, the **Advanced Settings** screen will be shown as following.



The following table describes the items found on the Advanced Settings screen.

<b>Power Save Mode</b>	Shows the power save mode. Power management is disabled in ad hoc mode. The options include: <ul style="list-style-type: none"> <li>• <b>Continuous Access Mode</b></li> <li>• <b>Maximum Power Saving</b></li> <li>• <b>Fast Power Saving</b></li> </ul>
<b>802.11b Preamble</b>	Displays the 802.11b preamble format. The options include: <ul style="list-style-type: none"> <li>• <b>Long</b></li> <li>• <b>Short</b></li> <li>• <b>Auto</b></li> </ul>

<b>RTS Threshold</b>	Value from 0 ~ 2347
<b>FRAG Threshold</b>	Value from 256 ~ 2346
<b>Wireless Mode</b>	Enable or disable 802.11n mode.

After advance settings are finished, the following screen showed as below.  
You can activate the profile now or later.

**Wireless Client Utility** Profile Settings

Wireless Settings

Profile Name: Wireless  
SSID: ADSL  
Network Type: Infrastructure  
Wireless Mode: 802.11n  
Channel: Auto

Security Settings

Security: WEP  
Authentication: Auto Switch

Back Activate Later Activate Now Cancel



# Chapter 3 – Maintenance

This chapter describes how to uninstall or upgrade the Wireless Utility.

## 3.1 Uninstall the Driver

Follow the steps below to remove (or uninstall) the Card driver from your computer.

- Step 1.** To remove the driver from the OS, go to **Start -> Control Panel**
- Step 2.** Double-click **System**
- Step 3.** Under **Hardware** tab, click **Device Manager**.
- Step 4.** Double-click **Network Card**
- Step 5.** Right-click mouse button on “**802.11n Wireless Network Adapter**”, and choose **Uninstall**
- Step 6.** Click **OK** to confirm that you are going to uninstall the driver

## 3.2 Uninstall the Client Utility

Follow the steps below to remove the Client Utility from your computer.

- Step 1.** To remove the utility from the OS, go to **Start -> Control Panel**
- Step 2.** Double-click **Add-Remove Programs**
- Step 3.** Select **802.11n Wireless Network Adapter**, and click the **Uninstall** button

## 3.3 Upgrading the Wireless Utility

To perform the upgrade, follow the steps below.

- Step 1.** Download the latest version of the utility from the web site and save the file on your computer.
- Step 2.** Follow the steps in *Section 3.2* to remove the current Wireless Utility from your computer.
- Step 3.** Restart your computer if prompted.
- Step 4.** After restarting, refer to the procedure in the Chapter 2 to install the new utility.

# Glossary

For unfamiliar terms used below, look for entries elsewhere in the glossary.

## **AD-HOC (IBSS)**

Ad-hoc mode does not require an AP or a wired network. A network that transmits wireless from computer to computer without the use of a base station (access point).

Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

## **CHANNEL**

A radio frequency used by a wireless device is called a channel.

## **EAP AUTHENTICATION**

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1X transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

## **ENCRYPTION**

The reversible transformation of data from the original to a difficult-to-interpret format. Encryption is a mechanism for protecting confidentiality, integrity, and authenticity of data. It uses an encryption algorithm and one or more encryption keys.

## **FRAGMENTATION THRESHOLD**

This is the maximum data fragment size that can be sent before the packet is fragmented into smaller packets.

## **IEEE 802.1X**

The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

## **INFRASTRUCTURE (BSS)**

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

## **ROAMING**

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization among other factors.

## **SSID**

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

## **TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)**

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server.

## **USER AUTHENTICATION**

WPA applies IEEE 802.1X and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. If you do not have an external RADIUS server, use WPA-PSK/WPA2-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, clients will be granted access to a WLAN.

## **WEP**

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the WCB-321A and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

## **WPA/WPA2**

Wi-Fi Protected Access (WPA) and WPA2 (future upgrade) is a subset of the IEEE 802.11 i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.