CardBus WiFiCard™

User's Manual

Version 1.1

WARNING - Disclaimer

<div style="border: 2px solid black; padding: 10px; color: red; font-weight: bold;">

Do not use this device in applications for which any failure of the wireless link or any data error may cause death, injury or damage of any kind.

</div>

Aboundi Inc., its Sales, Manufacturing and Design Organizations, Reps., Distributors, VARs and distribution channels are absolutely not liable for any death, injury, property damage, loss of data, and loss of business of any other unmentioned loss. The aforementioned entities are not liable even in the event that any of these entities were apprized of the specifics or generalities of an application or intended installation at any time.

Radio Linkages of any type can be fragile and tenuous. Over 1/5th of the entire population of the world now owns cellular telephones, and as any user of a cell phone knows, the cell phone radio communications link may be easily disrupted or completely lost simply by turning your head or by other small environmental movements or changes. This clearly demonstrates to everyone the fragility of any radio link and why radio should not be used for critical implementations, or where death, personal injury, physical damage, property damage or environmental damage may result.

Aboundi Inc products are not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to the operation of nuclear facilities, aircraft navigation, vital communication systems, air traffic control, life support machines, weapons systems, or any industry in which environmental disruptions or technology failure could lead directly to death, personal injury, physical damage, property damage or environmental damage.

Copyright © 2005 by Aboundi Inc. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from the copyright owner.

All the other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

The content described in this manual may be improved or changed at any time and it is subject to be changed without notice.

Manufacturer assumes no responsibility for errors contained herein or for direct, indirect, special, incidental or consequential damages with the furnishing, performance, or use of this manual or equipment supplied with it, even if manufacturer of its suppliers have been advised of the possibility of such damages.

Electronic Emission Notices

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 will accept any interference received, including interference that may cause undesired operation.

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.

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.

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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Regulatory Information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

Limited Warranty

This product is warranted by manufacturer to be free from defects in material and workmanship for one (1) year from the date of purchase unless otherwise stated.

During this period if this product is found to be defective in material or workmanship, manufacturer or one of its authorized service facilities will at its option either repair or replace this product without charge, subject to the following conditions, limitations and exclusions:

1. This warranty extends to the original consumer purchaser only and is not assignable or transferable.
2. This warranty shall not apply to any product which has been subjected to misuse, abuse, abnormal use, negligence, alteration or accident, or has had its serial number altered or removed.
3. This warranty does not apply to any defects or damage directly or indirectly caused by or resulting from the use of unauthorized replacement parts and/or service performed by unauthorized personnel.
4. This warranty does not apply to the software driver that accompanies this product.

This warranty is made expressly in lieu of all other warranties, expressed or implied, including but not limited to any implied warranty of merchantability of fitness for a particular purpose, and all other obligations on the part of Manufacturer provided, however, that if the disclaimer of implied warranties is ineffective under applicable law, the duration of any implied warranties arising by operation of law shall be limited to one (1) year from the date of purchase or such longer period as may be required by applicable law.

Manufacturer hereby disclaims any and all liabilities for consequential and incidental damages arising out of or in connection with any breach of this warranty or any other claim with respect to this product, including but not limited to claims of negligence, strict liability in tort or breach of contract.

Table of Contents

1. Introduction

The CardBus WiFiCard™ (hereafter, referred as APC4000 or WiFiCard™) offers high-speed wireless connection up to 54Mbps with seamless full mobility and cell to cell roaming capability. It enables web browsing, access to POP3 email accounts and synchronization of data wirelessly.

The APC4000 incorporates the WEP (Wired Equivalent Privacy) with 64-bit/128-bit encryption design that supports secure and reliable wireless communication. It also enhances security in Windows XP through the WPA (Wi-Fi Protected Access) supporting TKIP (Temporary Key Integrity Protocol) or AES (Advanced Encryption Standard) algorithms to meet the higher requirements.

It provides power saving mode in the "Infrastructure" environment application to extend the battery life. The automatic fallback feature enhances reliability in noisy environments or extended distance situations. In addition, its Plug-and-Play feature provides care free adaptability for mobile applications on notebook computers.

Overall, the APC4000 provides carefree adaptability for home networking, device sharing, wireless or mobile networking in an office environment and the bandwidth to support wireless multimedia applications such as video streaming.

1.1 Features

- Seamless full mobility and 802.11d roaming from cell to cell and between 802.11b to 802.11g

- IEEE 802.11 Direct Sequence Spread Spectrum (DSSS) high rate compatible

- Supports RADIUS (Remote Authentication Dial-In User Service) security function

- Enhances security in Windows XP through WPA (Wi-Fi Protected Access) supports of TKIP (Temporary Key Integrity Protocol) or AES (Advanced Encryption Standard) algorithm

- WEP (Wired Equivalent Privacy) 64 / 128-bit encryption

- Supports IEEE802.1x VPN pass through

- Supports "Ad-Hoc" and "Infrastructure" topologies

- Power saving mode in infrastructure mode to minimizes power consumption

- Enhances reliable connectivity through auto data rate fallback under noisy environment

- Build-in diversity chip antenna

- Compliant with Windows 98 / Me / 2000 / XP

- Easy-to-Use Graphical Configuration utility saves detailed connectivity profiles for frequently accessed networks

- Supports 32-bit CardBus Interface

- Plug and Play installation

1.2 Applications

- Home networking for device sharing - Remote access to corporate network information email, file transfer and terminal emulation

- Frequently changing environments - Retailers, manufacturers and banks that frequently rearrange the workplace and change location

- SOHO (Small Office and Home Office) users - SOHO users need easy and quick installation of a small computer network functions.

- Inter-building connection - The wireless building-to-building network installs quickly, requires no monthly lease fees, and provides the flexibility to reconfigure easily.

- Typical applications include hard-to-wire buildings, campuses, hospitals/medical offices, warehouse, security huts, exhibition centers, etc.

- Temporary LANs for special projects or occasions - Auditors require workgroups at customer sites. Trade shows, exhibitions, retailers, airline, and shipping companies need additional workstations for a peak period of data traffic.

1.3 Wireless LAN System

1.3.1 Ad-Hoc Configuration

An Ad-Hoc wireless LAN is a group of computers, each equipped with one WLAN PC Card (e.g., APC4000) connected as an independent wireless LAN, refer to Figure 1-1.

Computers in a specific Ad-Hoc wireless LAN must be configured at the same radio channel. Ad-Hoc wireless LAN is applicable to a departmental scale for a branch or SOHO operation.

Notebook with
APC4000

Notebook with
APC4000

Figure 1-1 Ad-Hoc Configuration

1.3.2 Infrastructure Configuration

- An integrated wireless and wired LAN is called an infrastructure configuration (refer to Figure 1-2). A group of WLAN PC Card (e.g. CardBus WiFiCard™) and an Access Point (e.g. AAP2000) is called a Basic Service Set (BSS). Each BSS will have one unique SSID. Each WLAN PC Card in this BSS can be linked to any computer in the wired LAN infrastructure via the AP.

- Infrastructure configuration not only extends the accessibility of a WLAN PC to the wired LAN, but also doubles the effective wireless transmission range between two WLAN PC Cards.

- BSS ID is, in essential, the ID of each independent WLAN PC Card. All WLAN PC Cards configured without roaming options in this independent BSS must be configured with BSS ID of that AP. You may need to check BSS ID of your AP by using its vendor supplied program.

- Infrastructure configuration is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

- Two APs can be used as a point-to-point link between two LANs. LAN interconnection is applicable to a wireless backbone between buildings.
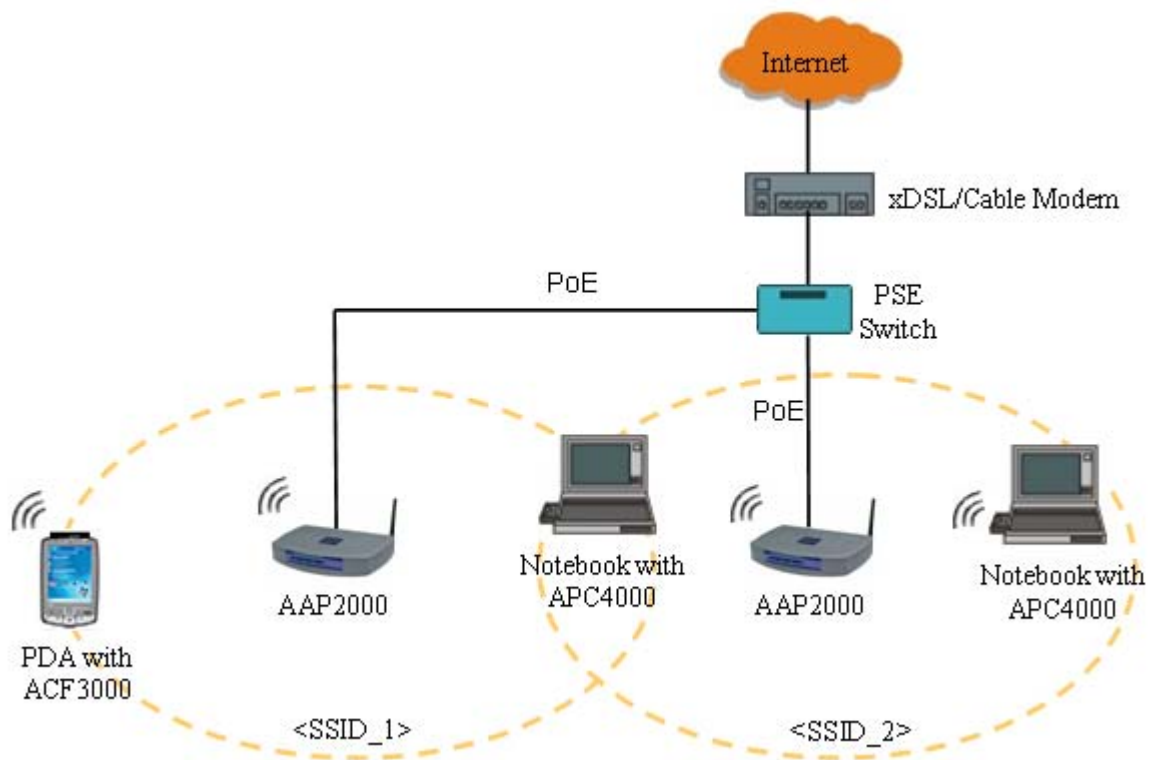

Figure 1-2 Infrastructure Configuration

- The infrastructure configuration supports roaming capability for mobile workers. More than one

BSS can be jointly configured as an Extended Service Set (ESS). On account of a continuous connection to the network, users within this ESS can roam freely. All WLAN PC Cards and APs within one ESS must be configured with the same ESS ID.

- Before setting up an ESS for roaming, it would be helpful to achieve good performance by choosing a feasible radio channel and right places for APs.

2. Installation

Use the procedures described in this chapter to install your CardBus WiFiCard™ adapter under MS Windows 98SE/Me/2000, and XP.

2.1 Product Kit

Before starting installation, please make sure the CardBus WiFiCard™ adapter package you purchased includes the following items:

- WiFiCard™
- CD-ROM (including Driver/Utility and User's Manual).
- Quick Start Guide.

If anything is missing, please contact your vendor.

2.2 PC's Minimum Requirements

To install the APC4000 successfully, your PC (notebook, or desktop) should meet the following minimum requirements:

- A PCMCIA slot compliant with Release 2.1 of the PCMCIA specification.
- Windows 98SE, Me, 2000, or XP operating system.
- Minimum 10 Mbytes free disk space for installing the driver and the utility program.

2.3 Installing the Utility and Driver

Note: Please do not plug your WiFiCard™ until the following setup procedure has been completed.

Follow the steps below to install the utility and driver.

- Insert the supplied CD-ROM in the CD-ROM drive.
- The InstallShield Wizard should start automatically. If AUTORUN is disabled in your Windows

settings, you will need to go to the Windows "Start" button, choose "Run" and type "D:\setup.exe" in the text box, where D is the drive letter of your CD-ROM drive.

- Follow the InstallShield Wizard to install the driver and utility.

- Reboot your PC after completing the installation process. (Recommended)

- Plug your WiFiCard™. The "Add New Hardware Wizard" automatically loads the driver, and then a new application (the Configuration & Monitor Utility) icon will be displayed in the task bar.

- Go to Section 3 for Configuration.

Note: In the MS Windows 2000/XP installation procedure, an extra window prompts you to select the options whether you would like to install the "Digital Signature Not Found" or not. You can safely select "YES".

3. Wireless LAN Configuration Utility

The Wireless LAN Configuration Utility is a powerful application that helps you to configure the APC4000 and monitor the statistics of the communication. Unlike the standard method of configuring the card via the operating system utilities (e.g. Control Panel), this application permits the dynamic modification of configuration parameters while the card is operating. This application also offers more configuration options.

3.1 Icon

The Wireless LAN Configuration Utility appears as an icon on the system tray of Windows while the card is running. You can open it by clicking the icon (see Figure 3-1).

Figure 3-1 Wireless LAN Configuration Utility Icon

The icon is appeared as bar diagram with different color and level for representing different connection status. When the station is not associated with other Station/AP, the icon will appear as an empty (blank) bar diagram. Once it is associated, it will appear as different color for different level of signal strength (RSSI). There are 3 levels of icons to represent the signal strength, the green one (100%~50%), the yellow one (50%~25%), and the red one (below 25%).

The Wireless LAN Configuration Utility is a highly integrated application included the following options:

- Status (including Configuration)

- Site Survey

- Statistics

- About

3.2 Status

A typical status screen of the application in Infrastructure mode is shown in Figure 3-2. The wireless configuration parameters are shown at the upper part of the screen.
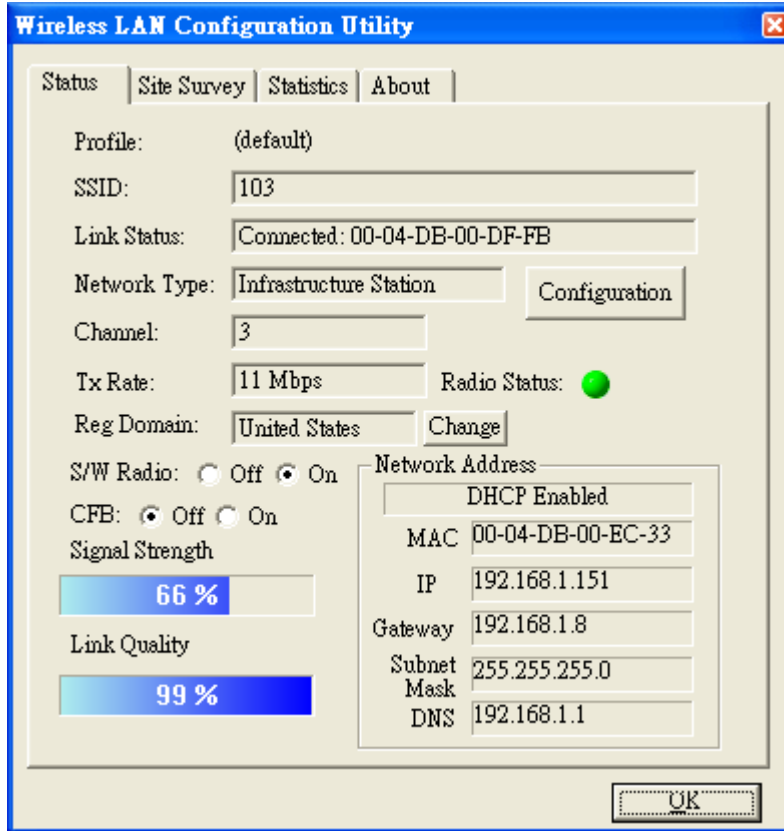

Figure 3-2 WLAN Status

Network Address:

Section shows the current Network status such as the MAC address, DHCP (Enable or not), IP address, Subnet Mask address, Gateway Address and DNS server address.

Change:

By clicking the **Change** button, you can perform the multi-country roaming (802.11d).

S/W Radio:

Shifting RF to ON/OFF via the WLAN configuration tool (software shifting) is possible.
The default is on.

CFB:

The Contention Free Bursting is supported, which allows the transmission of a train of small packets without intermediate contention to improve the throughput.

3.3 Configuration

Press **Configuration** button (refer to Figure 3-3) in order to change the configuration parameters, and then a pop-up Configuration dialog box will be appeared for you to modify your settings. The configuration dialog box includes **General**, **Encryption**, and **Advanced**.
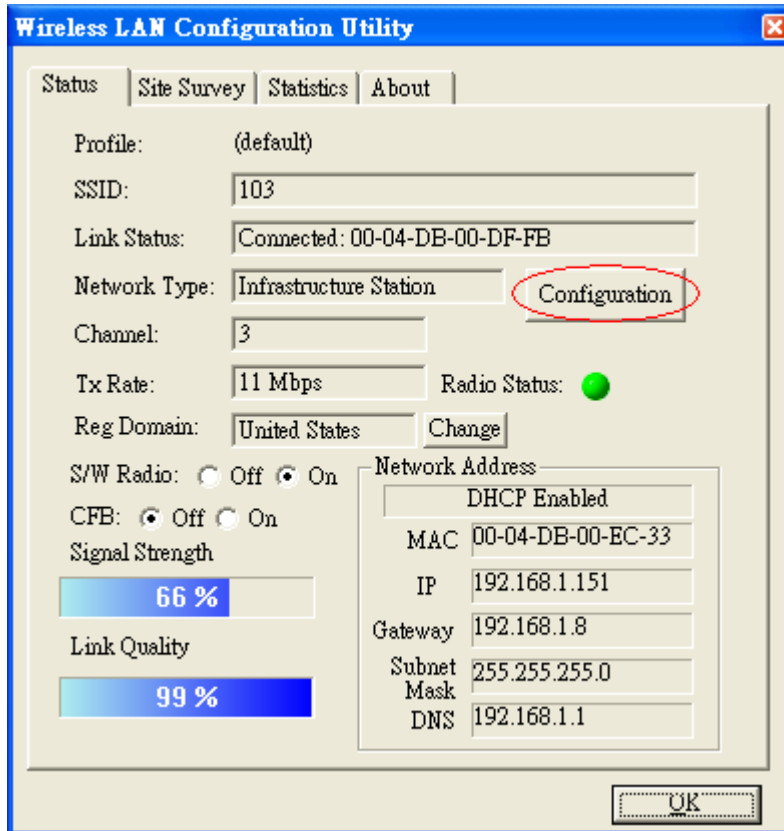

Figure 3-3 Configuration

3.3.1 General

In this page, the user can configure the station card with its network type (Infrastructure/Ad-Hoc), SSID (up to 32 characters), channel (only in Ad hoc mode, and its range is according to the regulatory domain), and Tx Rate (Automatic/1/2/5.5/6/9/11/12/18/24/36/48/54 Mbps), refer to Figure 3-4.
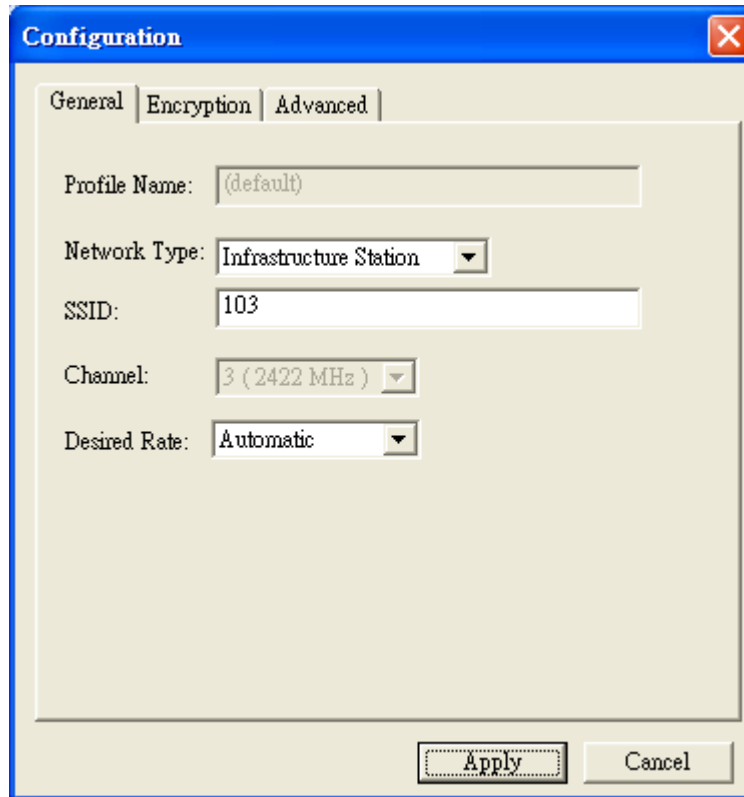

Figure 3-4 General Settings

3.3.2 Encryption

Note: When AP turns on the WEP function, APC4000 must have same WEP settings as those set in AP.

Figure 3-5 allows the encryption settings.

Encryption Mode

Base on AP encryption settings, you can set the encryption mode to be **None** or **WEP**.

Authentication

There are 3 options in the **Authentication** mode -- Open system, Shared key, and Auto Switch.

- **Open System** authentication is not required to be successful while a client may decline to authenticate with any particular other client.

- When WEP Key setting will be used, it should be set to **Shared key**.

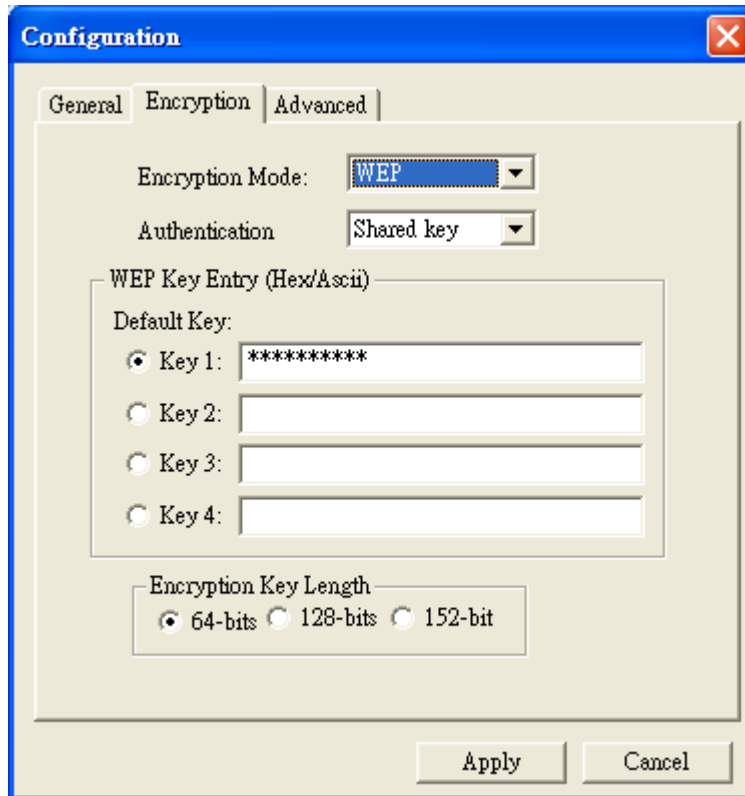- By choosing **Auto Switch**, it will detect these 2 modes automatically.

Figure 3-5 Encryption Settings

WEP Key # and Encryption Key Length

The Key # can be 64-bit, 128-bits or 152-bits specified in the **Encryption Key Length**.

- 64-bit: 10-digit Hexadecimal number e.g. 12345abdef (in the range of A~F, a~f, and 0~9)

- 128-bit: 26-digit Hexadecimal number e.g. 12345678901234567890abcdef (in the range of A~F, a~f, and 0~9)

- 152-bit: 32-digit Hexadecimal number e.g. 12345678901234567890abcdefabcdef (in the range of A~F, a~f, and 0~9)

When the WEP Key is set complete, then click **Apply.**

3.3.3 Advanced

In this tap window, the advanced configuration settings can be changed, such as the Power Saving mode, Preamble Type, Fragmentation Threshold, and RTS Threshold. Figure 3-6shows the recommended configuration for the advanced settings.

Before selecting Short Preamble, make sure that the other stations and APs are also supporting this feature.
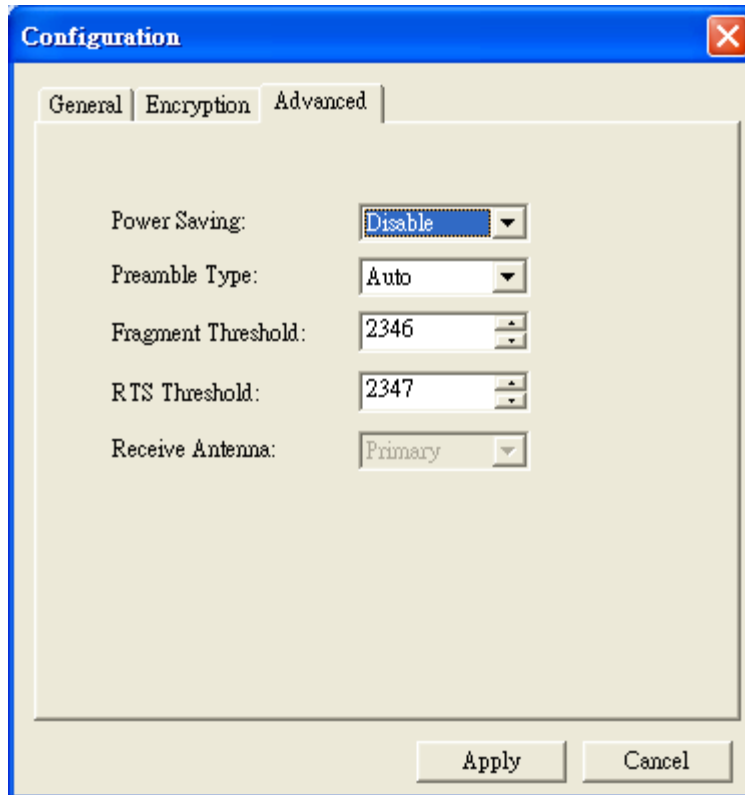

Figure 3-6 Advanced Settings

3.4 Site Survey

By choosing the **Site Survey** tap in the upper frame, you can scan all the channels to find all the access points/stations within the accessible range of your APC4000. As shown in Figure 3-7, the list of the "Available Networks" includes the information about the BSSID, SSID, Mode (Network Type), WEP (On/Off), Channel, Signal Strength and Supports Rate.

You may press the **Rescan** button dynamically in order to update this list and double-clicking at the one on the list once you want to associate with it, and then the **Configuration** window will be displayed (refer to 3.3).
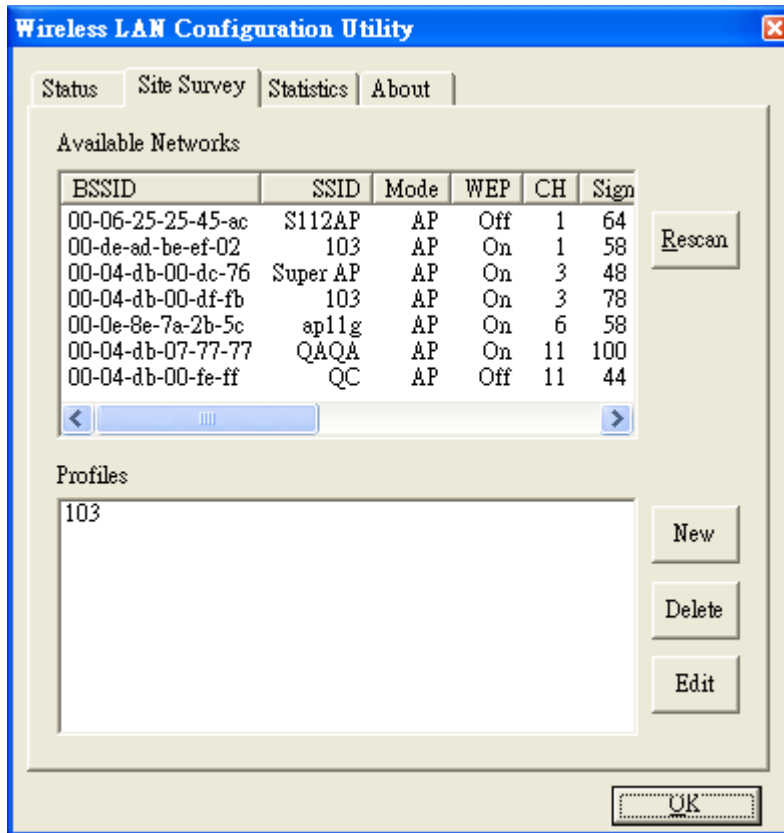
Figure 3-7 Site Survey page

3.4.1 Profiles Selection

The Wireless LAN Configuration Utility provides the easy-to-use profile function. It shows all the profiles (up to 32 sets) with its configurations currently stored in the program, which includes Profile Name, Network Type, SSID, Desired Rate, Encryption Key and other advanced settings.

There are two methods to access the profile:

- **Site Survey Window**

    From the lower part of the Site Survey window, there are three options can be selected:

    - New: When selected, the **Configuration** window will be displayed for adding new profile (refer to 3.3).

    - Delete: Select the profile to be deleted, and then click the **Delete** button.

    - Edit: When **Edit** is selected, the **Configuration** window will be displayed for updating the profile (refer to 3.3)

- **System Tray**

    The profiles can be selected by right clicking the mouse on the Wireless LAN Configuration Utility icon in the system tray, refer to Figure 3-8, and then select **Connect**.

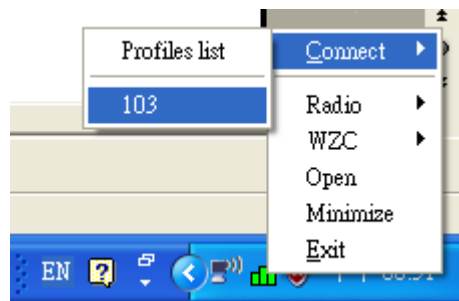   You can apply the profile by double-clicking the item in the profiles list.

Figure 3-8 Profile list of the icon in system tray

3.5 Statistics

This tap window provides the statistic information with Tx success, Tx error, Tx Throughput, Rx success, Rx CRC success, Rx CRC error, and Rx Throughput.

You may reset the counters by pressing the **Reset** button (refer to Figure 3-9)
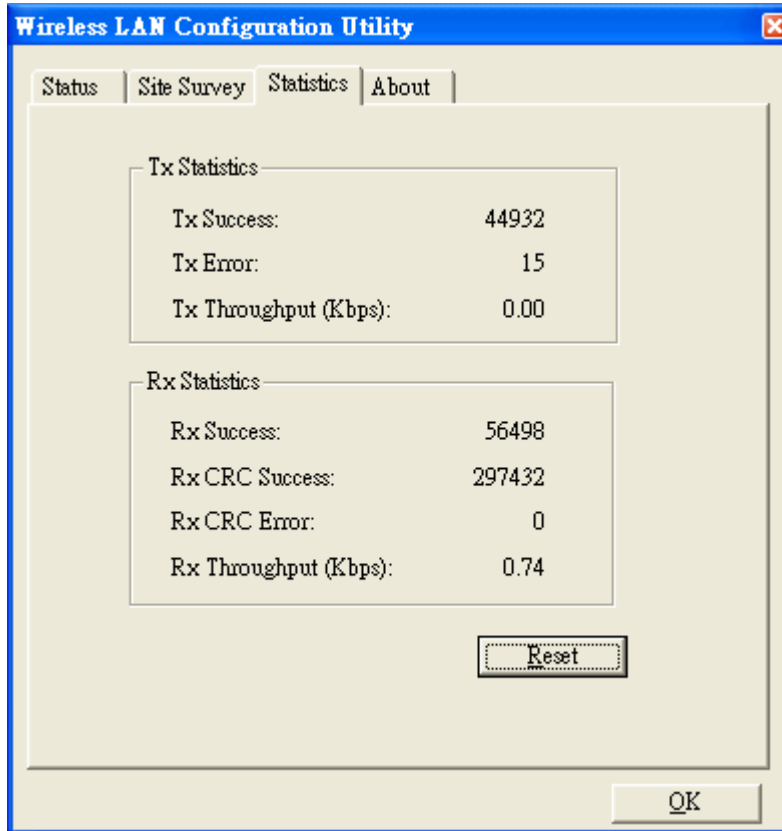

Figure 3-9 Statistics page

3.6 About

By choosing this option (see Figure 3-10), you can check the basic information about the versions of Driver and Utility.
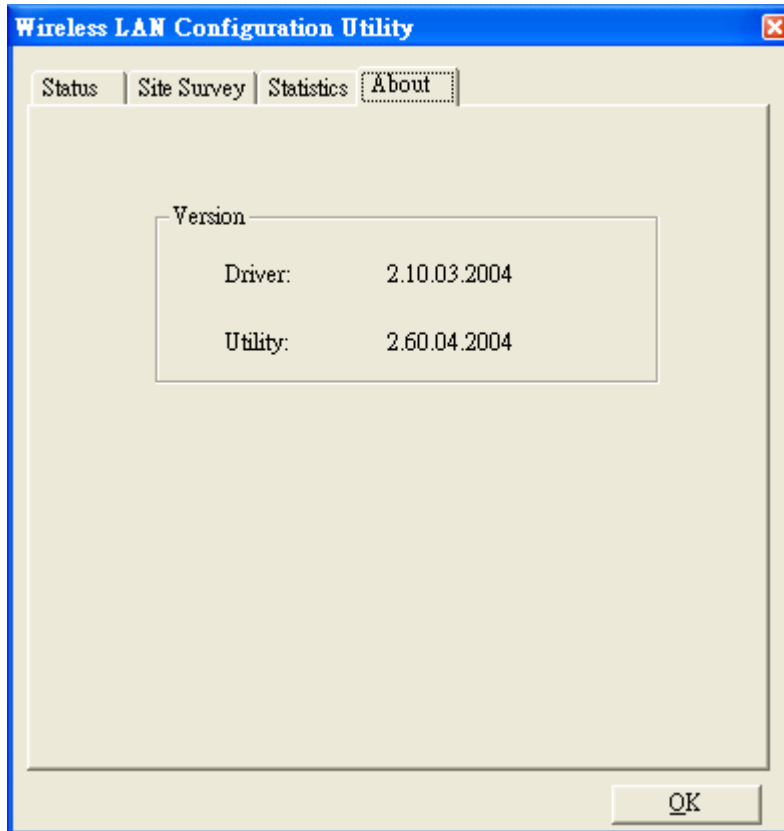

Figure 3-10 About Information

3.7 Soft Access Point

By taking advantage of the Soft AP, you can easily build up a cost-effective wireless connectivity without the expense of deploying a hardware-based access point.

It's great ideal for mobile groups, who want to contribute a connection from their wireless network to an existing network backbone, providing their wireless clients with access to the Internet and other resources on their network.

Note: Refer to http://www.microsoft.com/technet/prodtechnol/winxppro/plan/xpbrdgnt.mspx for more Network Bridge information.

Note: The NB or PC equipped with APC4000 need to run Windows XP in order to set up the Soft AP.

3.7.1   AP Mode Setting

As shown in Figure 3-11, form the **Configuration** windows (refer to section 3.3), set the **Network Type** to be one of the following three AP modes:

- AP (Mixed): Support both 802.11b and 802.11g operation

- AP (11g Mode): Only support 802.11g operation

- AP (11b Mode): Only support 802.11b operation

Follow the steps described in section 3.3 to set other parameters in General, Encryption and Advanced tap windows, for example: SSID, channel, WEP, etc.
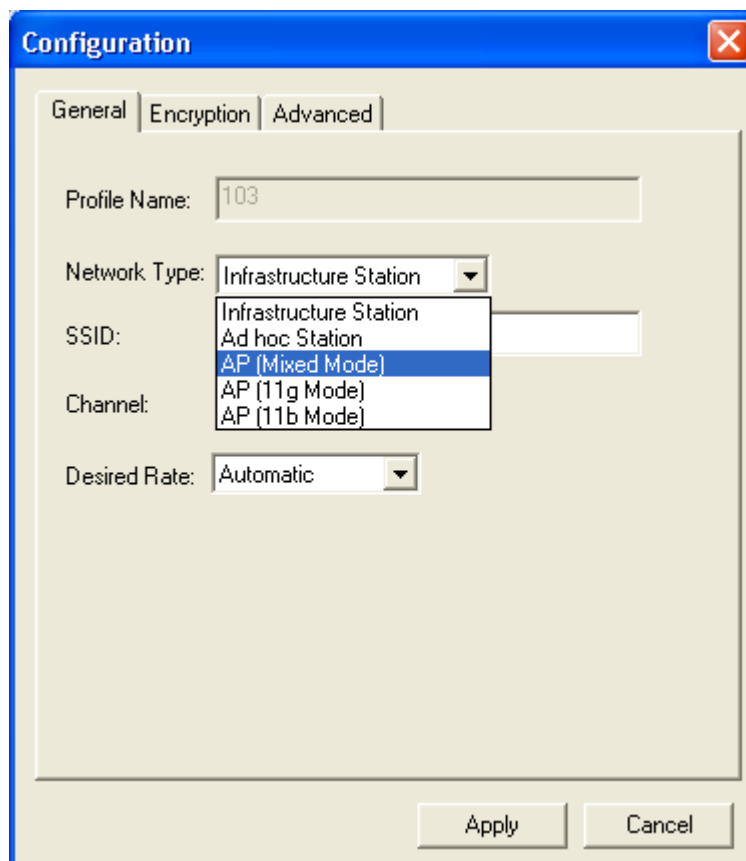

Figure 3-11 Soft Access Point

3.7.2 Window XP with Bridge Network

As shown in Figure 3-12, the NB/PC equipped with APC4000 will be connected to the wired network via the Ethernet connection. From the NB/PC Window XP, set the bridge connection, so other client WLAN stations (for example two NBs at the right of Figure 3-12) can access the Internet via APC4000 via WLAN connection.

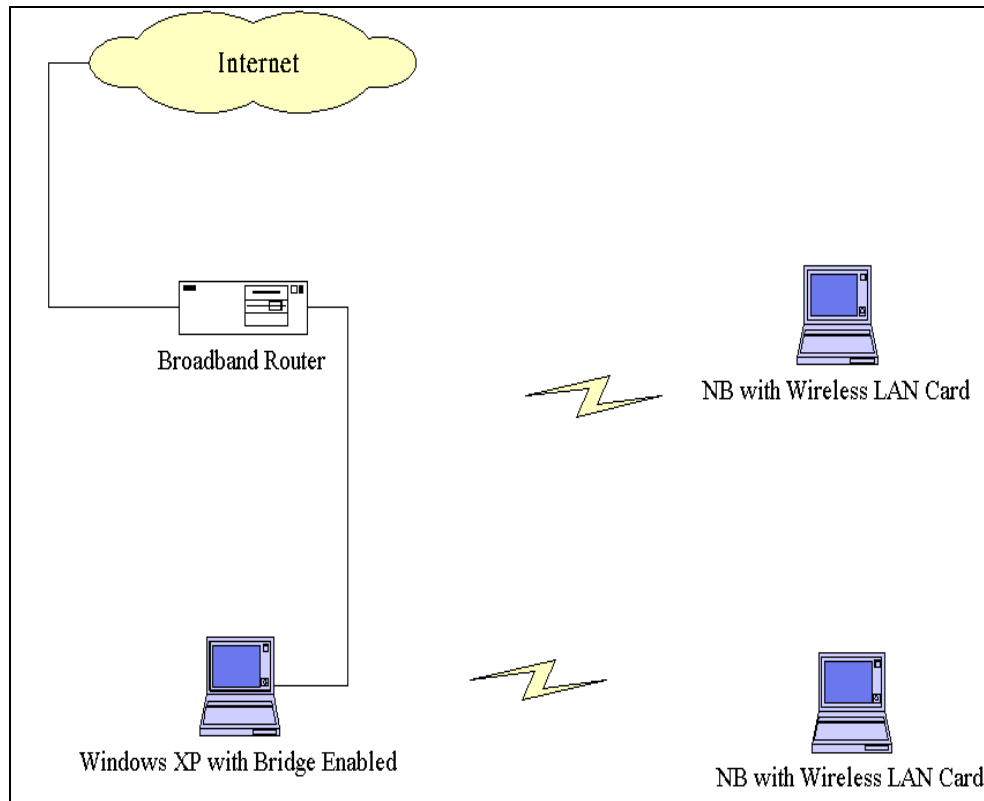Note: Make sure you can reach the Internet using your Ethernet connection.

Figure 3-12 Windows XP with Bridge Network

Follow the steps below to configure both the Ethernet adapter and the APC4000 WiFiCard™ adapter under your Windows XP computer. As shown in Figure 3-13,

- Open the **Network Connections** from your Window XP computer

- Highlight both of your network adapters (Ethernet Adapter and APC4000 Adapter)

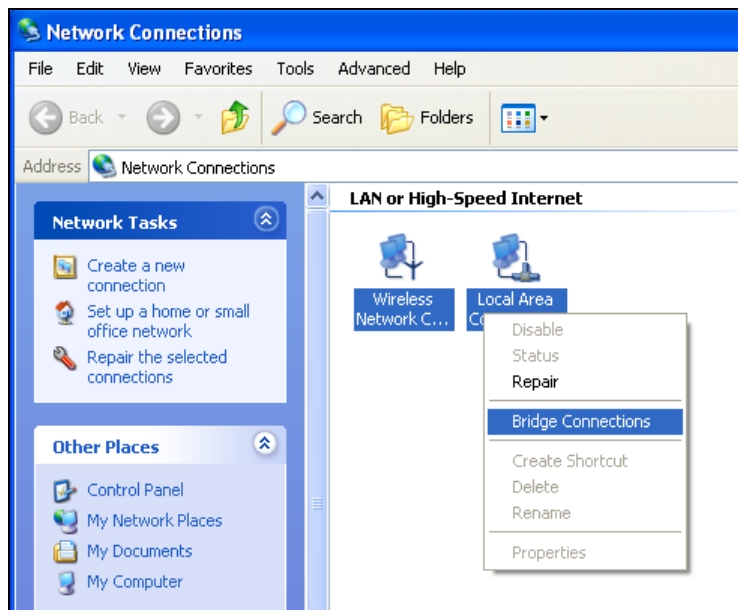- Right click on any one of them and select **Bridge Connections**

Figure 3-13 Bridge Connections

- Please wait while Windows bridges the connections (refer to Figure 3-14).
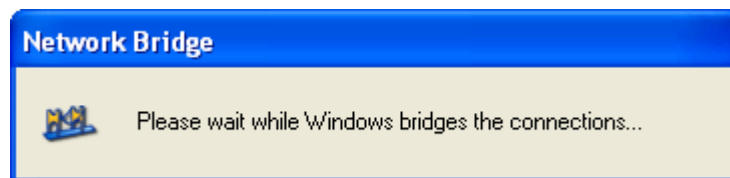
Figure 3-14 Network Bridge Connecting

- When the bridge setup is complete, the Network Bridge icon will be displayed as shown in Figure 3-15.

Figure 3-15 Network Bridge Connections

Once the Network Connections are finished, you will get an IP address from your Broadband Router on the Ethernet LAN.

Your network adapters no longer have anything in the network properties at this time.

If you want to modify the network properties, you have to do it via the Network Bridge Properties as shown in Figure 3-16

Figure 3-16 Network Bridge Properties
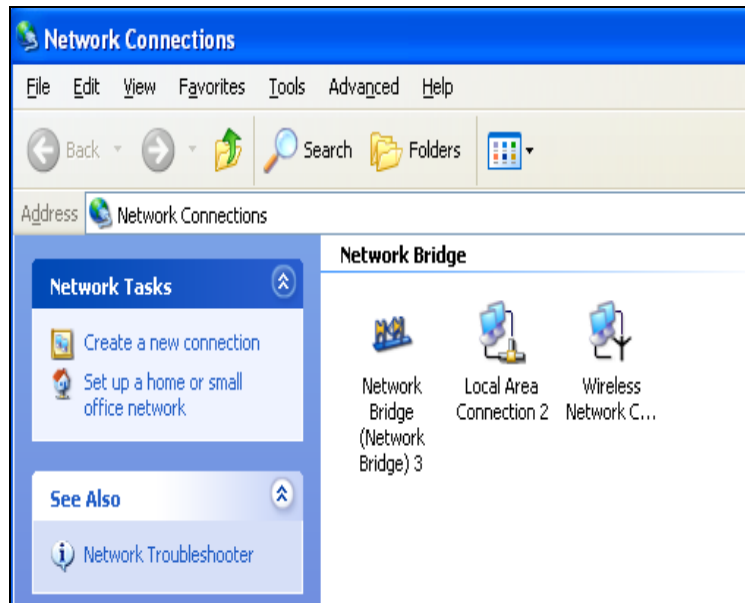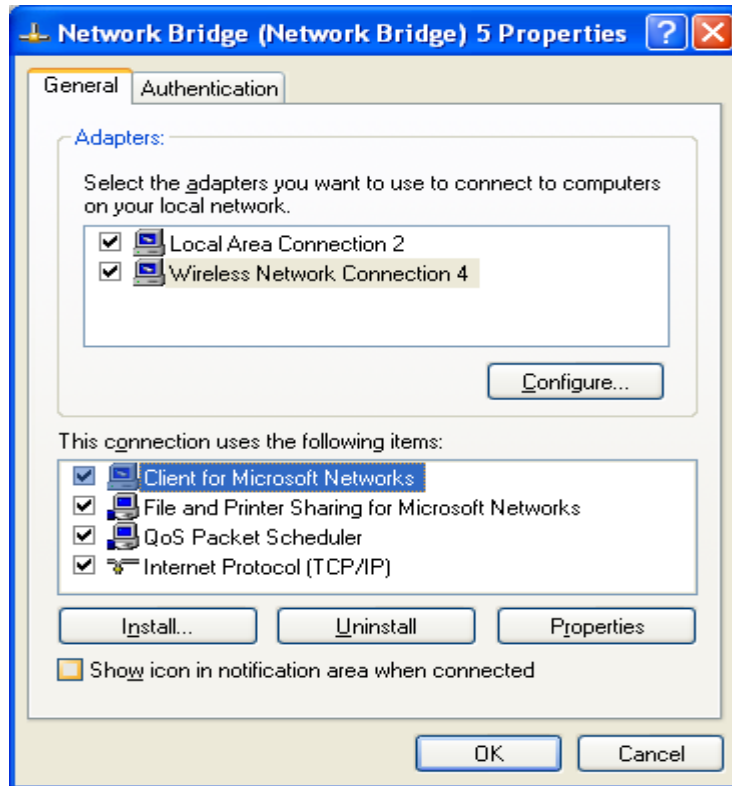
3.8 Windows XP WPA Support

APC4000 also enhances security through the WPA (Wi-Fi Protected Access) supporting TKIP (Temporary Key Integrity Protocol) or AES (Advanced Encryption Standard) algorithms to meet the higher requirements.

From your Windows XP computer, open the Wireless Zero Client Configuration (refer to Microsoft web site www.microsoft.com for more detail about the Wireless Zero Client Configuration):

- Open **Network Connections**

- Right-click the connection for which you want to set up automatic wireless network configuration, and then click **Properties**.

- On the **Wireless Networks** tab select the **Use Windows to configure my wireless network settings** check box. This check box is selected by default.

- From the Preferred networks list, right-click the connection for which you want to enable or disable WPA authentication, and then click **Properties** and make all the settings as those settings in the AP that also supports WPA.

4. Specifications

General	
Standard compliance	Compliant IEEE 802.11b/g Standard
Security	64-bit, 128-bit, 152-bit WEP, WPA, AES and IEEE 802.1x
Hardware	
RF Range	Frequency range: 2.4 ~ 2.4835GHz
Data rate	54/48/36/24/18/12/11/9/6/5.5/2 /1Mbps
Modulation	DSSS,OFDM (Orthogonal Frequency Division Multiplexing)
	DBPSK/DQPSK/CCK
Coding	1, 2Mbps: 11 chip/bit Barker Coding
	5.5, 11Mbps: Complementary Code Keying
Number of channels	Europe: 13 (3 non-overlapping)
	US: 11 (3 non-overlapping)
	France: 4 (1 non-overlapping)
	Japan: 14 (3 non-overlapping)
Host Interface	32bit CardBus
Transmit power	+13dBm (Typ.) , 10mW/MHz for Japan
Receive sensitivity	-80 dBm Typical. (11Mbps, @ BER 10E-5)
	-82 dBm Typical. (5.5 / 2 / 1Mbps, @ BER 10E-5)
Software	
Driver Support	MS Windows 98SE/Me/2000/XP
Utility	User setup and diagnostic tool
Mechanical	
Dimensions	54.0 x 118.5 x 6.0mm
Weight	40 grams
Environmental	
Temperature	0 ~ 55°C (operation),
	-20 ~ +65°C (storage)
Relative Humidity	95% (non-condensing)
Certificate	
EMC	U.S.: FCC Part 15, sections 15.247, 15.205, 15.209

5. Glossary

The following glossary is for your reference only, and is not need for the installation of your Wireless LAN PC Card.

Wireless Access Point (AP) – Any entity that has station functionality and provides access to the distribution services via the wireless medium (WM) for associated stations

Ad-Hoc – A network is composed solely of stations within mutual communication range of each other via the wireless medium (WM).

An ad hoc network is typically created in a spontaneous manner.

The principal distinguishing characteristic of an ad hoc network is its limited temporal and spatial extent.

These limitations allow the act of creating and dissolving the ad hoc network to be sufficiently straightforward and convenient so as to be achievable by non-technical users of the network facilities; i.e., no specialized technical skills are required and little or no investment of time or additional resources is required beyond the stations that are to participate in the ad hoc network.

The term ad hoc is often used as slang to refer to an independent basic service set (IBSS).

BSS (Basic Service Set) – An AP associated with several wireless stations

ESS (Extended Service Set) – More than one BSS can be configured as an Extended Service Set.

An ESS is basically a roaming domain.

Ethernet – A popular local area data communications network, originally developed by Xerox Corp., which accepts transmission from computers and terminals

Ethernet operates on 10 Mbps baseband transmission over shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation Threshold – Indicates how much of the network resources is devoted to recovering packet errors. The value should remain at its default setting of 2,436. If you experience high packet error rates, you can decrease this value but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

Infrastructure – The infrastructure includes the distribution system medium (DSM), AP, and portal entities.

It is also the logical location of distribution and integration service functions of an extended service set (ESS).

An infrastructure contains one or more APs and zero or more portals in addition to the distribution system (DS).

IEEE – Institute of Electrical and Electronic Engineering

LAN – Local Area Network

Roaming – A function that allows one to travel with a mobile end system (wireless LAN mobile station, for example) through the territory of a domain (an ESS, for example) while continuously connecting to the infrastructure.

RTS (Request To Send) Threshold –It should remain at its default setting of 2,347. A preamble is a signal used to synchronize the transmission timing between two or more systems.

A series of transmission pulses are sent before the data to indicate that "someone is going to transmit data." This ensures that systems receiving the information correctly when the data transmission starts.

SOHO – Small Office Home Office

SSID – Service Set Identifier

Wired Equivalent Privacy (WEP) – The optional cryptographic confidentiality algorithm specified by IEEE 802.11 is used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network medium that does not employ cryptographic techniques to enhance privacy.

Network Address Translation (NAT) – The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.

One network is designated the internal network and the other is the external.

The internal network then appears as one entity the outside world.

TKIP – Temporal Key Integrity Protocol is a standard technique for re-keying a WEP connection and establishing a "per packet" encryption key based on the WEP key and the packet's initialization vector.

TKIP resists attack because a significant number of intercepted packets must be encrypted under the same key for WEP attacks to succeed.

WPA – The Wi-Fi Protected Access (WPA) is a standards-based interoperable security specification. Its purpose is to increase the level of security for existing and future wireless LANs.

Wi-Fi Protected Access is the stopgap measure between WEP and the upcoming 802.1X security standard. WPA specifies the use TKIP on existing RC4 WEP to impose strong data encryption and 802.1X EAP (Extensible Authentication Protocol.) based authentication to enforce mutual authentication.

WPA is an interim security solution that targets on all know WEP vulnerabilities.

It will be forward compatible with the upcoming 802.11i standard.

The ultimate wireless security solution is still 802.11i.

All products are supposed to comply with 802.11i standard once the standard is released.