11g Wireless Cardbus Adapter

User's Manual

Version: 1.0

Table of Contents

Revision History

Version	Date	Notes
1.0	June 14, 2004	Initial Version

1 Introduction

This chapter describes the features & benefits, package contents, Cardbus description, system requirements, applications, and network configuration.

1.1 Features & Benefits

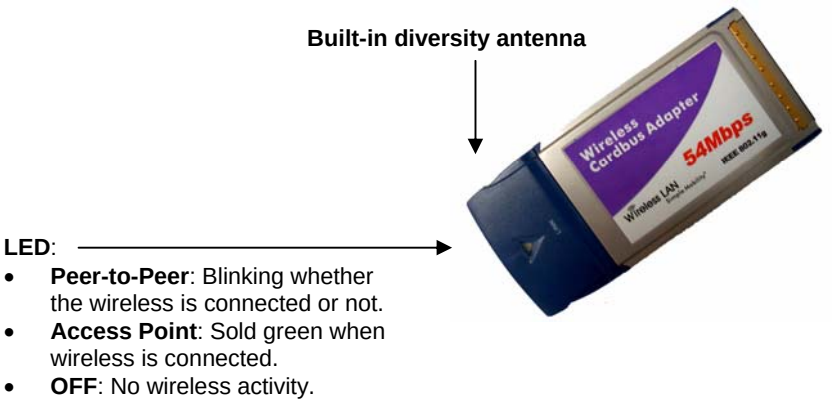
Features	Benefits
High-speed data rate up to 54 Mbps	Capable of handling heavy data payloads such as MPEG video streaming.
Up to 64/128-bit WEP Data Encryption, WPA, AES and TKIP	Powerful data security.
IEEE 802.1x client support	Enhances authentication and security.
Multi-country roaming (802.11d) support	Automatically adjusts regulatory domain to operate in different countries.
Advanced power management	Low power consumption in power saving mode.

1.2 Package Contents

- One 11g Wireless Cardbus
- One Installation CD
- One Quick Installation Guide

1.3 Cardbus Description

The Cardbus is a standard PC card that fits into any PCMCIA card Type II slot. The Cardbus has a LED indicator and an integrated built-in diversity antenna



1.4 System Requirements

The following are the minimum system requirements in order to use the Cardbus.

- PC/AT compatible computer with a PCMCIA Type II slot.
- Windows 98SE/ME/ /2000/XP operating system.
- 5 MB of free disk space for installing the PC Card driver and utility program.

1.5 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
   There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
b) **Temporary workgroups**
   Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
c) **The ability to access real-time information**
   Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
d) **Frequently changed environments**
   Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
e) **Small Office and Home Office (SOHO) networks**
   SOHO users need a cost-effective, easy and quick installation of a small network.
f) **Wireless extensions to Ethernet networks**
   Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
g) **Wired LAN backup**
   Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
h) **Training/Educational facilities**
   Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

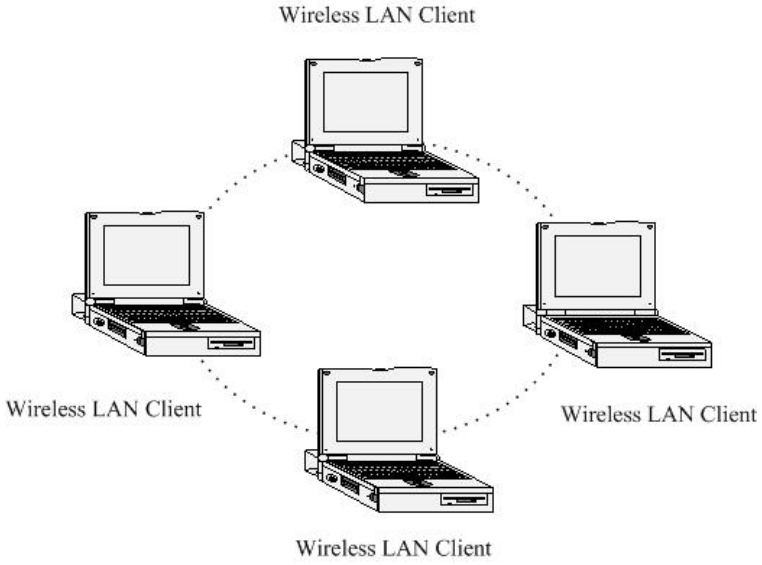
1.6 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
b) Infrastructure for enterprise LANs.

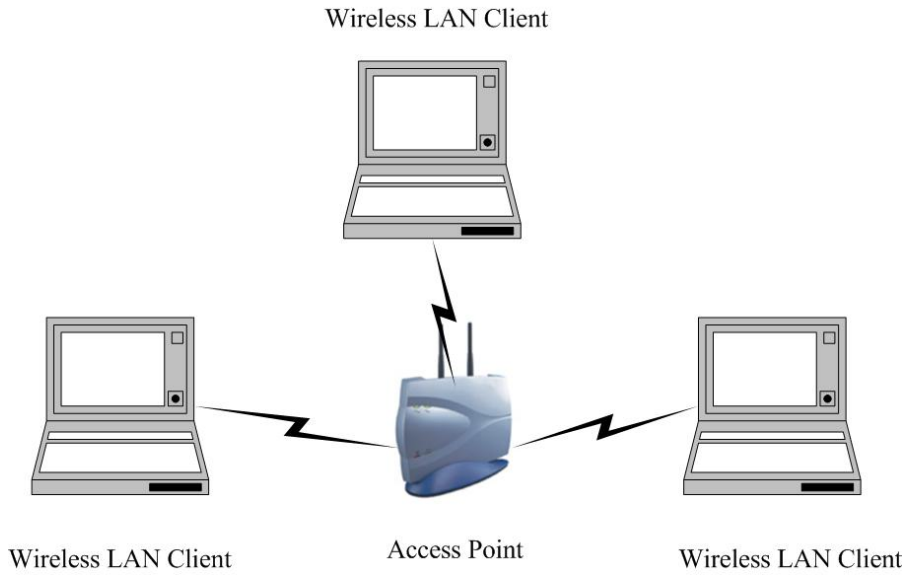
a) Ad-Hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



2 Install Drivers & Client Utility

This chapter describes how to install the drivers and client utility in Windows 98SE/ME/2000/XP.

2.1 Before You Begin

Before installing the new drivers into your PC, you need to remove any improperly installed Cardbus adapters, as these drivers may conflict with the new drivers you are about to install.

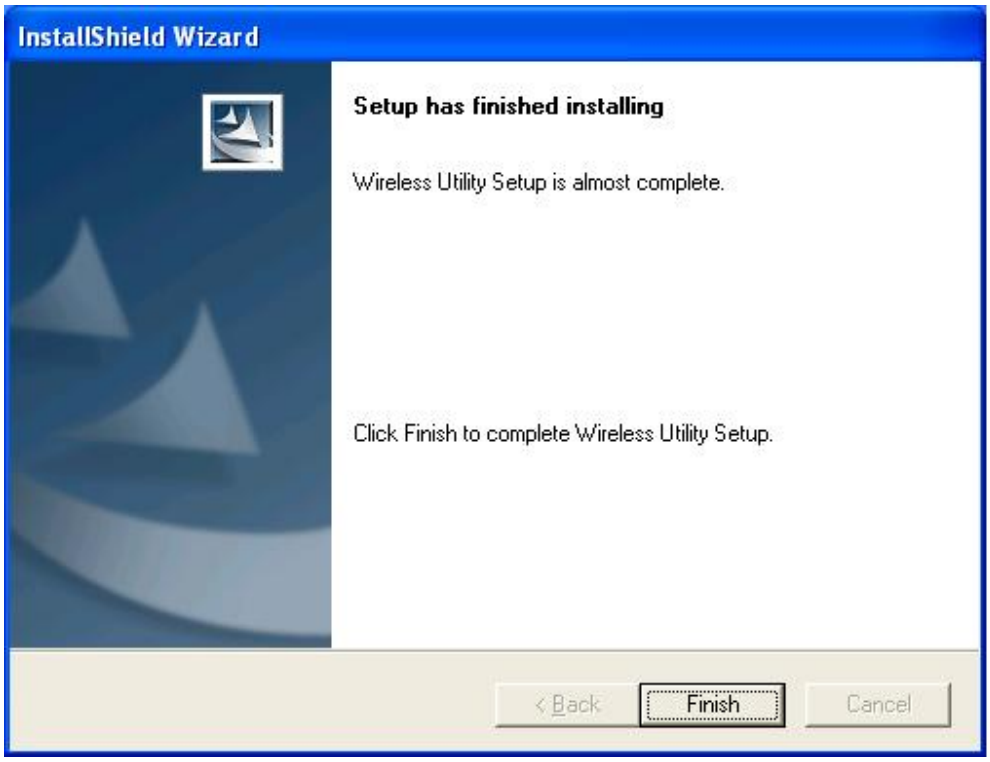
During the installation, Windows 98SE/ME/2000/XP may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS \OPTIONS\CABS directory.

2.2 Installing the Drivers

Follow the steps below in order to install the r drivers:

1. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.
2. Once the setup begins you will see the **Install Shield Wizard**, as the image depicts below.

3. Click on the **Next** button to continue. The Setup Wizard will copy all the necessary files and then display the following message.

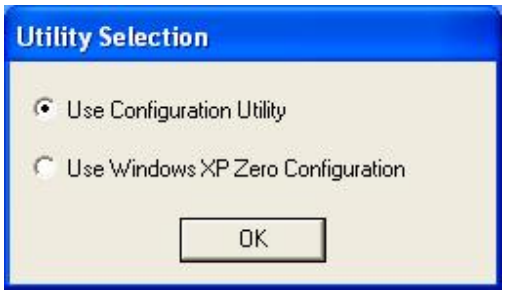


4. The first part of the driver installation is complete, click on the **Finish** button.
5. Insert the Cardbus into the PCMCIA slot of your notebook. Windows will automatically detect the adapter and display the **Found New Hardware Wizard**, as the image depicts below.

6. Select the **Install the software automatically (Recommended)** radio button, and then click on the **Next** button to continue.

7. If you are using Windows XP, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

8. The Setup Wizard will then copy the necessary files. The Driver & Utility installation is now complete, click on the **Finish** button.



9. You will then need to decide which configuration utility you would like to use. Details on using the **Configuration Utility** are discussed in **Chapter 3**. However, if you decide to use **Windows XP Zero Configuration**, please refer to your Windows XP User's Guide.

2.3 Verify the Installation

Follow the steps below in order to verify that the device has been installed and is functioning properly:

1. Click on **Start > Settings > Control Panel**.
2. Double click on the **System** icon.
3. Click on the **Hardware** tab, and then click on the **Device Manger** button.
4. Select **Network adapters** to view a list of network adapters on your PC. You will then see a window similar to the image below.

5. Make sure that there isn't a yellow (**?**) or a red (**X**) next to the Card Bus adapter (*IEEE802.11g Wireless LAN Card*). If you see a (**?**) or (**X**) you would need to uninstall the drivers, and reinstall them again. In order to uninstall the drivers refer to **Chapter 4**.

3 Using the Client Utility

After a successful installation you will see the PC card **Client Utility radio** icon in the system tray.

PC Card Client Utility radio

Green indicates good or excellent link status.

Yellow indicates fair link status.

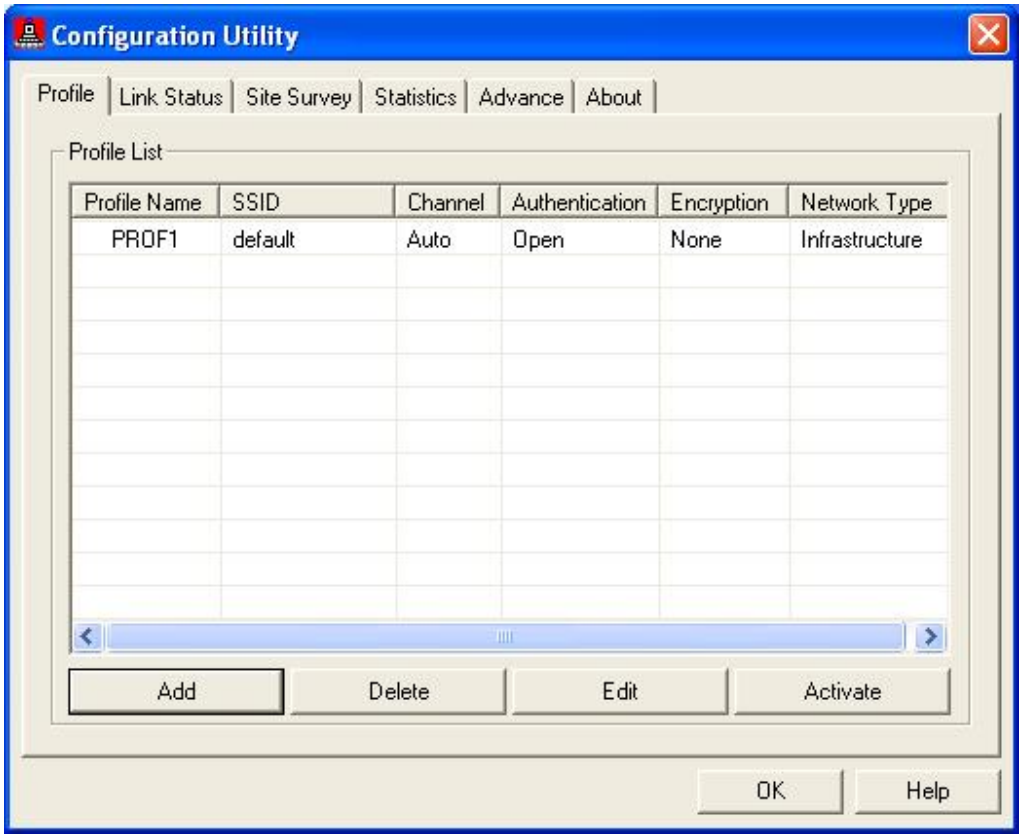
Red indicates poor or no link status.

To manually run the Client Utility click **Start > Programs > Wireless IEEE 802.11g > RT2500 > Wireless Config**

3.1 PROFILE

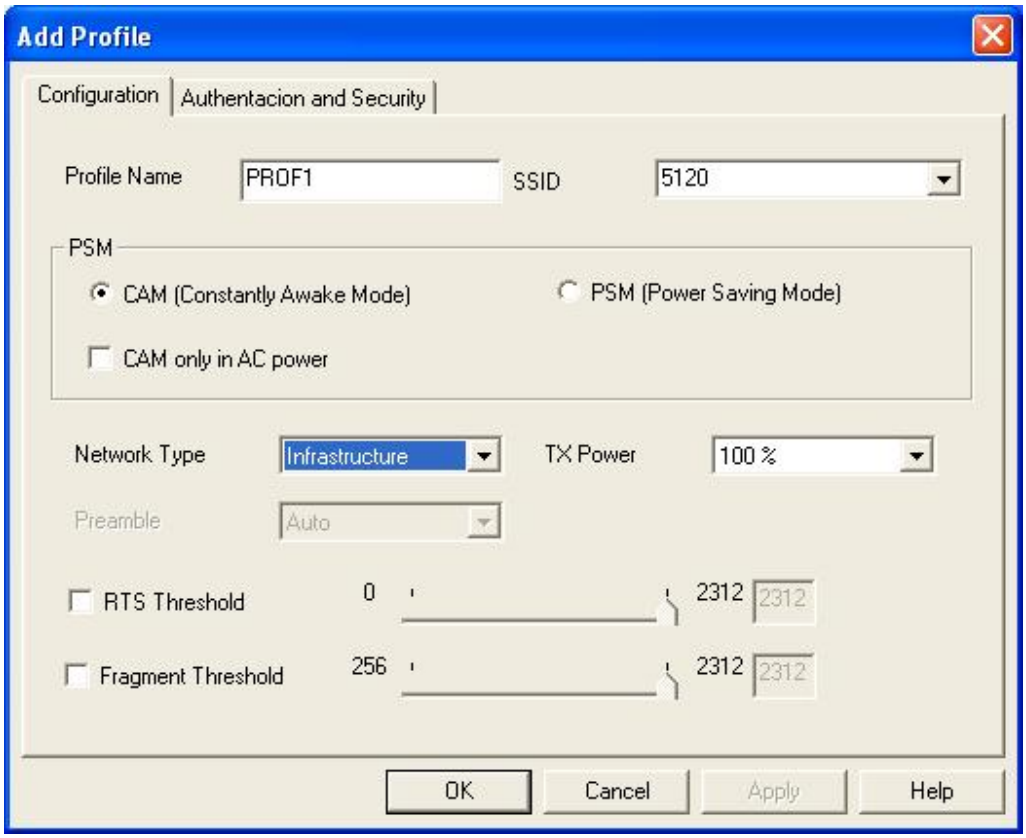
The **Profile** tab displays the profile lists and allows you to add, delete, edit or activate an existing profile. The next few sections will guide you through the steps in order to crate a new profile.

Begin creating a profile by clicking on the **Add** button.



3.1.1 Infrastructure Configuration

After clicking on the **Add** button in **Profile** tab, the **Configuration** tab will be displayed.

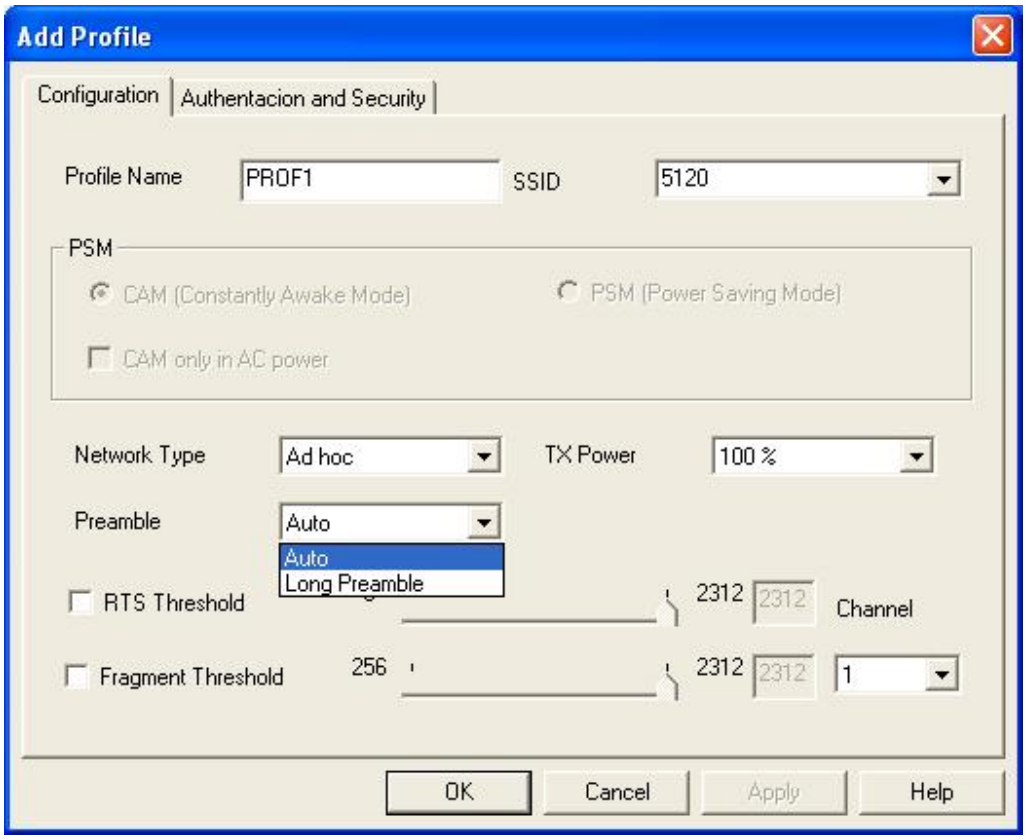


- **Profile Name:** Specify a name for this profile; this can be any name that you may associate with your network. This feature comes in handy when you need to work at several locations where there are different network settings. Using this you can configure a different profile for each of your networks.
- **SSID**: Specify the SSID of the network. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **PSM:** There are two options for PSM (Power Saving Mode). Select a radio button for either **CAM** (Constantly Awake Mode) or **PSM** (Power Saving Mode).
- **Network Type:** Select **Infrastructure** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list.
- **RTS Threshold:** place a check in this box and adjust the value for the RTS threshold. Any packet in the RTS/CTS handshake larger than the specified size will be discarded. It is recommended to leave this value at its max.
- **Fragment Threshold:** place a check in this box and adjust the value for the fragment threshold. It is recommended to leave this value at its max.

- Click on the **OK** button to create the profile with the specified settings.

3.1.2 Ad-hoc Configuration

After clicking on the **Add** button in **Profile** tab, the **Configuration** tab will be displayed.



- **Profile Name:** Specify a name for this profile; this can be any name that you may associate with your network. This feature comes in handy when you need to work at several locations where there are different network settings. Using this you can configure a different profile for each of your networks.
- **SSID**: Specify the SSID of the network. The SSID is a unique name shared among all points in your wireless network. The SSID must be
- **Network Type:** Select **Ad hoc** from the drop-down list.
- **Preamble:** Select **Auto** or **Long Preamble** from the drop-down list.
- **RTS Threshold:** place a check in this box and adjust the value for the RTS threshold. Any packet in the RTS/CTS handshake larger than the specified size will be discarded. It is recommended to leave this value at its max.
- **Fragment Threshold:** place a check in this box and adjust the value for the fragment threshold. It is recommended to leave this value at its max.
- **Channel:** Select the channel number from the drop-down list.

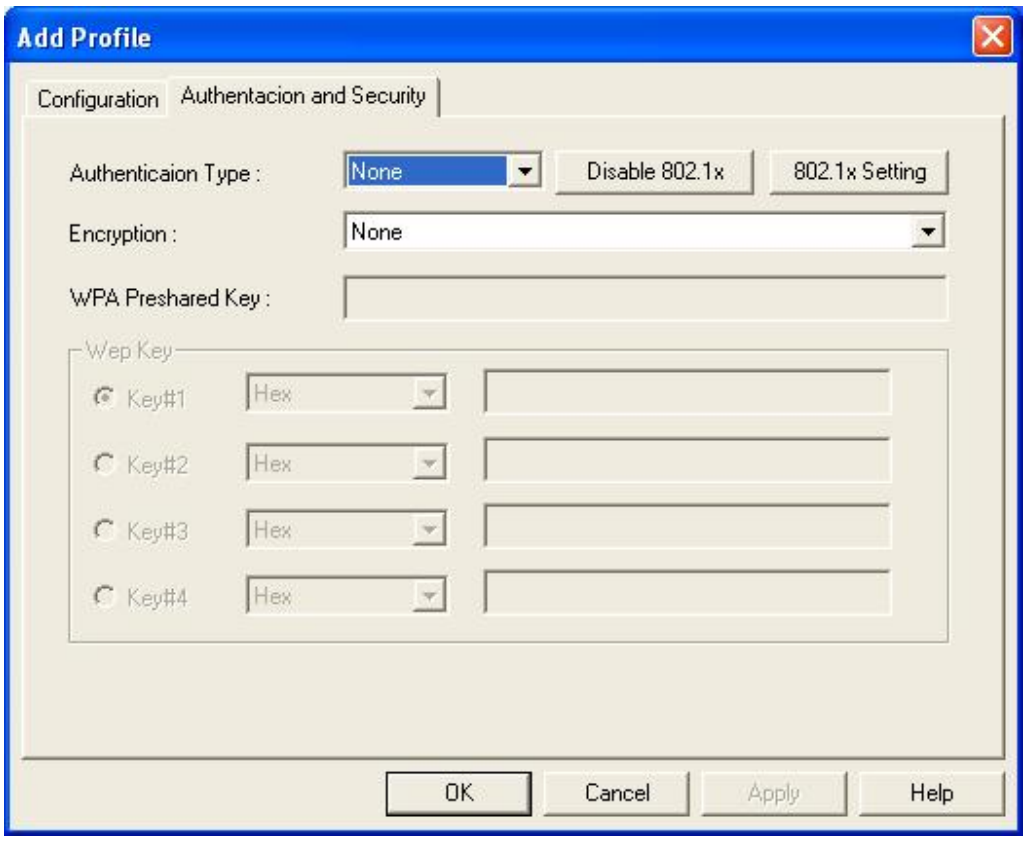
➢ Click on the **OK** button to create the profile with the specified settings.

3.1.3 Authentication and Security

Click on the Authentication and Security tab to configure the authentication and encryption settings. The next few sections discuss how to configure these settings.

3.1.3.1 Authentication & Encryption Disabled

In order to disable authentication and encryption follow the steps below.

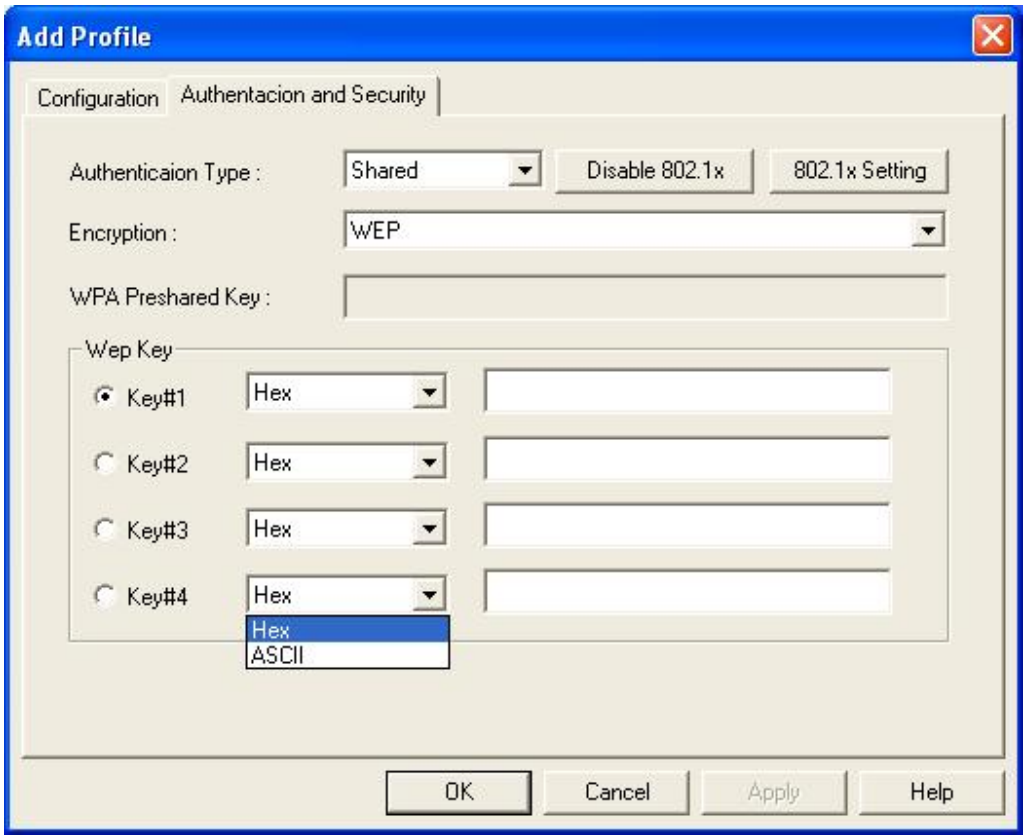


➢ **Authentication Type:** Select **None** from the drop-down list.
➢ **Encryption:** Select **None** from the drop-down list.
➢ Click on the **OK** button to save the changes.

3.1.3.2 WEP Encryption

WEP (Wired Equivalent Privacy) is designed to make the data transmission as secure as a wired connection. You may select 64 or 128-bit WEP key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase.

In order to use WEP encryption follow the steps below.

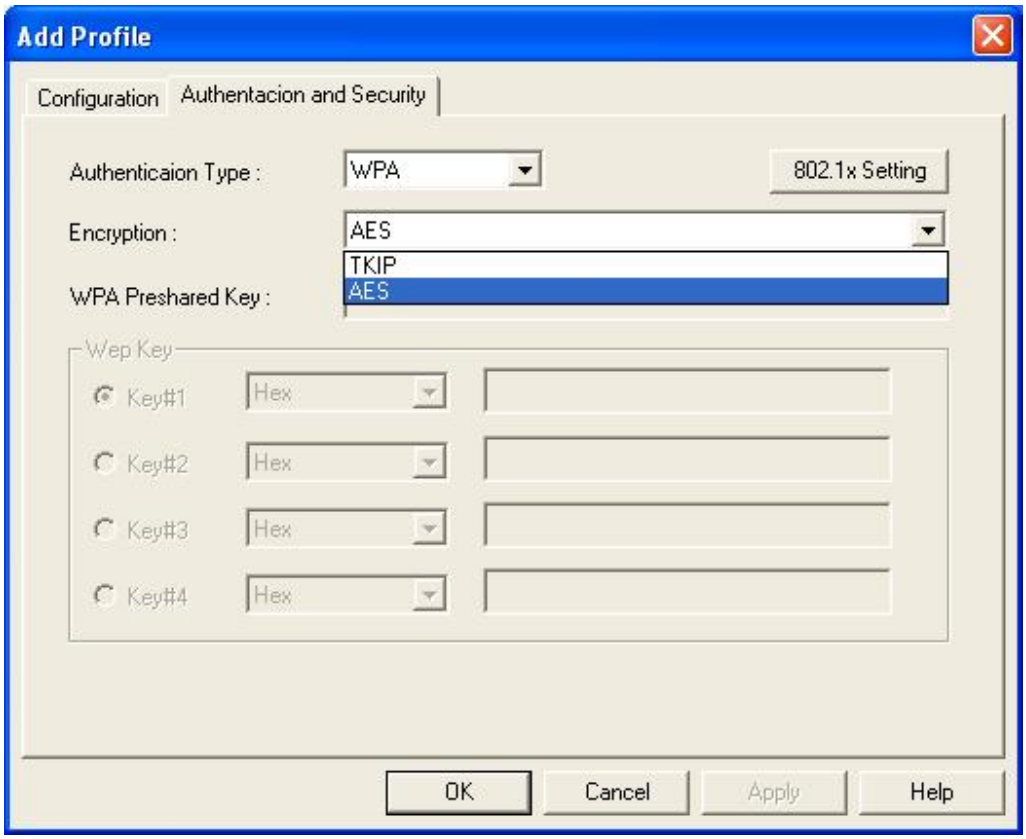


- **Authentication Type:** Select **Shared** from the drop-down list.
- **Encryption:** Select **WEP** or **None** from the drop-down list.
- **WEP Key:** Select a key number, and then select **Hex** or **ASCII** from the drop down list. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the **OK** button to save the changes.

3.1.3.3 WPA Authentication with TKIP / AES encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with.

In order to use WPA authentication follow the steps below.



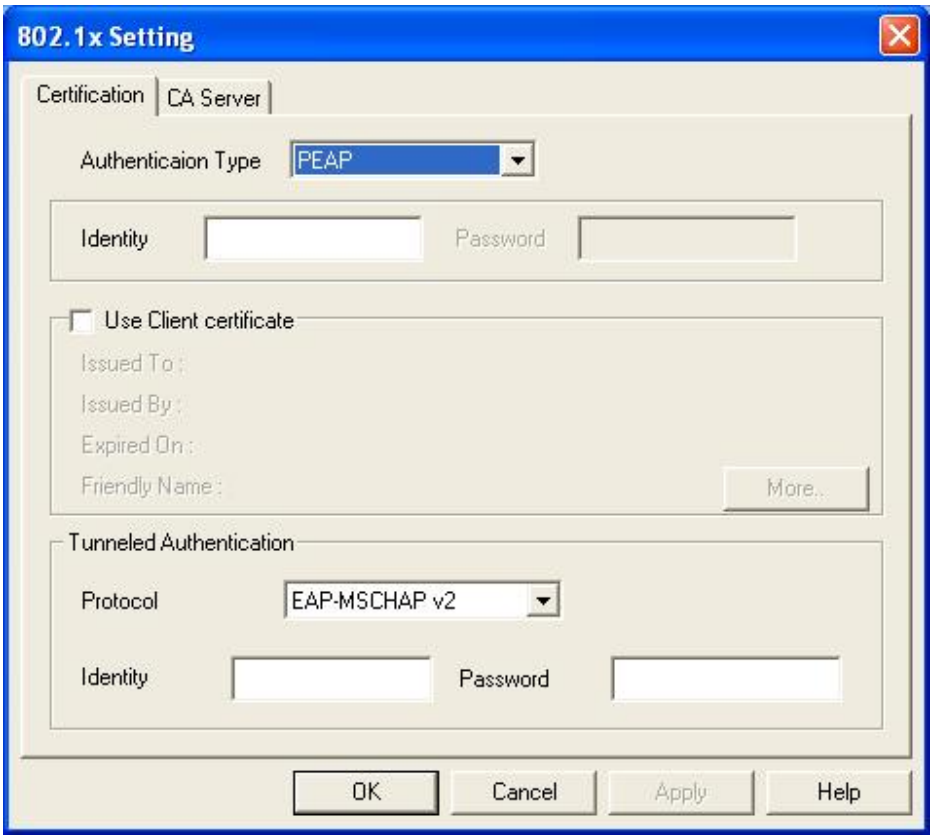
- **Authentication Type:** Select **WPA** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- **WPA-Preshared Key:** Specify the pre-shared key.
- Click on the **OK** button to save the changes.

3.1.3.4 802.1x Settings

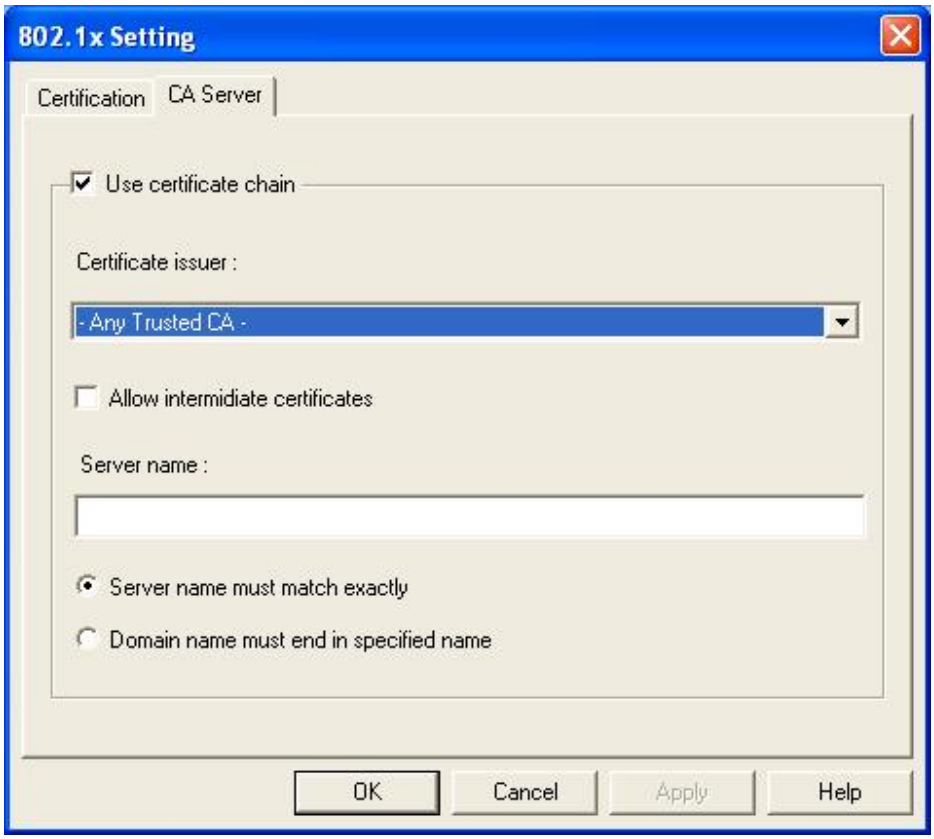
Click on the **802.1x Settings** button in order to configure 802.1x. The following encryptions methods can be configured: PEAP, TLS / Smartcard, TTLS, LEAP, MD5-Challenge.

3.1.3.4.1 PEAP

PEAP (Protected Extensible Authentication Protocol) is a protocol developed jointly by Microsoft, RSA Security, and Cisco for transmitting authentication data, including passwords over an 802.11 wireless network. PEAP authenticates wireless LAN clients using only server-side digital certificates by creating an SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.



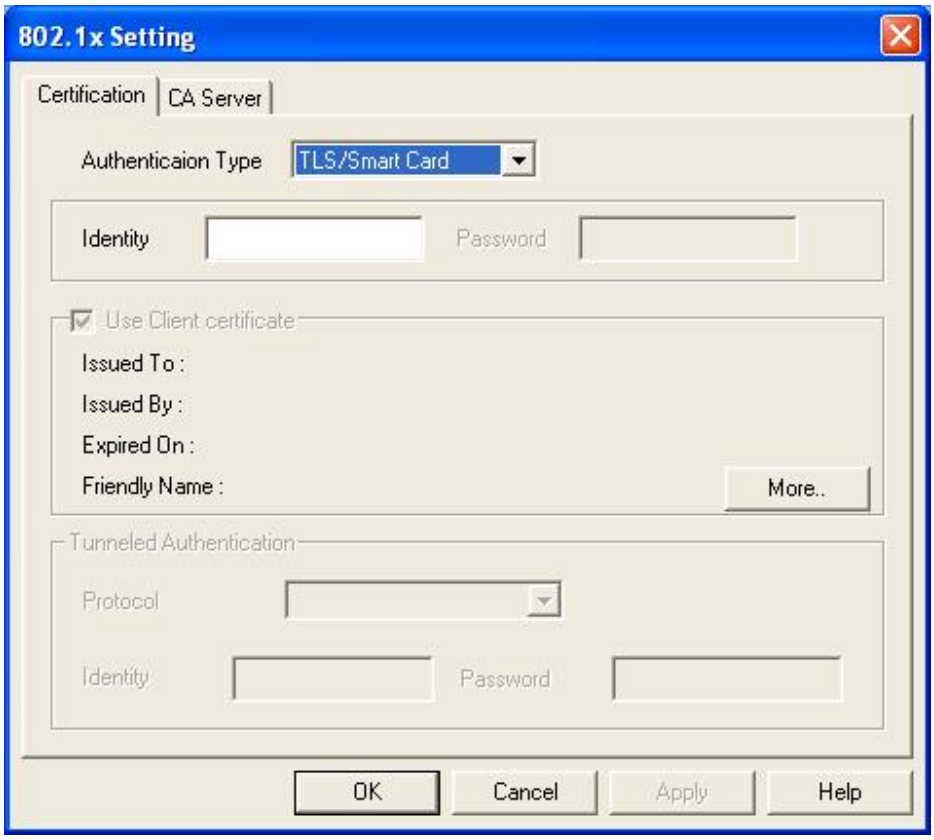
- **Authentication Type:** Select **PEAP** from the drop-down list.
- **Identity:** Specify the user name.
- **Use Client certificate:** Place a check in this box, and then click on the **CA Server** tab to configure the CA settings.
- **Tunneled Authentication:** Select the protocol from the drop down list and then enter the username and password.
- **CA Server:** If you need to configure the CA settings, click on the **CA Server** tab.



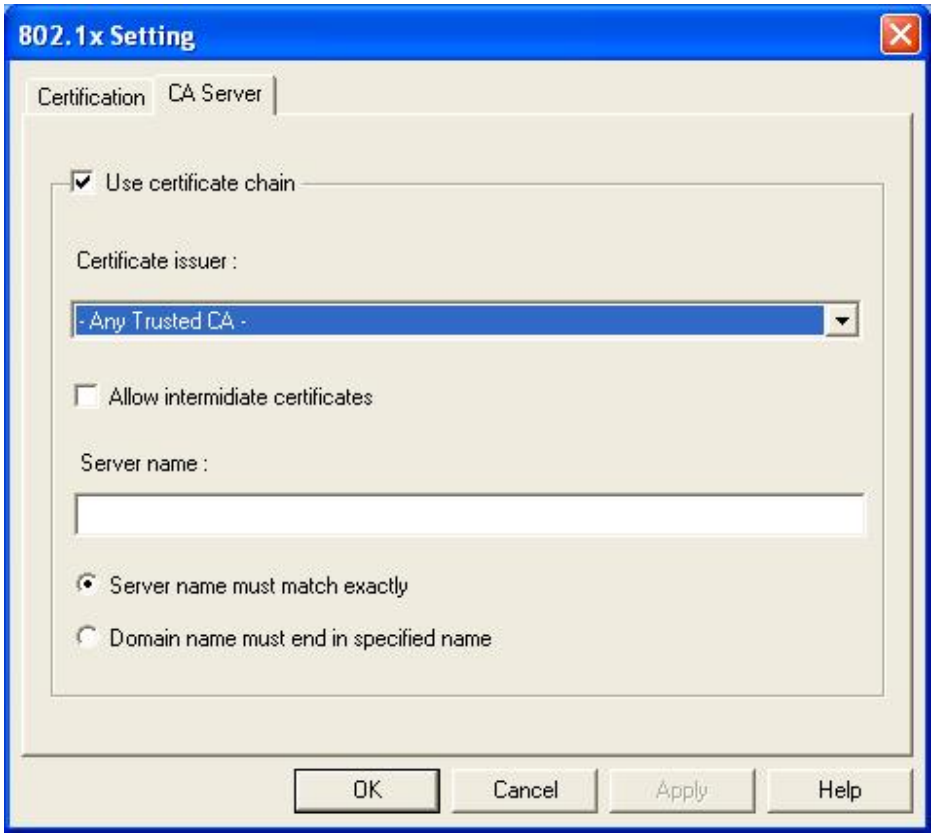
- **Use certificate chain:** Place a check in this box if you would like to use a CA, and then select a CA from the drop-down list.
- **Allow intermediate certificates:** Place a check in this box if you would like to allow intermediate certificates. During tunnel creation the Client must verify the Server's certificate. When checking this certificate the signature is verified against a list of trusted certificate authorities. If this parameter is true then the Client will also accept a signature from a trusted intermediate certificate authority, otherwise we will not.
- **Server name;** Specify the Server's name. During tunnel creation the Client must verify the Server's certificate. This parameter indicates whether the Server's name must match the **Server Name** parameter exactly or if only the sub domain must match.
- Click on the **OK** button to save the changes.

3.1.3.4.2 TLS / Smartcard

TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.

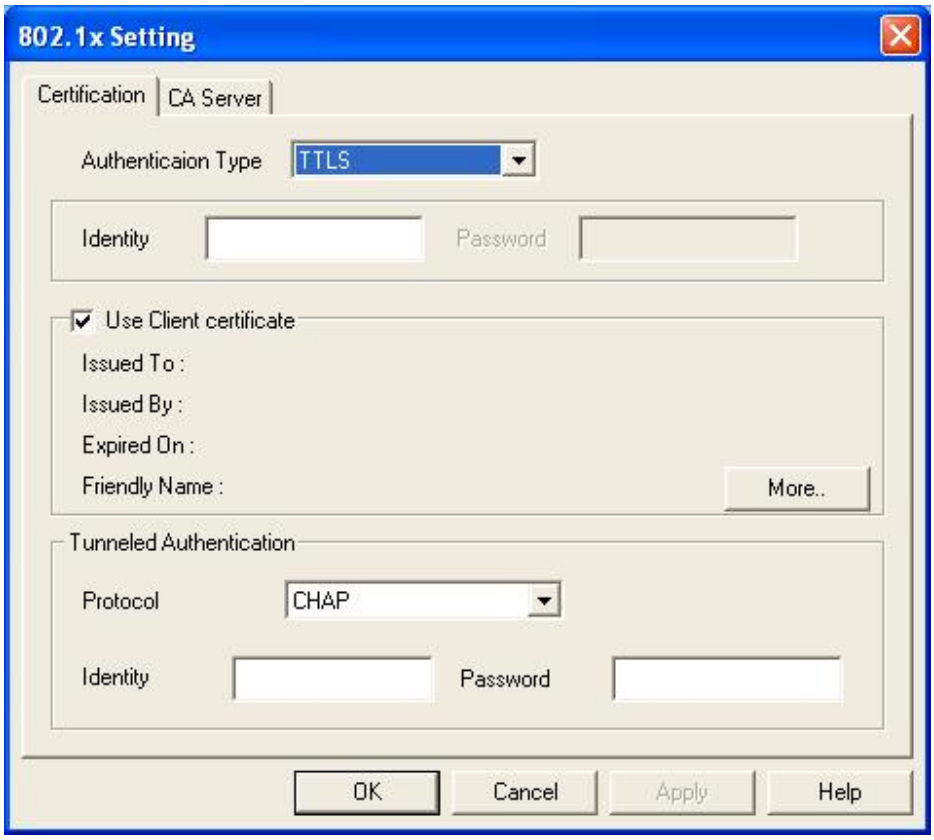


- **Authentication Type:** Select **TLS / Smartcard** from the drop-down list.
- **Identity:** Specify the user name.
- **CA Server:** If you need to configure the CA settings, click on the **CA Server** tab.

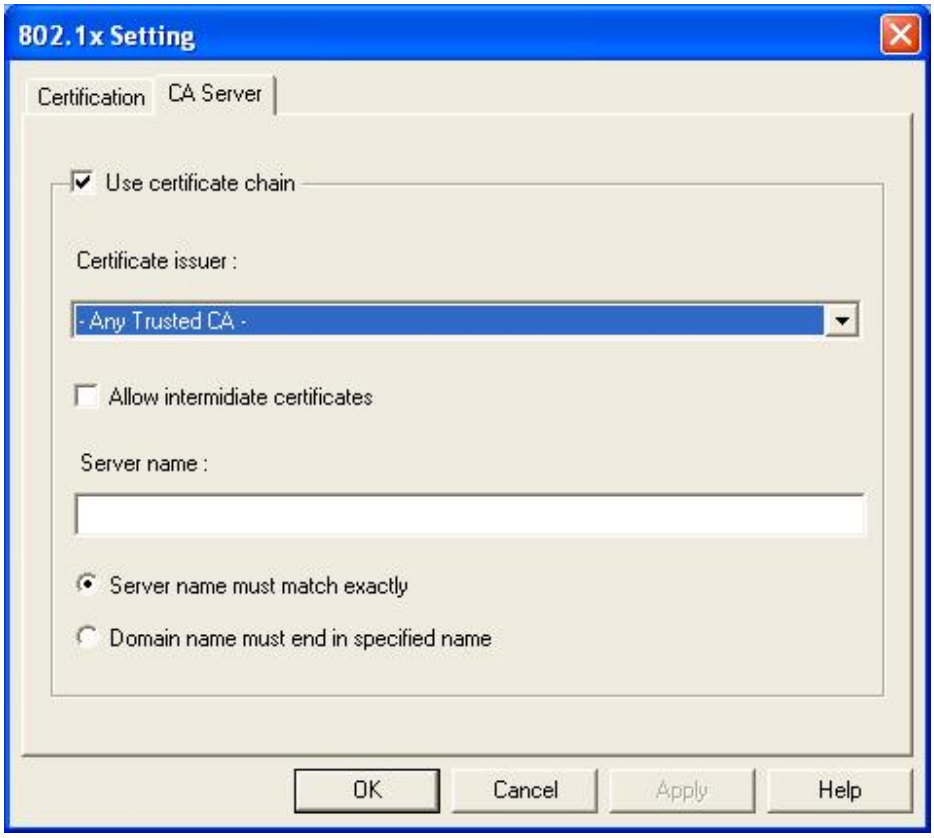


- **Use certificate chain:** Place a check in this box if you would like to use a CA, and then select a CA from the drop-down list.
- **Allow intermediate certificates:** Place a check in this box if you would like to allow intermediate certificates. During tunnel creation the Client must verify the Server's certificate. When checking this certificate the signature is verified against a list of trusted certificate authorities. If this parameter is true then the Client will also accept a signature from a trusted intermediate certificate authority, otherwise we will not.
- **Server name;** Specify the Server's name. During tunnel creation the Client must verify the Server's certificate. This parameter indicates whether the Server's name must match the **Server Name** parameter exactly or if only the sub domain must match.
- Click on the **OK** button to save the changes.

3.1.3.4.3 TTLS



- **Authentication Type:** Select **TTLS** from the drop-down list.
- **Identity:** Specify the user name.
- **Password:** Specify the password.
- **Use Client certificate:** Place a check in this box, and then click on the **CA Server** tab to configure the CA settings.
- **Tunneled Authentication:** Select the protocol from the drop down list and then enter the username and password.
- **CA Server:** If you need to configure the CA settings, click on the **CA Server** tab.



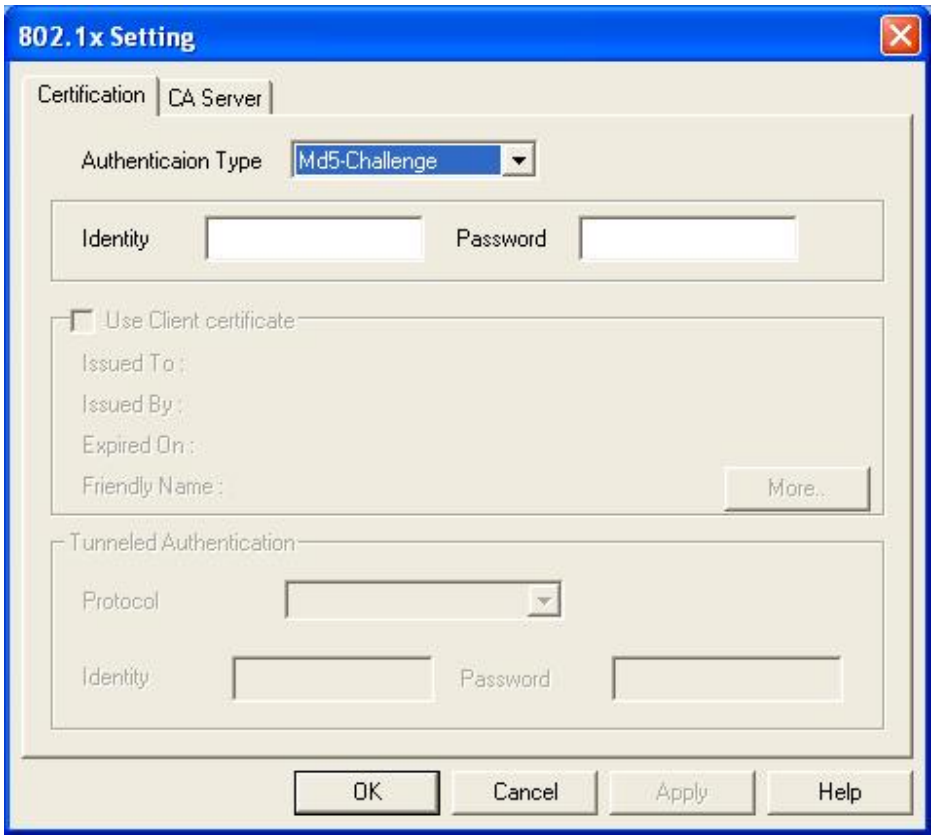
- **Use certificate chain:** Place a check in this box if you would like to use a CA, and then select a CA from the drop-down list.
- **Allow intermediate certificates:** Place a check in this box if you would like to allow intermediate certificates. During tunnel creation the Client must verify the Server's certificate. When checking this certificate the signature is verified against a list of trusted certificate authorities. If this parameter is true then the Client will also accept a signature from a trusted intermediate certificate authority, otherwise we will not.
- **Server name;** Specify the Server's name. During tunnel creation the Client must verify the Server's certificate. This parameter indicates whether the Server's name must match the **Server Name** parameter exactly or if only the sub domain must match.
- Click on the **OK** button to save the changes.

3.1.3.4.4 LEAP

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN.

- **Authentication Type:** Select **LEAP** from the drop-down list.
- **Identity:** Specify the user name.
- **Password:** Specify the password.
- Click on the **OK** button to save the changes.

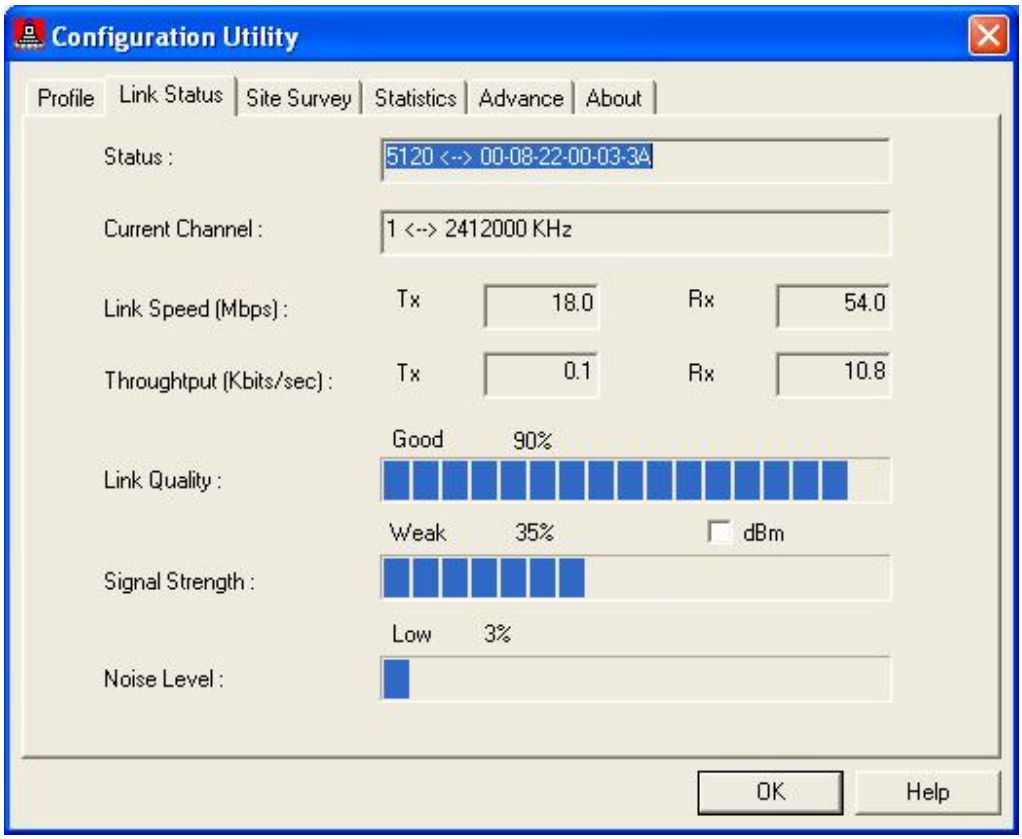
3.1.3.4.5 MD5 – Challenge



- **Authentication Type:** Select **MD5-Challenge** from the drop-down list.
- **Identity:** Specify the user name.
- **Password:** Specify the password.
- Click on the **OK** button to save the changes.

3.2 LINK STATUS

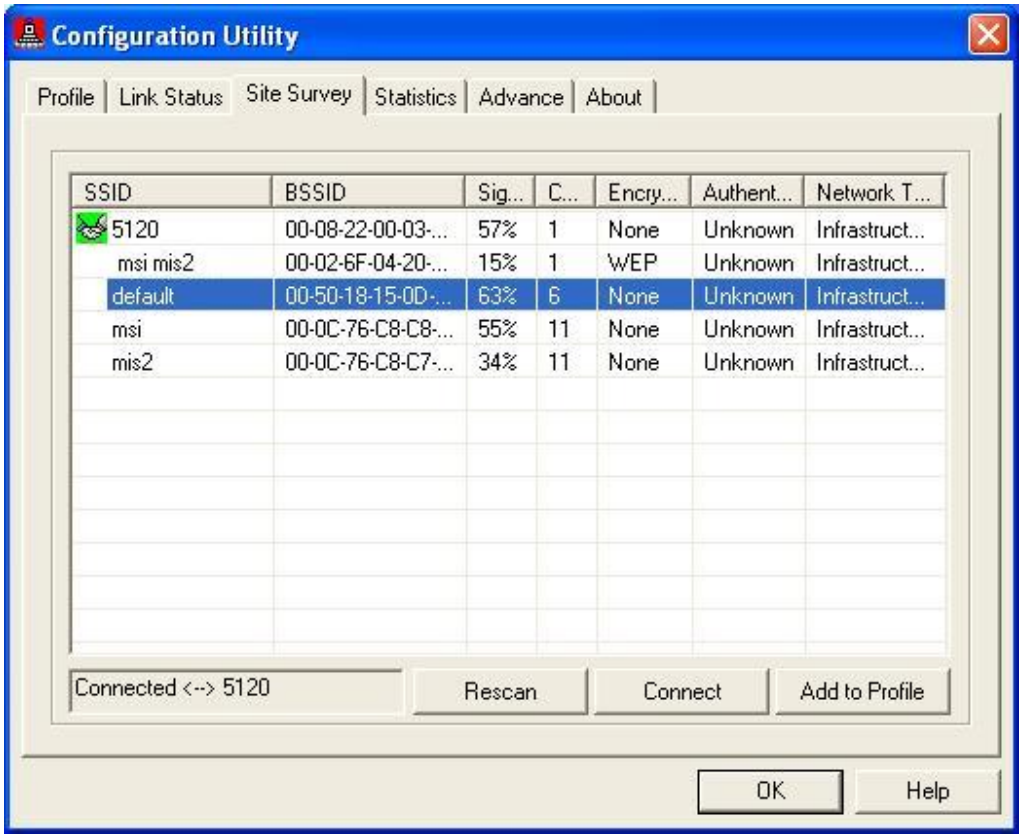
The **Status** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.



- **Status**: This indicates the status of the client and the MAC address of the Access Point (Infrastructure) or Client (Ad-hoc) that it is connected to.
- **Current Channel:** The operating frequency channel that the client is using (infrastructure mode). Displays the operating channel and frequency.
- **Link Speed (Mbps)**: The current data rate at which the client is transmitting.
- **Throughput (Kbits/sec):** Displays the Tx (transmit) and Rx (receive) bytes per second.
- **Link Quality:** In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- **Signal Strength:** This bar displays the strength of the signal received from an AP or client.
- **Noise Level:** displays the amount of interference in the surrounding area.
- Click on the **OK** button.

3.3 SITE SURVEY

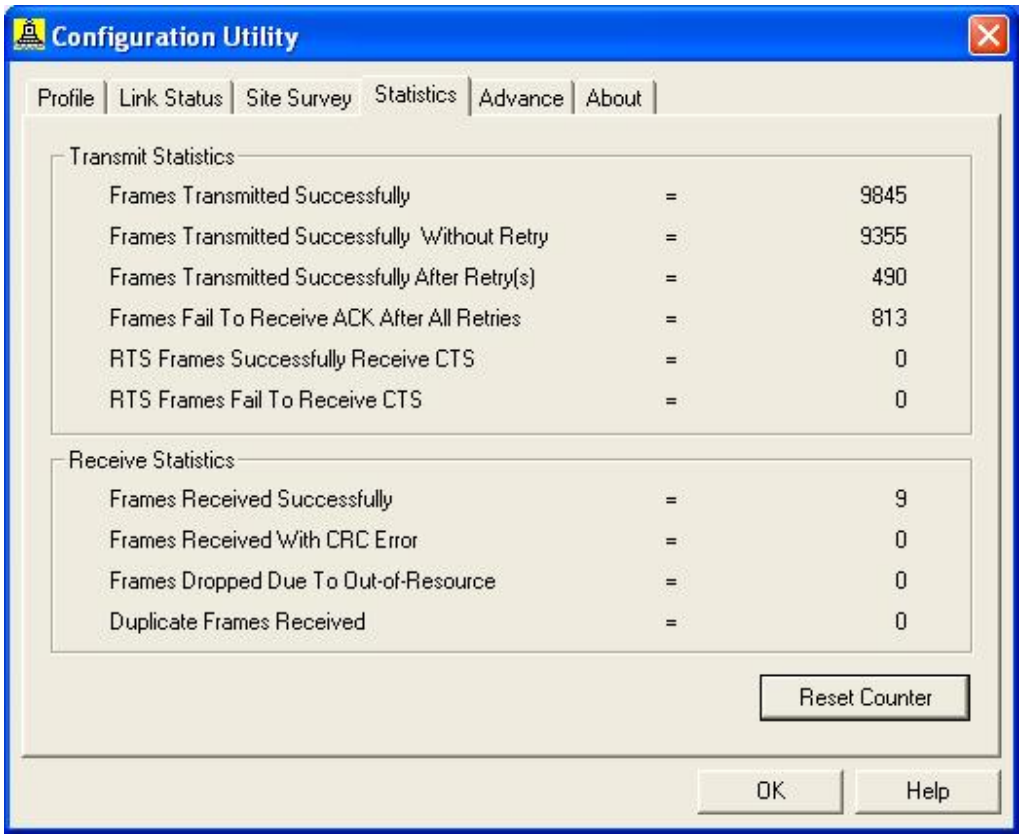
The **Site Survey** tab displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.



- **Rescan:** Click on this button to rescan the environment for a better signal/frequency and more AP or Stations.
- **Connect**: to connect with a specific Access Point, select the Access Point from the drop-down list, and then click on the **Connect** button.
- **Add to Profile**: Click on this button to add the selected setting to a profile.
- Click on the **OK** button.

3.4 STATISTICS

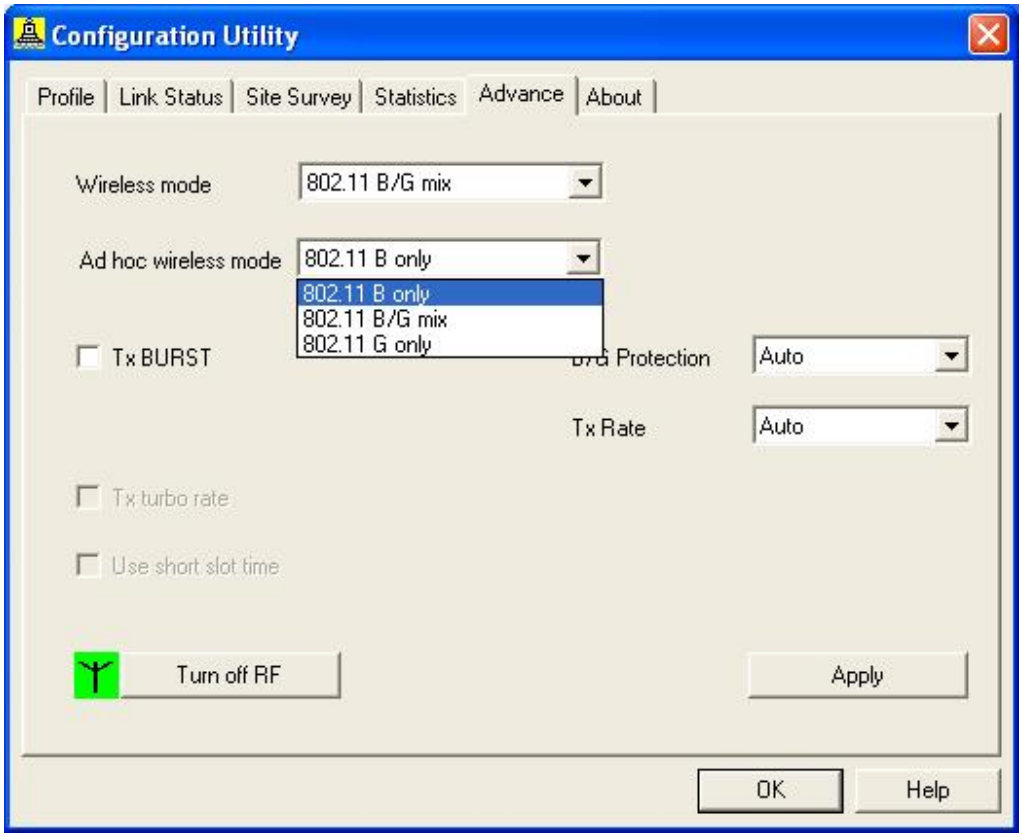
The **Statistics** tab displays the transmitted and received statistics. The following information is included in this tab, as the image depicts below.



- **Reset Counter**: Click on this button to clear the results.
- Click on the **OK** button.

3.5 ADVANCE

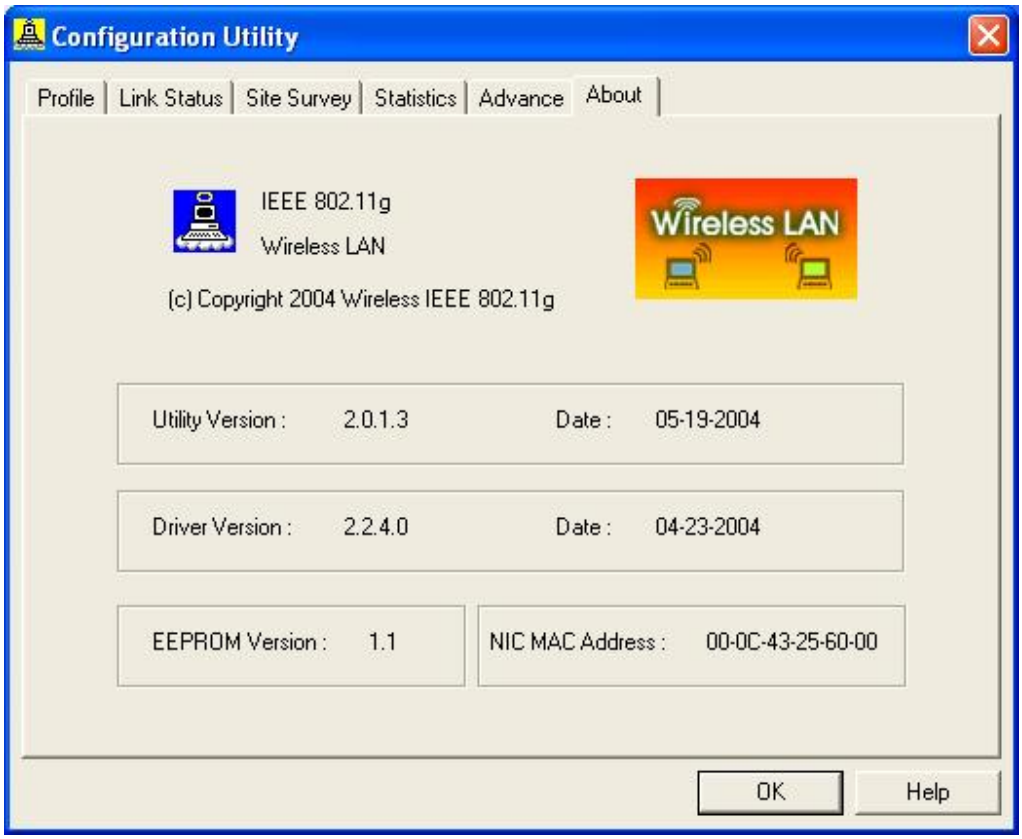
The **ADVANCE** tab allows you to configure the wireless transfer mode.



- **Wireless mode:** Select **B/G-mix** or **B-only** from the drop-down list. For best performance, this should be the same as your AP settings.
- **Ad hoc wireless mode:** Select **B-only**, **B/G-mix** or **G-only** from the drop-down list.
- **Tx BURST:** Place a check in this box if you would like to use Transmit Burst. This is the amount of time the radio will be reserved to send data without requiring an ACK. Adding a burst time should help throughput for 802.11g clients when running in G-only or B/G mix modes.
- **Turn off RF:** Click on this button to turn OFF the radio. Click on it once again to turn the radio back ON.
- Click on the **OK** button.

3.6 ABOUT

This tab displays information about the device. This includes the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) MAC address.



➤ Click on the **OK** button.

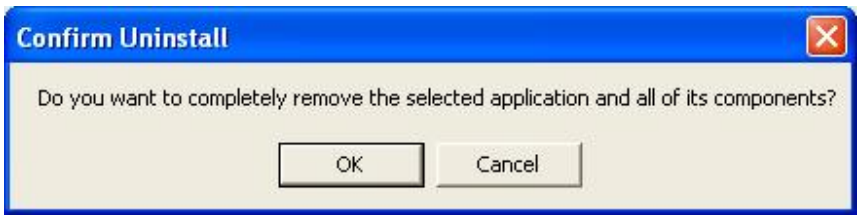
4 Uninstall the Drivers & Client Utility

If the device installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the device and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the Client Utility:

1. Click on Start > Programs > Wireless IEEE 802.11g > RT2500 > **Uninstall**
2. You will then see the following screen, select the **Remove** radio button and then click on **Next** button.

3. You will then need to confirm your decision. Click on the **OK** button.



4. At this point you must remove the device from your computer, and then click on the **OK** button. The Uninstallation is complete.

Appendix A – Specifications

General	
Data Rates	1,2,5.5,6,9,11,12,18,24,36,48,54 Mbps
Network Standards	IEEE802.11, IEEE 802.11b, 802.11g
Compliance	FCC Part 15/UL, ETSI 300/328/CE
Drivers	Windows 98/ME/2000/XP
Operational voltage	3.3 ± 0.15V
Current consumption	Continue Tx: < 480mA Continue Rx: < 250mA
Security	IEEE802.1x Client Support—Work with Windows XP Utility WPA -- Wi-Fi Protected Access (64,128-bit WEP with TKIP) —Work with Windows XP Utility
RF Information	
Frequency Band	2412 – 2483.5 MHz
Channels	11 for North America, 14 for Japan, 13 for Europe, 2 for Spain, 4 for France
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation Technology	Orthogonal Frequency Division Multiplexing (OFDM) DBPSK @ 1Mbps DQPSK @2Mbps CCK @ 5.5 & 11Mbps BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps
Receive Sensitivity (Typical)	-89dBm @ 1Mbps -84dBm @ 6Mbps -77dBm @ 24Mbps -89dBm @ 2Mbps -84dBm @ 9Mbps -74dBm @ 36Mbps -87dBm @ 5.5Mbps -82dBm @ 12Mbps -69dBm @ 48Mbps -84dBm @ 11Mbps -80dBm @ 18Mbps -67dBm @ 54Mbps

Available transmit power (Depends on Different Countries' Regulation)	17 ± 2dBm @1, 2, 5.5 and 11Mbps 13 ± 2dBm @48, 54Mbps
Physical	
LED	RF Link activity
Interface	32-bit CardBus PC Card Standard V7.1 Type II
Antenna	Integrated built-in diversity Antenna
Dimensions	118(L) mm x 54(W) mm x 7.5(H) mm
Environmental	
Temperature Range	0°C to 55°C – Operating -40°C to 70°C – Storage
Humidity (non-condensing)	5%~95% Typical

Appendix B – FCC Interference Statement

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.
This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Senao declared that WPC-3006 is limited in CH1~11 by specified firmware controlled in USA.

The equipment has been SAR-evaluated for use in laptops (notebooks) with sidw slot confiquration.