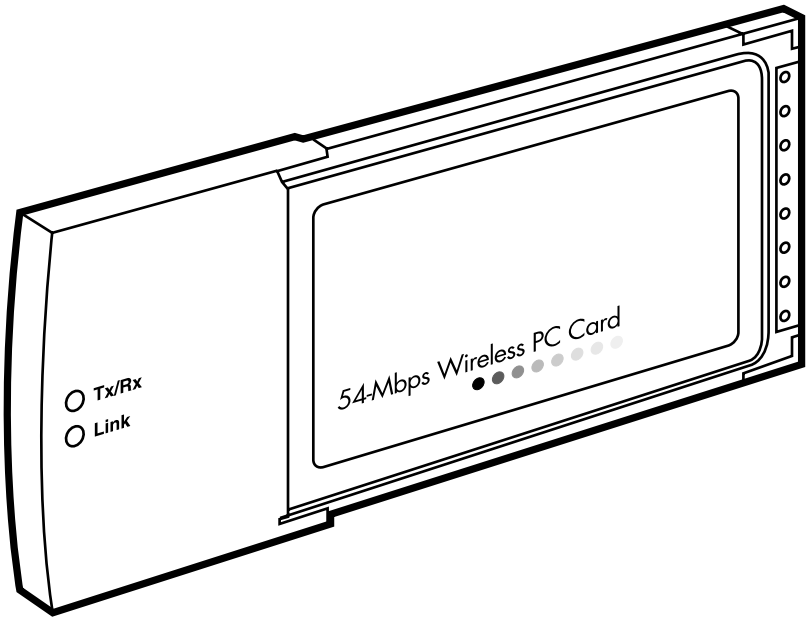
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

JUNE 2004
LW6000A

Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S.: Call **877-877-BBOX** (outside U.S. call **724-746-5500**)
FREE technical support 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mailing address: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION and INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular 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. If this equipment does cause harmful interference to radio or telephone 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 an experienced radio/TV technician for help.

CAUTION

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

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

EUROPEAN UNION DECLARATION OF CONFORMITY

This equipment complies with the requirements of the European EMC Directive 89/336/EEC.

CE

NORMAS OFICIALES MEXICANAS (NOM)
ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

TRADEMARKS USED IN THIS MANUAL

Linux is a registered trademark of Linus Torvalds.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

NetWare is a registered trademark of Novell, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Contents

1. Specifications

Antenna: Diversity patch

Distance (Maximum): 328 ft. (100 m)

Frequency Band: 2.4000–2.4835 GHz

Interface: 32-bit cardbus

Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g) BPSK, QPSK, CCK (11b)

Operating System: Compatible with all major operating systems; Drivers included for Windows® 98 SE/Me/XP, Windows 2000, and Linux®

Security: 64-/128-/152-bit WEP data encryption, WPA (TKIP with IEEE 802.1x), and AES

Speed: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1 Mbps with auto fallback

Standards: IEEE 802.11b, IEEE 802.11g

Transmit Power: 16 dBm to18 dBm

Receive Sensitivity: 54 Mbps OFDM, 10% PER, -70 dBm, 11 Mbps CCK, 8% PER, -86 dBm, 1 Mbps BPSK, 8% PER, -92 dBm

Connectors: (1) Type 2 PCMCIA

Indicators: LEDs: (1) TX/RX, (1) Link

Temperature Tolerance: 32 to 131°F (0 to 55°C)

Humidity: Up to 95%, noncondensing

Power: From the interface

Size: 0.3"H x 4.6"W x 2.1"D (0.8 x 11.7 x 5.3 cm)

2. Introduction

2.1 Overview

The Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter is used to attach a PC to another network device using wireless technology to transfer data. It complies with the IEEE 802.11g standard, which supports high-speed wireless network connections up to 54 Mbps. It can also work with IEEE 802.11b devices. When the adapter connects to 11b devices, maximum link speed is 11 Mbps.

High throughput supports multimedia data bandwidth, and 64-/128-/152-bit WEP, WPA (TKIP [Temporal Key Integrity Protocol] with IEEE 802.1x), and AES functions for a high level of security. Client users are required to get authorization before connecting to access points (APs) or AP routers, and the data transmitted in the network is encrypted/decrypted by a dynamically changed secret key. Automatic fallback also increases data security and reliability.

The adapter works with Windows 98 SE/Me/XP and Windows 2000, and it supports a 32-bit cardbus interface.

Two power-saving features make the adapter particularly efficient. First, the adapter's power consumption is very low. Second, you can control how long the adapter's attached devices' power stays on. Simply set the time (in minutes) that your portable or handheld devices wait before powering off.

2.2 What's Included

Before you begin the installation, check the contents of your package. The package should include the following items:

- (1) Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter
- (1) CD-ROM containing this users' manual and software drivers

If anything is missing or damaged, please contact Black Box at 724-746-5500.

3. Installation

Before you proceed with the installation, read the following notes.

NOTES

Do not install the adapter in your laptop computer before installing the software program from the CD.

The following installation was operated under Windows XP. (Procedures are similar for Windows 98 SE/Me and Windows 2000.)

If you have installed the Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter driver and utility before, please uninstall the old version first.

1. Insert the Installation CD in your CD-ROM drive. The screen shown in Figure 3-1 appears.

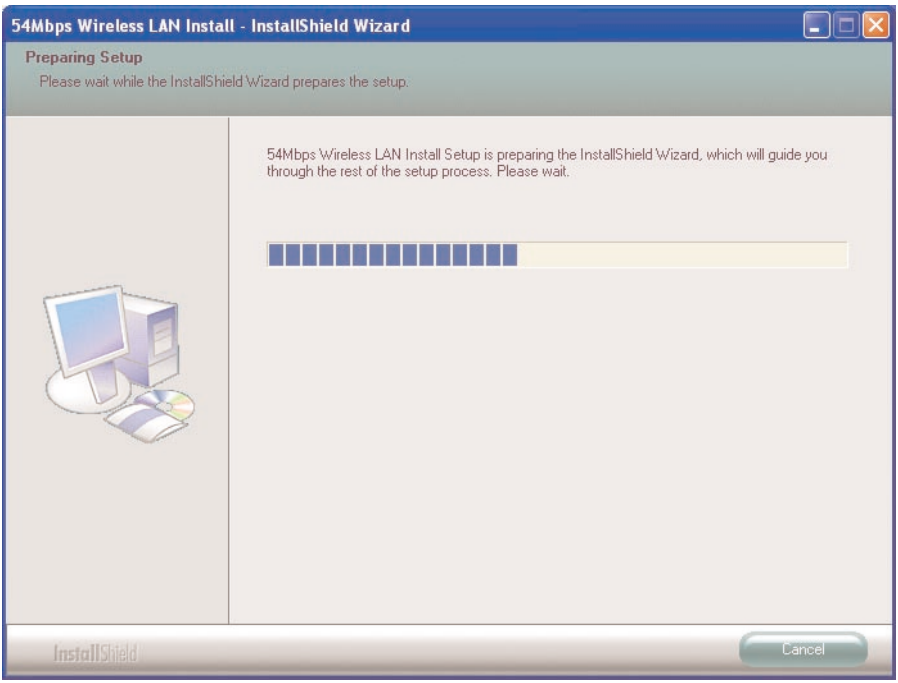


Figure 3-1. InstallShield Wizard screen, preparing setup.

2. Once the software finishes preparing for setup, the screen shown in Figure 3-2 appears. Click on **Easy Install** or **Next** to continue.

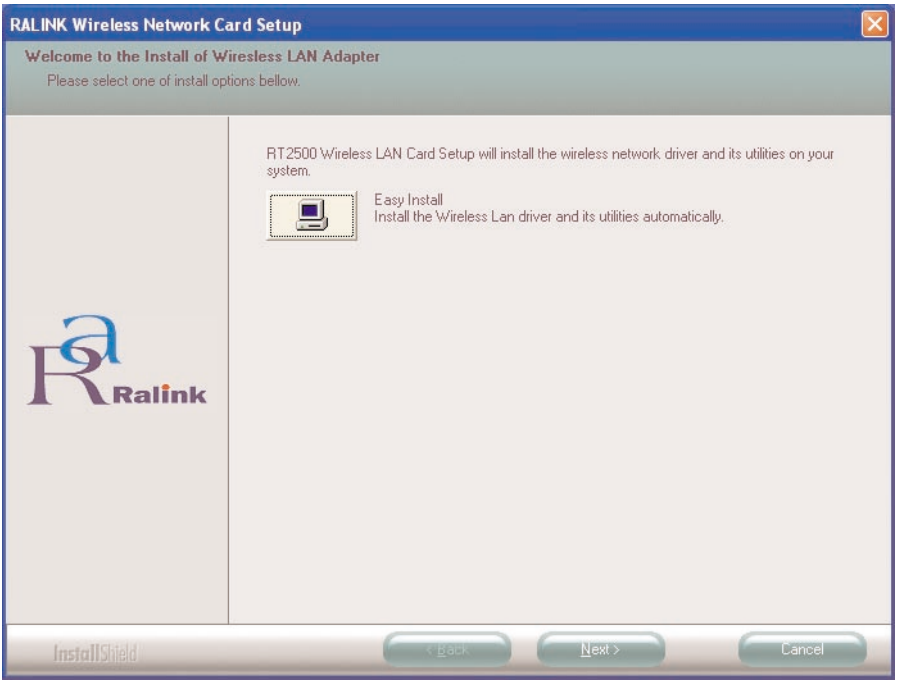


Figure 3-2. Setup screen.

3. The system starts to install the card's software (sees Figure 3-3 and 3-4). Follow the program's instructions to plug the PC card into your laptop computer's cardbus slot (see Figure 3-5).

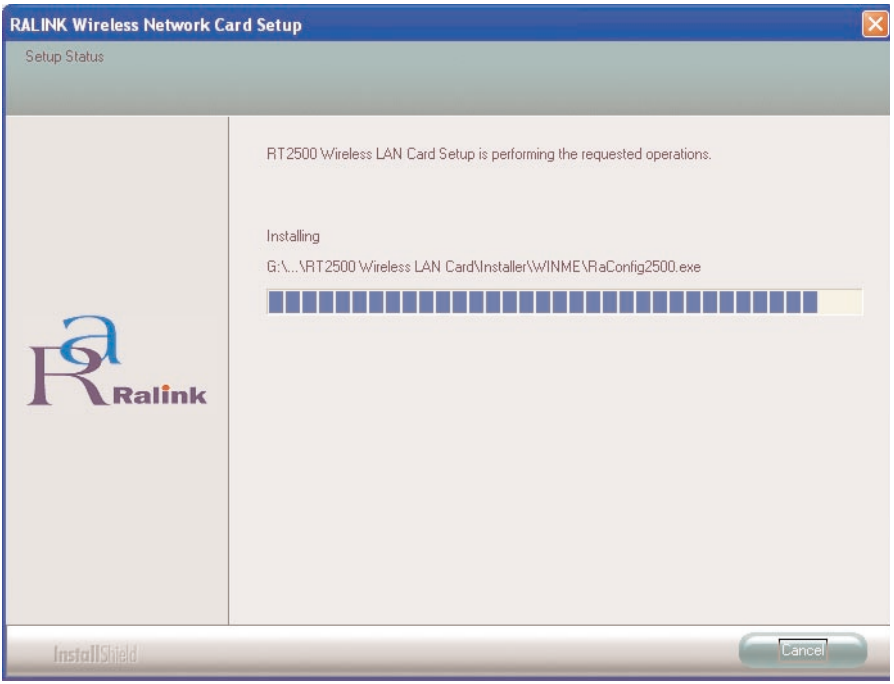


Figure 3-3. This screen appears first as the system installs the software, then the two screens below appear.

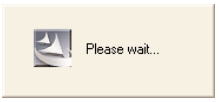


Figure 3-4. Wait while software is installed.

Figure 3-5. Plug in the adapter.

4. The system will automatically detect the card and display the Hardware Installation screen. See Figure 3-6. Click on **Continue Anyway** to continue. Figure 3-7 appears as the adapter is installing.

Figure 3-6. The hardware installation screen.

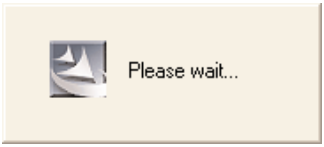


Figure 3-7. Wait while hardware is installed.

5. The current card's country channel setting is displayed for your reference. See Figure 3-8. If you are in different country, please change the country channel from the drop-down menu, then click on **Next**.

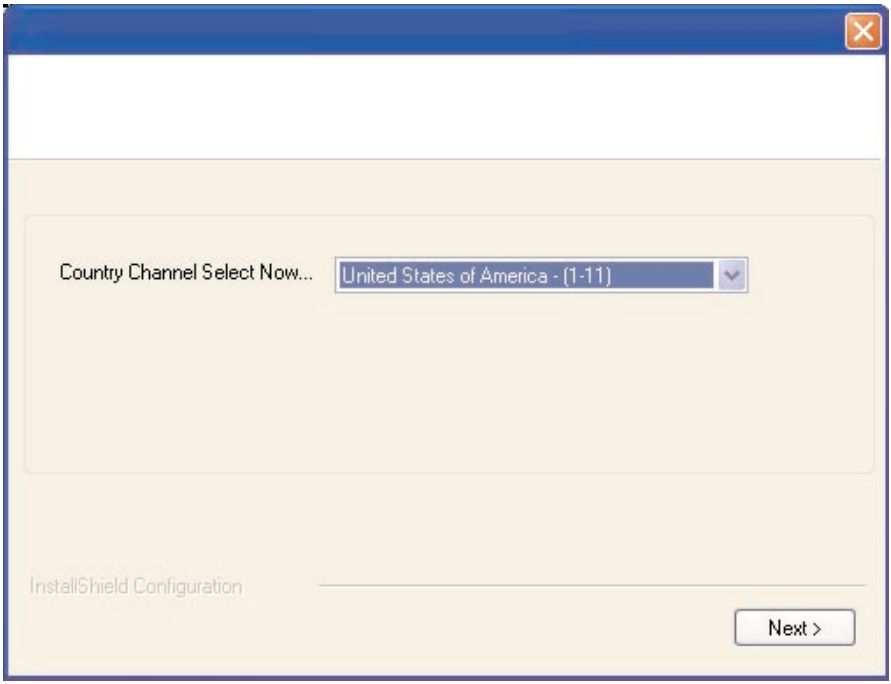


Figure 3-8. Selecting the country channel.

6. The Ralink Chipset screen (a common hardware chipset) appears. See Figure 3-9. Click on **Finish** to complete the installation.

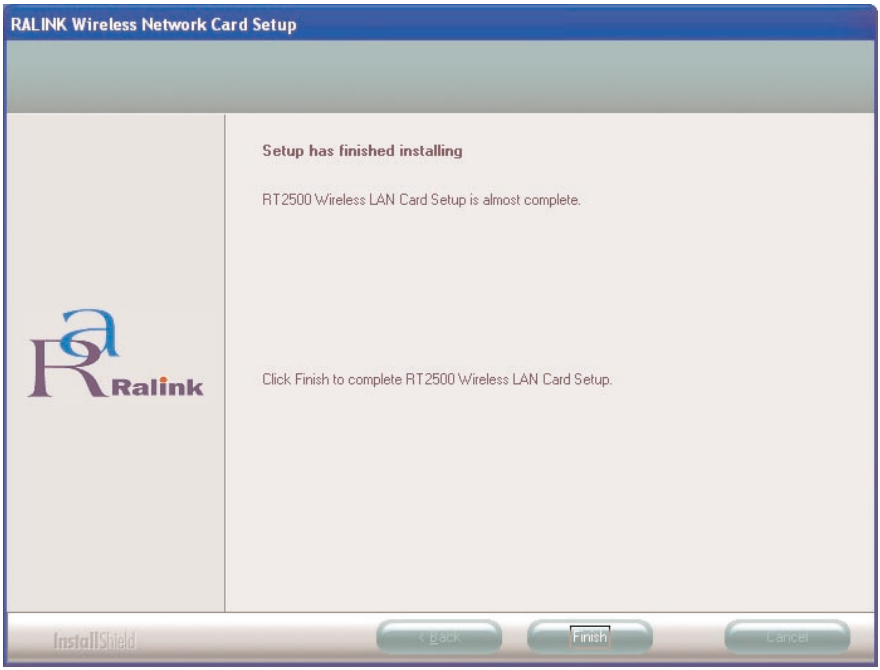


Figure 3-9. The Ralink Chipset screen.

7. The Config utility screen appears, and you can begin configuring the card as described in **Chapter 4**.

4. Configuration Utility

The Configuration Utility is a powerful application that helps you configure the adapter and monitor the link status and the statistics during the communication process.

The Configuration Utility appears as an icon on the Windows system tray while the card is running. Open it by double-clicking on the workstations icon (fourth from left in Figure 4-1). The next screen (not shown in this manual) appears. From this screen, select **Launch Config Utilities** to open the Configuration Utility tool, or select **Exit** to close the Configuration Utility tool.

Figure 4-1. Windows system tray.

4.1 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your card and automatically connect to the wireless device with the highest signal strength. From the Site Survey tab, all the networks nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list. See Table 4-1.

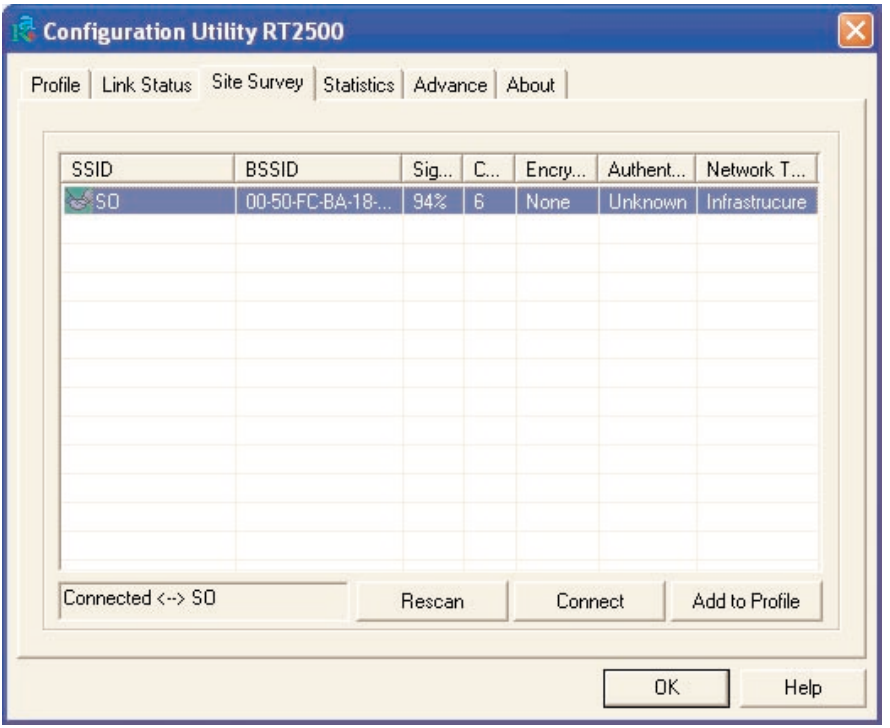


Figure 4-2. Configuration Utility, Site Survey tab.

Table 4-1. Site survey parameters.

Parameter	Description
Available Networks	This list shows all available wireless networks within range of your card. It also displays network information, including the SSID, BSSID, Signal Strength, Channel, Encryption, Authentication, and Network Type. If you want to connect to any networks on the list, double-click the item on the list. The card will automatically connect to the selected network.
Rescan Button	Click on this button to collect the information for all the wireless networks nearby.

Table 4-1 (continued). Site survey parameters.

Parameter	Description
Connect Button	Click on this button to connect to the selected network.
Add to Profile Button	Add the selected network to the Profiles List.
OK	Click on this button to save your changes.

4.2 Profile

The Profiles List enables you to manage the networks that you connect to frequently. You can Add/Delete/Edit/Activate a profile. See Figures 4-3 through 4-5 and Tables 4-2 through 4-4.

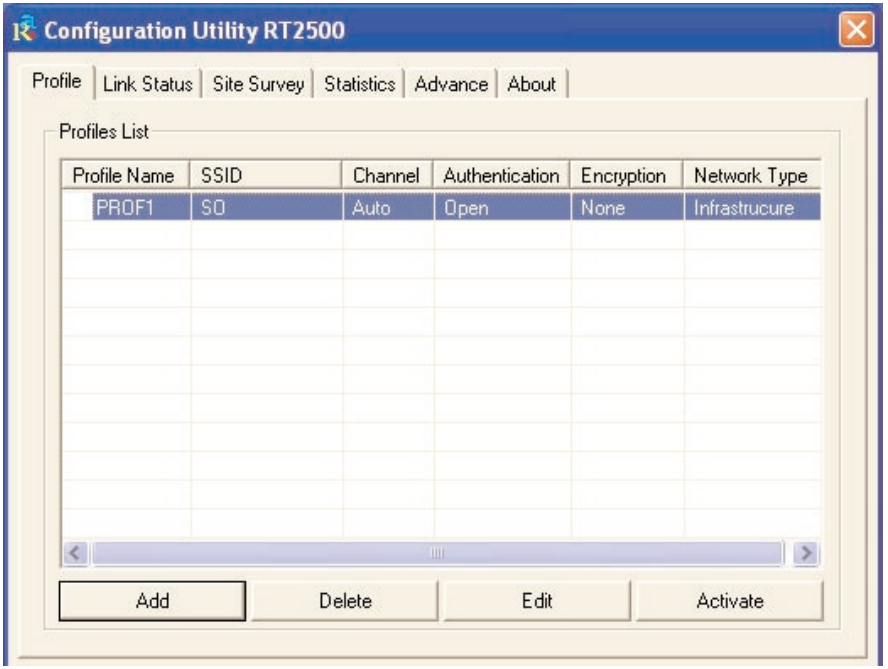


Figure 4-3. Profile tab.

Table 4-2. Profiles List parameters.

Parameter	Description
Profiles List	The Profiles List displays all the profiles and the relative information, including Profile Name, SSID, Channel, etc.
Add/Delete/Edit Button	Click on these buttons to add/delete/edit the selected profiles.
Activate Button	Click on this button to connect to the selected profile.

4.2.1 Configure the Profile

To add a profile, select the **Profile** tab from the Configuration Utility screen (see Figure 4-3) and click on the **Add** button. The Add Profile screen, System Configuration tab appears (see Figure 4-4). In this screen, enter the parameters described in Table 4-3.

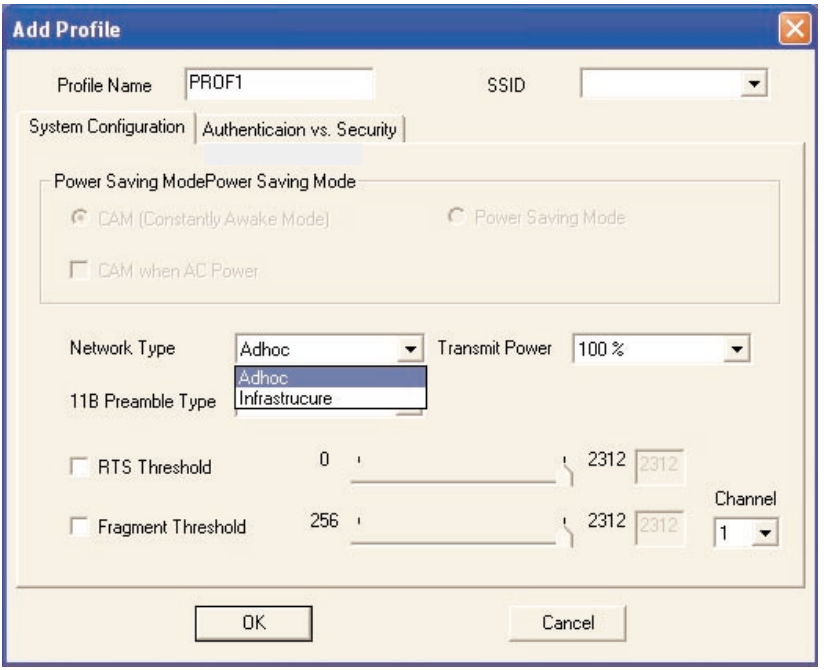


Figure 4-4. Add Profile screen, System Configuration tab.

Table 4-3. System Configuration parameters.

Parameter	Description
Profile Name	Define a recognizable profile name for identifying the different networks.
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the card; then, only the device with the same SSID can interconnect to the card. If you want to add one of the nearby networks to the profile list, pull down the menu. All the networks nearby will be listed and you can add one of them to the profile list.
Power Saving Mode	The power saving function is only available when the network type is in Infrastructure. CAM (Constantly Awake Mode)—The card will always be set in active mode. Power Saving Mode—Enable the card in the power saving mode when it is idle. CAM when AC Power—Select this option to automatically switch the card from power saving mode to CAM while your laptop computer's power is supplied by the AC power but not the battery.
Network Type	Infrastructure—This operation mode requires the presence of an 802.11 access point device. All communication is done via the access point or router.

Table 4-3 (continued). System Configuration parameters.

Parameter	Description
Network Type (continued)	Ad-hoc—Select this mode if you want to connect to another wireless station in the Wireless LAN network without an access point or router.
Transmit Power	To lower the card's transmit power to save system power, select the lower percentages from the list.
11B Preamble Type	The preamble defines the length of the CRC block for communication among wireless stations. This option is only active in the ad-hoc network. There are two modes including auto and long preamble. If auto mode is selected, the card will auto switch the preamble mode for the access point that you are connecting to.
RTS Threshold	This is the minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2312 bytes. We recommend changing the size in small increments.
Fragment Threshold	The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2312 bytes. We recommend changing the size in small increments.
Channel	This setting is only available for ad-hoc mode. Select the number of the radio channel used for the networking. The channel setting should be the same as the network you are connecting to.

Table 4-3 (continued). System Configuration parameters.

Parameter	Description
OK	Click on this button to save your changes.

Once you click on **OK** to save your changes, the screen refreshes, but this time the Authentication vs. Security tab is highlighted (see Figure 4-5). In this screen, enter the parameters' information described in Table 4-4.

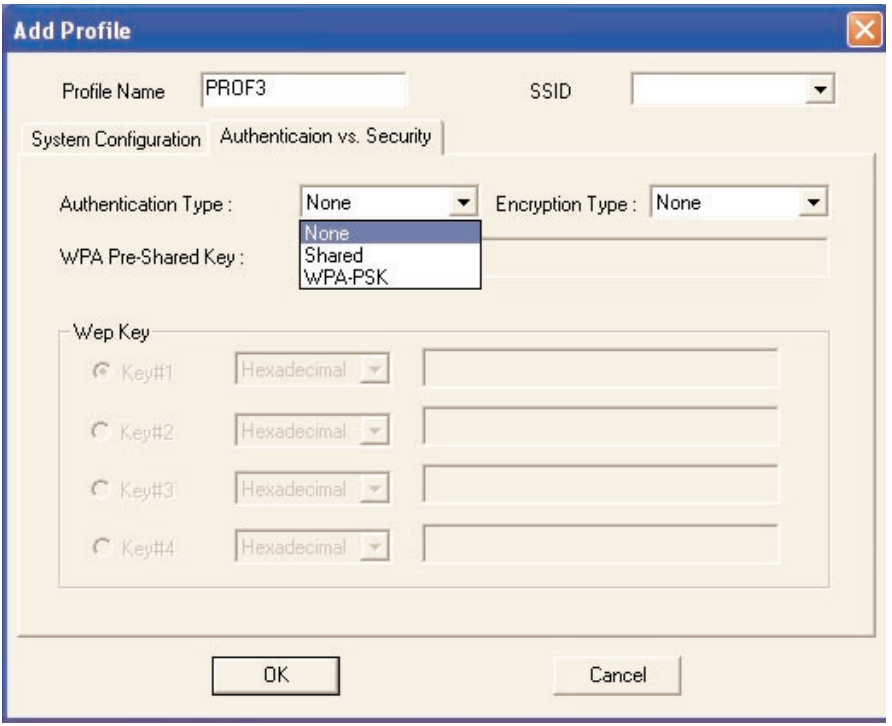


Figure 4-5. Add Profile screen, Authentication vs. Security tab.

Table 4-4. Authentication vs. Security parameters.

Parameter	Description
Authentication Type	This setting has to be consistent with the wireless networks that the card intends to connect to. None—No authentication is needed among the wireless networks. Shared—Only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other. WPA-PSK—This is a special mode designed for home and small-business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, manually enter the starting password in the access point or gateway, as well as in each wireless station in the network. WPA takes over automatically from that point, keeping unauthorized users that don't have a matching password from joining the network while encrypting the data traveling between authorized devices. The encryption methods include TKIP and AES. This option is only available for Windows XP.
Encryption Type	None—Disable the WEP Data Encryption. WEP—Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys. TKIP—TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a message transmitted over a network.) This ensures much greater security than the standard WEP security.

NOTE

All devices in the network should use the same encryption method to ensure proper communication.

Table 4-4 (continued). Authentication vs. Security parameters.

Parameter	Description
Encryption Type (continued)	AES—AES has been developed to ensure the highest degree of security and authenticity for digital information. It is the most advanced solution defined by IEEE 802.11i for security in a wireless network.
WPA Pre-Shared Key	The WPA-PSK key can be from eight to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.
WEP Key (Key 1–Key 4)	The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit and 128-bit. Select the default encryption key from Key 1 to Key 4 by clicking on the appropriate circular button in Figure 4-5. Type the text for either 64-bit or 128-bit operation in the blank box next to the circular button that corresponds to the key you selected (Key 1–Key 4), keeping in mind the points listed below. 64-bit—Type in 10-digit Hex values (in the A–F, a–f, and 0–9 range) or 5-digit ASCII characters (including a–z and 0–9) as the encryption keys. For example, “0123456aef” or “test1”. 128-bit—Type in 26-digit Hex values (in the A–F, a–f, and 0–9 range) or 13-digit ASCII characters (including a–z and 0–9) as the encryption keys. For example, “01234567890123456789abcdef“ or “administrator”.
OK Button	Click on this button to save your changes.

4.2.2 Enable WPA in Windows XP

In the Profiles screen (see Figure 4-5), there's an option for WPA Pre-Shared Key (described in Table 4-4). When you're using Windows XP, you can enable this option. Here's what it does: Wi-Fi Protected Access (WPA) is a standards-based, interoperable specification for security enhancement that strongly increases the level of data protection (encryption) and access control (authentication) for existing and future wireless LAN systems. The technical components of WPA include Temporal Key Integrity Protocol (TKIP) for dynamic key exchange, and 802.1x for authentication.

There are two types of WPA security: WPA-PSK (no server) and WPA (with server). WPA requires a radius server to complete the authentication among wireless stations and access points. Typically, this mode is used in a enterprise environment. WPA-PSK uses a so-called pre-shared key as the security key. A pre-shared key is a password that each wireless station uses to access the network. Typically, this mode will be used in a home environment.

To enable the WPA function in Windows XP, the following software systems are required: Windows XP Service Pack 1 with Windows XP Support Patch for Wi-Fi Protected Access program. Follow the steps below to use WPA.

1. Configure the card by the wireless built-in utility (Wireless Zero Configuration). See Figures 4-6 and 4-7.

NOTE

When WPA is enabled, there are two utility selections (either RaConfig or Wireless Zero Configuration) when you open the card's Configuration Utility (see Figure 4-6). Select the XP built-in utility with full WPA function. If you select XP Wireless Zero Configuration, you can only configure the Advance setting or check the Link Status and Statistics from the RaConfig utility. From Figure 4-6, click on OK to save your selection.

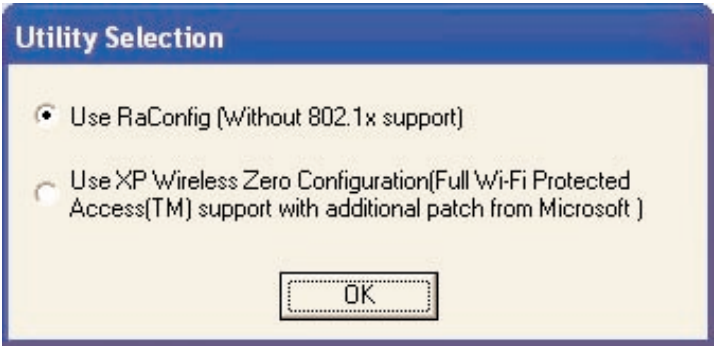


Figure 4-6. Selecting the utility.

2. Once you click on **OK**, the Wireless Network Connection screen appears (see Figure 4-7). From here, select the appropriate wireless network from the scroll-down menu.

3. Click on the **Advanced** button from the screen shown in Figure 4-7.

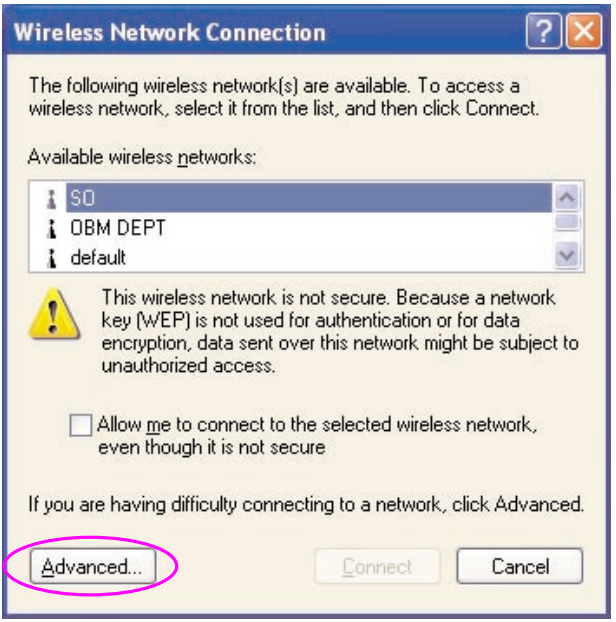


Figure 4-7. Selecting the wireless network.

4. The screen refreshes with the Wireless Networks tab highlighted (see Figure 4-8). In this screen, click on the **Configure** button to configure the WPA function for the current network.

NOTE

Uncheck "Use Windows to configure my wireless network settings," and the RaConfig utility will be enabled again.

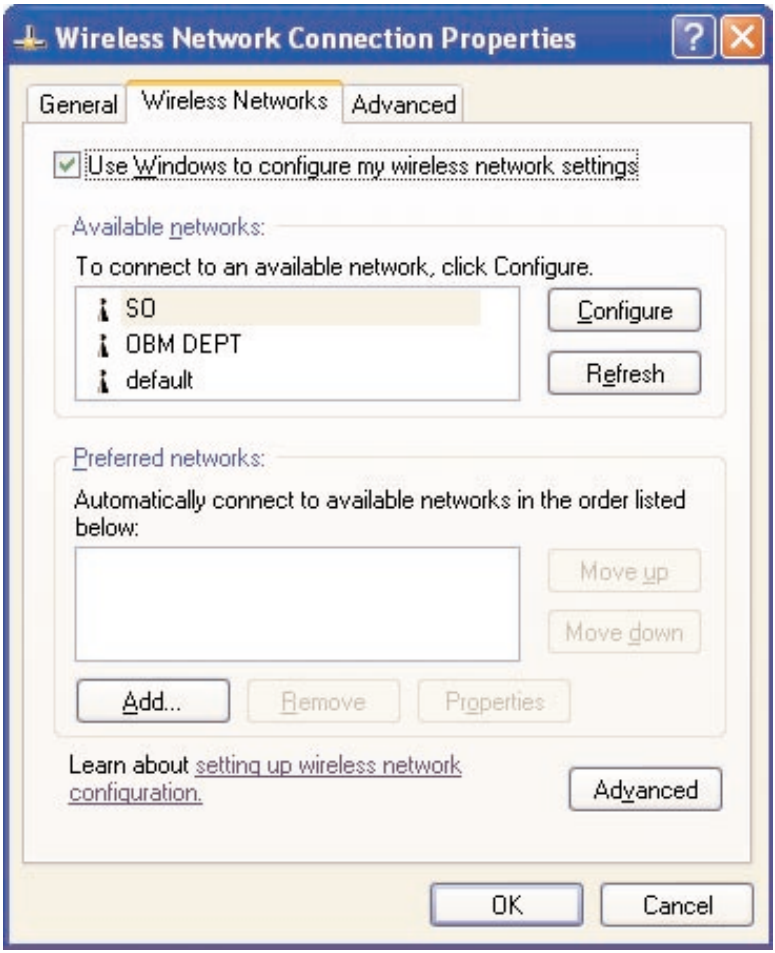


Figure 4-8. Wireless Networks tab.

5. Configure the network key. See Figure 4-9 and Table 4-5.

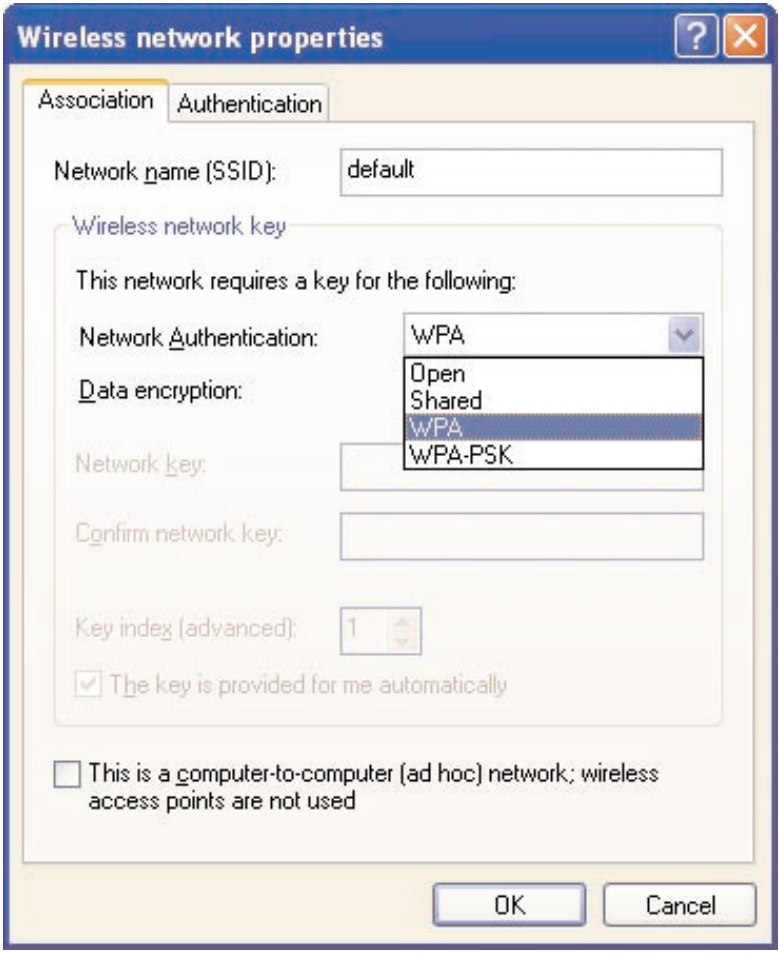


Figure 4-9. Association tab.

Table 4-5. Association parameters.

Parameter	Description
Network name (SSID)	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs.
Network Authentication	Open—No authentication is needed among the wireless networks. Shared—Only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other. WPA—This mode is for an enterprise network with an authentication server (radius server), WPA-enabled access point, and a WPA-enabled client. Once WPA is enabled, all clients and access points on the network must be WPA-enabled in order to access the network. WPA-PSK—This is a special mode designed for home and small-business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, manually enter the starting password in the access point or gateway, as well as in each PC on the wireless network. WPA takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

NOTE

All devices in the network should use the same encryption method to ensure the communication.

Table 4-5 (continued). Association parameters.

Parameter	Description
Data Encryption	WEP—In WPA or WPA-PSK mode, WEP is also able to be the encryption method for the transmission data. TKIP—TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a message transmitted over a network.) This ensures much greater security than the standard WEP security. AES—AES ensures the highest degree of security and authenticity for digital information. It is the most advanced solution defined by IEEE 802.11i for security in the wireless network.
Network Key	Type in an alphanumeric key. This will identify your network.
Confirm Network Key	Re-type the alphanumeric key you entered in the Network Key field to confirm it.
Key Index	Select a key index number from the drop-down menu, or check the box labeled “The key is provided for me automatically.”
Ad-Hoc Checkbox	Click on this checkbox if you have a computer-to-computer network (no access points).
OK button	Click on this button to save your changes.

6. Click on **OK** to save your changes.

4.3 Link Status

From the Link Status tab, you can view all the information of the network you are connecting to. See Figure 4-10 and Table 4-6.

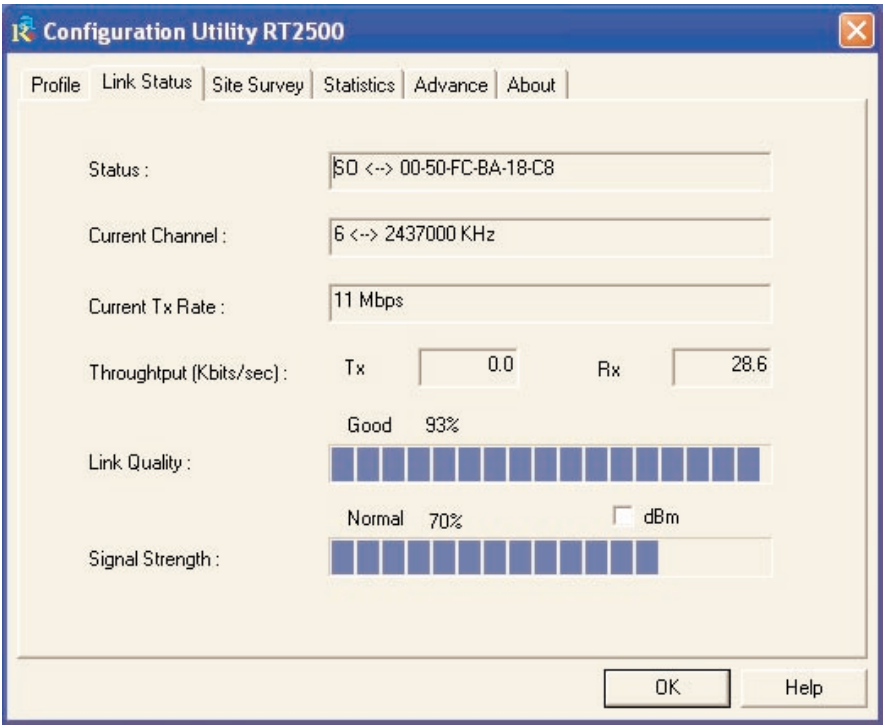


Figure 4-10. Link Status tab.

Table 4-6. Link Status parameters.

Parameter	Description
Status	Display the SSID and MAC ID of the network the card is connecting to.
Current Channel	Display the number of the radio channel and the frequency used for networking.
Current Tx Rate	Display the transmission rate of the network. The maximum transmission rate is 54 Mbps.
Throughput (kbits/sec)	Display the speed of data transmitted and received.
Link Quality	This bar indicates the quality of the link. The higher the percentage, the better the quality.
dBm	If you want to know the signal strength in dBm, select this check box.
Signal Strength	This bar shows the signal strength level. The higher percentage shown in the bar, the more radio signal has been received by the card. This indicator helps find the proper position of the wireless device for quality network operation.
OK button	Click on this button to exit the screen.

4.4 Statistics

This tab enables you to view the available statistic information with its Tx counts (Tx success, Tx error, RTS success and RTS failed) and Rx counts (Rx success, Rx error). To reset the counters, click on **Reset Counter**. See Figure 4-11. Click on **OK** to save the change.

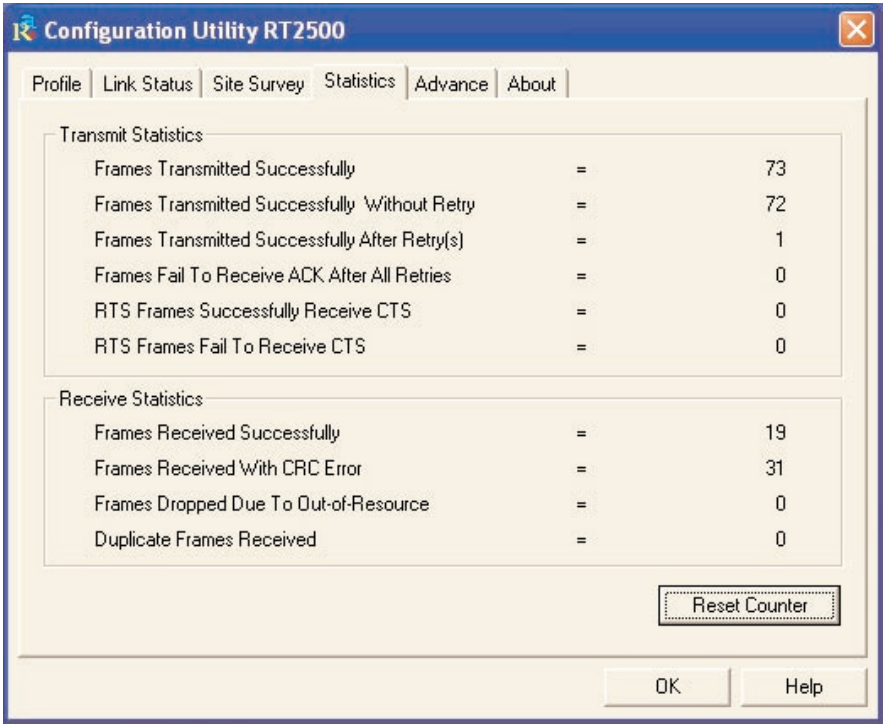


Figure 4-11. Statistics tab.

4.5 Advance

This option enables you to configure more advanced settings, such as wireless mode, protection mode, etc. See Figure 4-12 and Table 4-7.

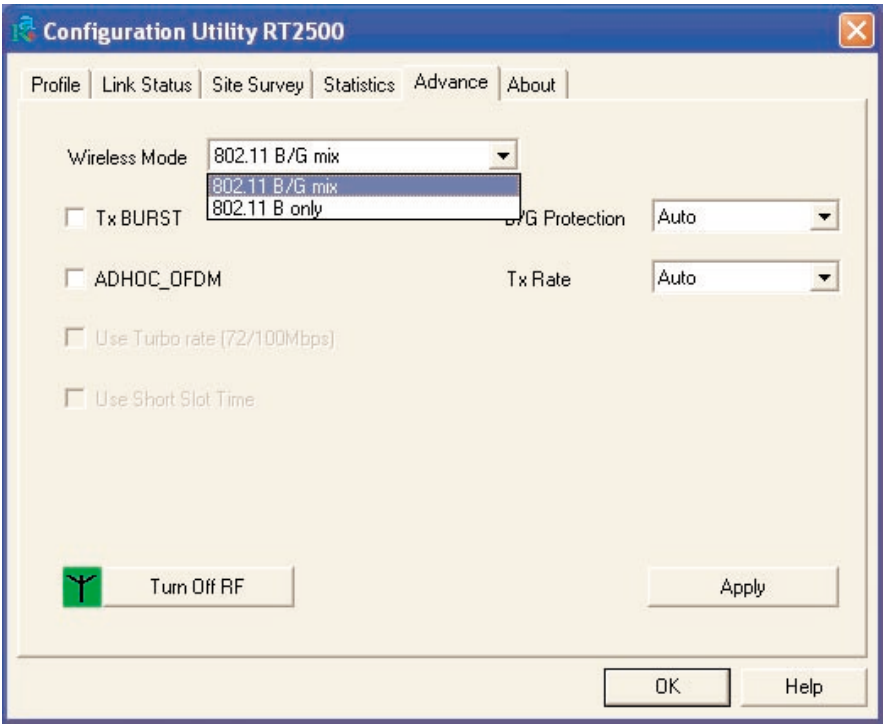


Figure 4-12. Advance tab.

Table 4-7. Advance parameters.

Parameter	Description
Wireless Mode	802.11 B/G mix—If you have a mix of 802.11b and 802.11g wireless stations in your network, we recommend that you set the card to this mode. This mode is also the default setting. 802.11 B only—This card can be compatible with both 802.11g and 802.11b wireless stations. If there are only 802.11b wireless stations in the network, set the card to this mode.
Tx BURST	Tx Burst enables the card to deliver better throughput in the same period and environment.
B/G Protection	If you have a mix of 802.11b and 802.11g wireless stations in the network, enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the card's throughput will be a little lower since many of the frame traffic is transmitted. Auto—Based on the network's status, automatically disables/enables protection mode. On—Always enables the protection mode. Off—Always disables the protection mode.
ADHOC_OFDM	When the network type is in ad-hoc mode, the card can only work in the 11b data rate. It is defined by the Wi-Fi organization. If you want to enable the data rate up to 54 Mbps (11g), select ADHOC_OFDM.

Table 4-7 (continued). Advance parameters.

Parameter	Description
Tx Rate	There are several options including Auto, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps. When auto is selected, the device will choose the most suitable transmission rate automatically. The higher the data rate you designate in the network, the shorter the distance allowed between the card and the wireless stations. When the wireless mode is 802.11 B only, the maximum data rate is 11 Mbps (11b). Auto, 1, 2, 5.5, and 11 Mbps are the available options.
Turn Off RF Button	If you want to turn off the card's radio frequency temporarily, click this button. To turn on the radio frequency, click this button again.
Use Turbo rate (72/100 Mbps)	Select this option when your network is configured as 802.11g.
Use Short Slot Time	Select this option when your network is configured as 802.11b.
Apply button	Click on this button to apply the current settings.
OK button	Click on this button to save your changes.

4.6 About

By choosing this tab, you can click the hyperlink to connect the Web site for the wireless chipset vendor's information and review basic information about the utility such as the driver, utility, and EEPROM version. The MAC address of the card is displayed on the screen as well. See Figure 4-13. Click on **OK** to exit the screen.

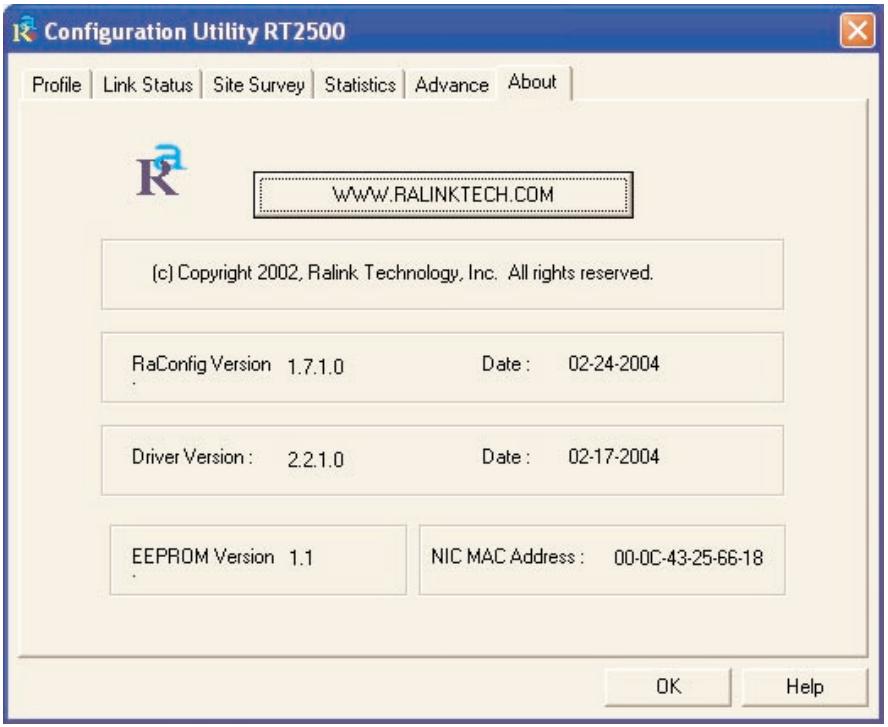


Figure 4-13. About tab.

5. Troubleshooting

5.1 Frequently Asked Questions

1. What is the IEEE 802.11g standard?

   802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office, and public networks.

   802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

   A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12, and 24 Mbps (mandatory speeds), and 18, 36, 48, and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

   B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. What is the IEEE 802.11b standard?

   The IEEE 802.11b Wireless LAN standard subcommittee formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufacturers to communicate.

3. What does the IEEE 802.11 feature support?

   The product supports the following IEEE 802.11 functions:

   • CSMA/CA plus Acknowledge Protocol

   • Multi-Channel Roaming

   • Automatic Rate Selection

   • RTS/CTS Feature

- Fragmentation
- Power Management

4. What is Ad-hoc?

   An ad-hoc integrated wireless LAN is a group of computers linked to each other *without* using an access point; each has a Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter connected as an independent wireless LAN. You'd typically use an ad-hoc wireless LAN for a branch or SOHO operation.

5. What is infrastructure?

   When you connect a wireless LAN and a combination (wireless and wired) LAN together, it's called an infrastructure configuration. Infrastructure is applicable on an enterprise scale for wireless access to a central database, or for a wireless application for mobile workers.

6. What is BSS ID?

   A specific ad-hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP?

   WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared key algorithm, as described in the IEEE 802.11 standard.

8. What is TKIP?

   TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard.

9. What is AES?

   AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in the IEEE 802.11i standard. Compared with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can wireless products support printer sharing?

    Wireless products perform the same function as LAN products. Therefore, wireless products can work with NetWare®, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air?

    WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security scrambling feature. On the software side, the WLAN series offer the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs.

12. What is DSSS? What is FHSS? And what are their differences?

    Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct Sequence Spread Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum?

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

5.2 Calling Black Box

If you determine that your Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

5.3 Shipping and Packaging

If you need to transport or ship your Pure Networking 802.11g Wireless Cardbus (PCMCIA) Adapter:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the adapter for repair, make sure you include everything that came in the original package. Before you ship, contact Black Box to get a Return Authorization (RA) number.