Wireless LAN PCI Card

EW-7126

User Manual

Version: 1.0
(Mar., 2002)

COPYRIGHT

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 FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.

2. Increase the separation between the equipment and receiver.

3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1 Introduction

Thank you for purchasing the Wireless LAN PCI Card. This card features the latest innovation wireless technology. IEEE 802.1x which request wireless stations to pass the authorization by entering a unique user name and password designated by the authorization server before connecting to the wireless devices such as Access Point or Router. TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) which are advanced WLAN security technology included in the IEEE 802.11i standard. Furhtermore, this card provides several kinds of power saving modes allowing user customizes the way of saving the power from his/her portable or handheld devices. This card is cost-effective, together with the versatile features, it is the best solution for you to builde your wirless network.

1.1   Features

- Complies with the IEEE 802.11b 2.4GHz (DSSS) standard.
- High data transfer rate - up to 11Mbps.
- Support 64/128-bit AES/TKIP/WEP Data Encryption function for high level of security.
- Supports IEEE 802.1x advanced WLAN Security.
- Supports peer-to-peer communication among any wireless users, no Access Point is required.
- Detachable antenna with long length cable provides convenience to locate the antenna.
- Automatic fallback increases data security and reliability.
- Supports the most popular operating system: Windows 98SE/Me/2000/XP, WinCE.Net and Linux.

1.2   Specifications

- Standards: IEEE 802.11b
- Bus Type: PCI V2.2/2.1
- Frequency Band: 2.4000~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: CCK@11/5.5Mbps, DQPSK@2Mbps, DBPSK@1Mbps
- Radio Technology: Direct Sequence Spread Spectrum (DSSS)
- Data Rate: 11/5.5/2/1Mbps auto fallback
- Security: 64/128-bit AES/TKIP/WEP Data Encryption, IEEE 802.1x
- Antenna: External detachable dipole antenna with coaxial cable
      (Part No.: W111-094-D200, Cable Length: 94cm)
- Drivers: Windows 98SE/Me/2000/XP and Linux
- LEDs: TX/RX, Link
- Transmit Power: 16dBm~18dBm
- Dimension: 19(H) x 135(W) x 121(D) mm
- Temperature: 32~131°F (0 ~55°C)
- Humidity: 5-95% (NonCondensing)
- Certification: FCC, CE, WHQL

1.3   Package Contents

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

- One PCI Card
- One Antenna
- One Quick Guide
- One CD (Driver/Utility/Manual)

If any of the above items is missing, contact your supplier as soon as possible.

2 Installation Procedure

2.1 Windows 98SE/Me/2000

Before you proceed with the installation, please notice following descriptions.

Note1: The following installation was operated under Windows 2000. (Procedures will be the same for Windows 98SE/Me.)

Note2: If you have installed the Wireless PCI Card driver & utility before, please uninstall the old version first.

2.1.1 Install the Driver

1. Turn off your PC.

2. Insert the card into the PCI slot of your PC, the system will automatically find the device and search for its driver.

3. Please select the "Driver\Win2000" folder (select the folder based on your PC's OS system) and the system will complete the driver installation.

2.1.2 Install the Utility

1. Insert the CD into the CD-ROM device and execute the "Utility\setup.exe" program. The InstallShield Wizard box will appear, click "Next" to continue.

2. Follow the instruction of the installation program. The program will install the software for this device directly.
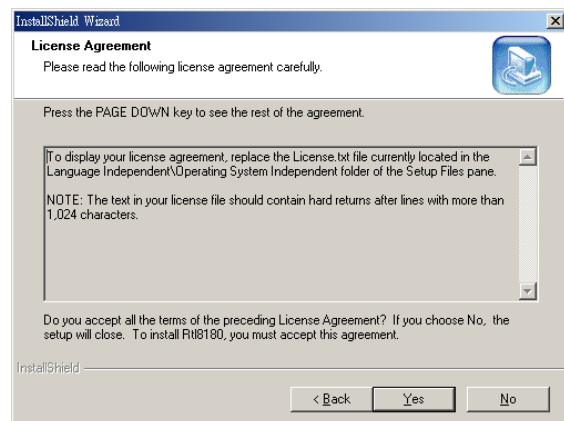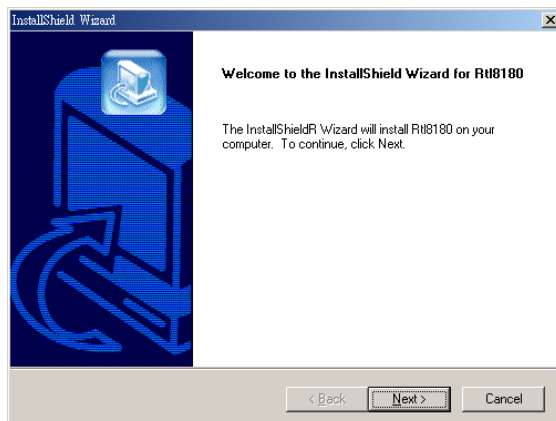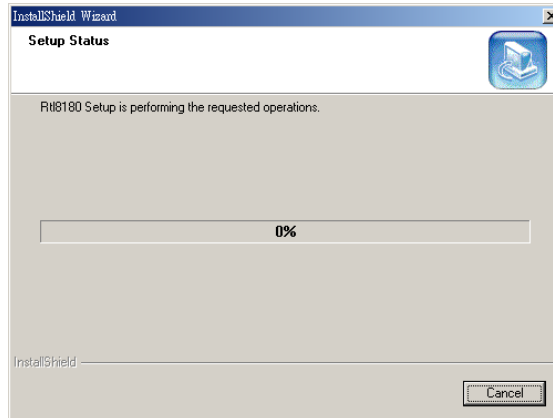
3. Click "Finish" to complete the installation.

4. When you complete the Utility installation, a shortcut named "Rtl8180" will appear in the computer's desktop and a new icon will be displayed in th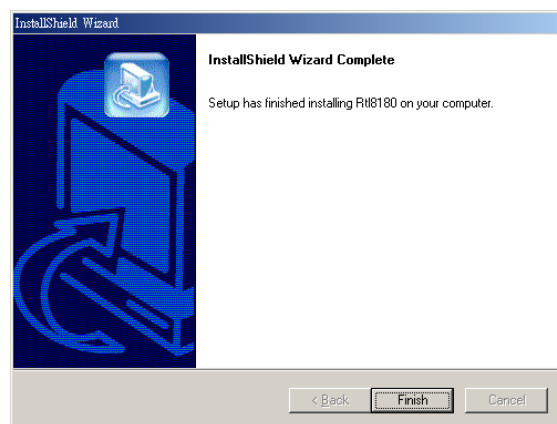e system tray at the bottom of the screen. Double click the shortcut or click the icon and start using the WLAN PCI Card.
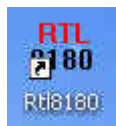
In the Desktop   *In the taskbar*

2.2   Windows XP

The installation process in Windows XP is similar with the process in Windows 98SE/Me/2000. Please refer to the instructions described in section 2.1.

Due to the Windows XP has built-in wireless network utility you may decide to use the system's utility or the one provided by this card. **It is strongly recommended to using the utility of this card**.

A. Using the Windows XP's Utility

Click the icon marked in red in the system tray and you may start using the Windows XP's wireless utility
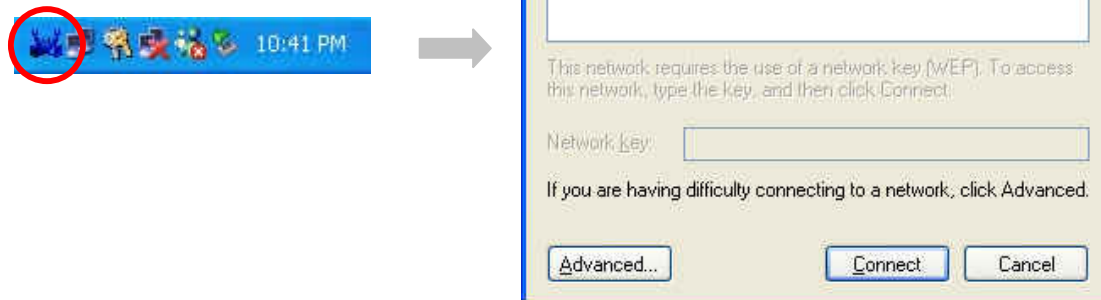
B. Using the Utility of this card
1. Get into Windows XP's Utility, click "Advanced" button.
2. In "Wireless Network Connection Properties" screen, uncheck the setting "Use Windows to configure my wireless network settings". Note that if you want to change back to the Windows XP built-in utility, check the item again.
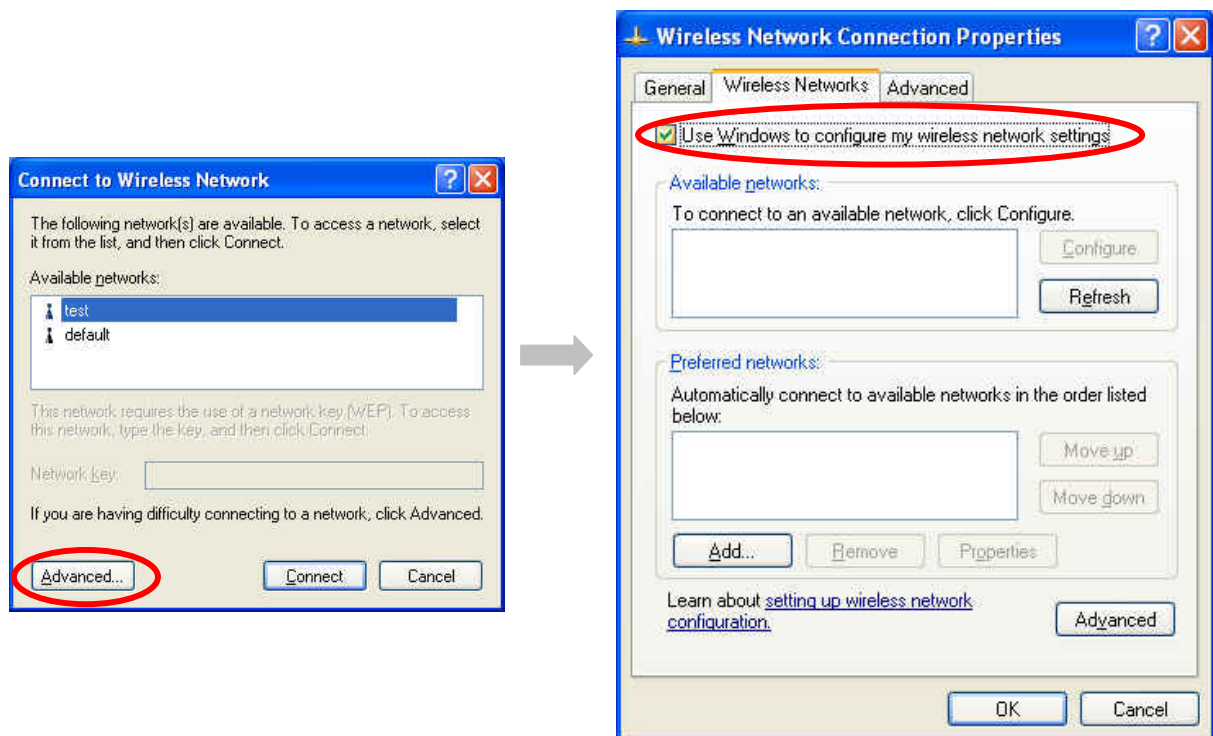
3. Double click the shortcut or click the icon and start using the WLAN PCI Card.
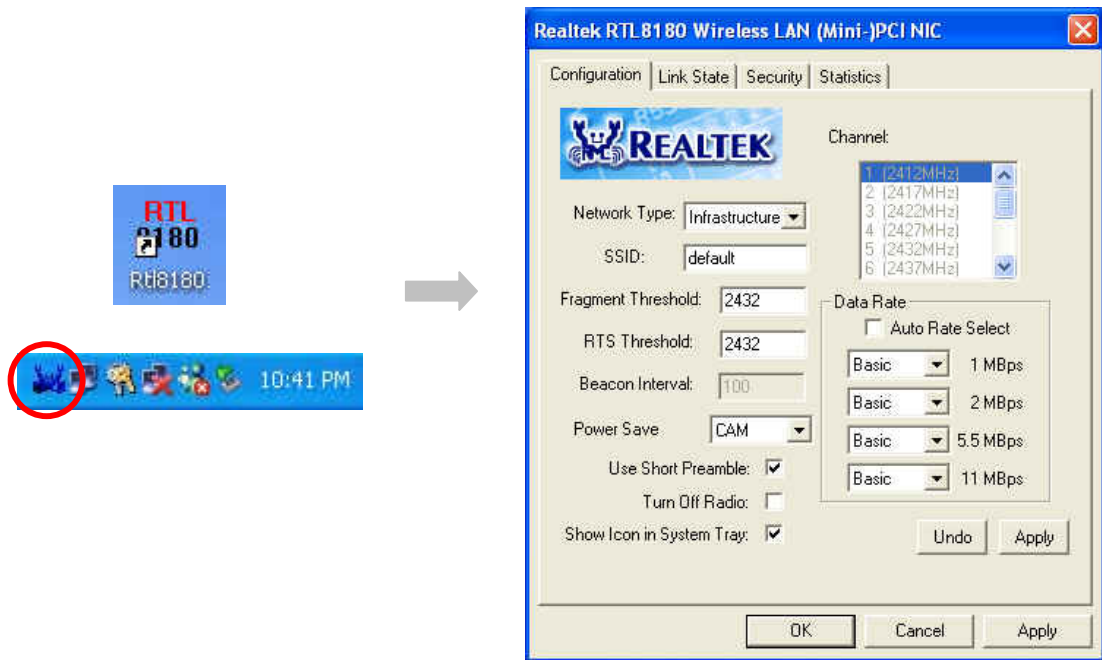
Note: If you don't disable the XP's Utility, you can still see the link status and statistics during communication process from the card's utility.

6
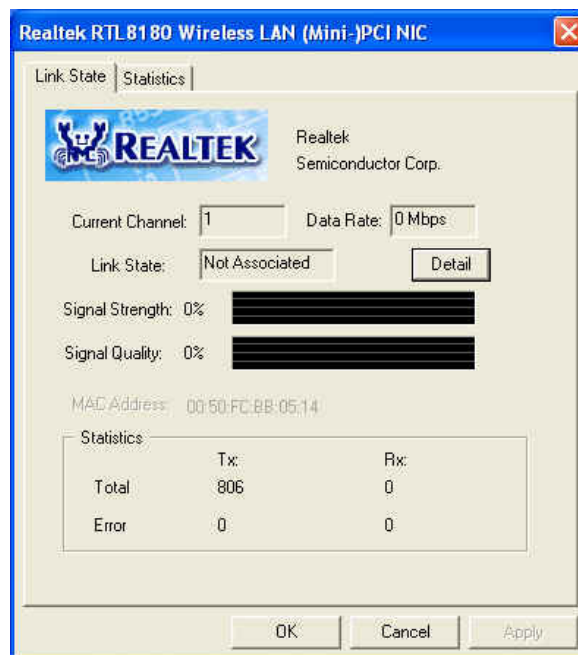
3 Configuration Utility

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

This utility can be used to change the following configuration parameters when the device is active.

3.1 Configuration

In the **"*Configuration*"**, you may set up the necessary parameters about the wireless LAN.

Parameter	Description
Network Type	• **Infrastructure –** This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point. • **Ad-Hoc –** Select this mode if you want to connect to another wireless stations in the Wireless LAN network without through a Access Point.
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 and then only the device with the same SSID can interconnect to the card.

Parameter	Description
Fragement 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 2432 bytes. Minor change is recommended.
RTS Threshold	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 WLAN. Select a setting within a range of 0 to 2432 bytes. Minor change is recommended
Beacon Interval	This value specifies the duration between beacon packets (milliseconds). The beacon packets include the card's information and are broadcasted to the WLAN network periodly. The beacon period is fixed in 100ms.
Power Save Mode	**CAM(Continuous Access Mode) –** This card will always set in active mode. **Max –** Enable the card in the power saving mode when it is idle. **Fast –** Enable the card in the power saving mode when it is idle, but some compoents of the card is still alive. In this mode, the power consumption is larger than "Max" mode.
Use Short Preamble	The preamble defines the length of the CRC block for communication between the Access Point and the card. High network traffic areas should use the shorter preamble type.
Turn Off Radio	When the setting is checked, the wireless connection of the card will be disabled.
Show Icon in System Tray	Enable or disable the icon shown in the taskbar.
Channel	Select the number of the radio channel used for the networking. The parameter is not active in the infrastructure operation mode.
Data Rate Auto Rate Select	When it is enabled, the device will choose the most suitable transmission rate automatically.

Parameter	Description
1, 2, 5.5, 11MBps	• **Not Used –** Prohibits the device from operating at the specified data rate. • **Used –** Allows the device operating at the specified data rate • **Basic –** Restrict the device to operate at least at the specified data rate. At least one kind of data rate has to be set "Basic". Click "Apply" button to save the above configurations, click "Undo" button to cancel the settings. *Note: The data rate is auto fallback among the range of the used data rate in case obstacles or interference.*

3.2 Link State

In the *"Link State"*, you can make connection to the wirelss devices and immediately monitor the link status.
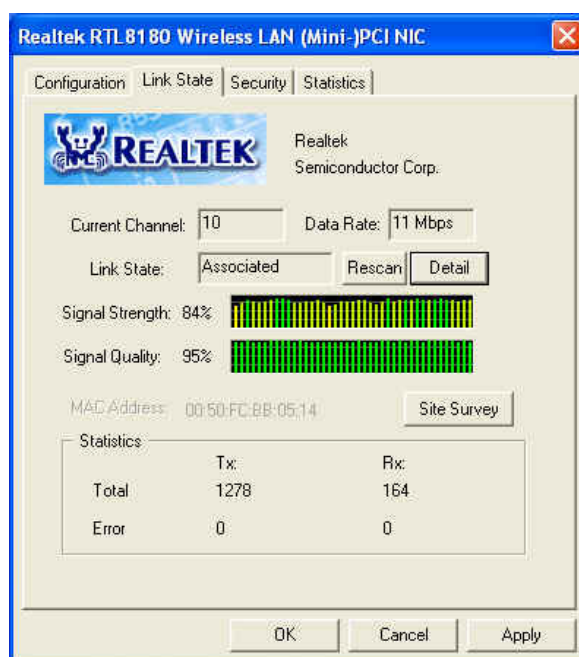

Parameter	Description
Current Channel	Shows the current channel used in the wireless connection
Data Rate	Shows the data rate of the connection.

9

Parameter	Description
Link State	Shows the status of the connection. • **Checking Status –** Represents the card is checking the status of the wireless device. • **Not Associated –** Represents the connection is interrupted. You may press "Rescan" button to reconnect the wireless device. • **Associated –** Represents the card is successfully linking to the wireless device.
Rescan button	Click this button to scan the Access Point or Adapter which the card connected before or intends to connect.
Detail	A screen will appear when you press the button. In this screen, you may see all the parameters of the card and also the link status.
Signal Strength	This bar shows the signal strength level. The higher percentage shown in the bar, the more radio signal been received by the card. This indicator helps to find the proper position of the wireless device for quality network operation.
Signal Quality	This bar indicates the quality of the link. The higher the percentage, the better the quality.
MAC Address	Shows the MAC Address of the card.
Site Survey button	Click this button to survey all APs or Adapters when operating in Ad-Hoc mode nearby.
Statistics	Shows the total amounts of data packets that have been successfully/unsuccessfully transmitted or received by the card.

3.2.1 Site Survey

This screen shows all Access Points, Routers or Adapters nearby when operating in Ad-Hoc mode.

Click "Refresh" button to collect the SSID and Channel information of all the wireless devices nearby. If you want to connect to any device on the list, double-click the item on the list, and the card will automatically connect to the selected device.
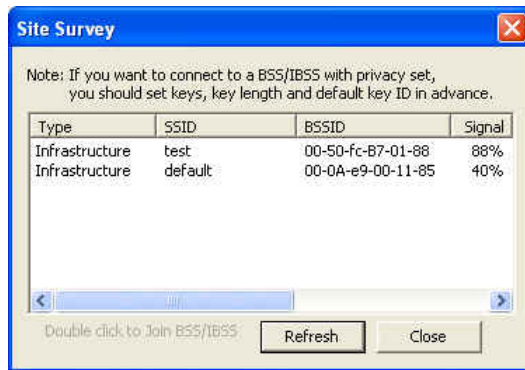
3.3   Security

In the *"Security"*, you can enable or disable the WEP, TKIP and AES WLAN security mechansims for the card.

WEP is an authentication algorithm, which protects authorized Wireless LAN users against eavesdropping. WEP has been found that it has some security problems. TKIP is a temporary quick-fix method defined in IEEE 802.11i standard to quickly overcome the inherent weaknesses in WEP security. AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.

The security setting must be the the same on the wireless devices within the network. This card supports 64/128-bit WEP, TKIP and AES encryption functions.

Parameter	Description
Data Encryption	• **No Encryption –** Disable the WEP Data Encryption. • **WEP –** Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Key Length and the encryption keys. • **Realtek TKIP –** Enable the TKIP Data Encryption. When the item is selected, you have to continue setting the TKIP Key Length and the encryption keys. • **Realtek AES –** Enable the AES Data Encryption. When the item is selected, you have to continue setting the AES Key Length and the encryption keys.
Auth Algorithm	This setting has to be consistent with the wireless devices which the card intends to connect. • **Open System –** No authentication is needed among the wireless devices. • **Shared Key –** Only wirelss devices using a shared key (WEP Key, TKIP Key or AES Key identified) are allowed to connecting each other. Setup the same key as the wireless devices which the card intends to connect. • **Auto Switch –** Auto switch the authentication algorithm depending on the wireless devices which the card is connecting to.
Default Key ID	Select one of the keys (1~4) as the encryption key.

Parameter	Description
Key Length	You may select the 64-bit or 128-bit to encrypt transmitted data. Larger key length will provide higher level of security, but the throughput will be lower.
Key1 ~ Key4	The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. • **64-bit** – Input 10 digit Hex values (in the "A-F", "a-f" and "0-9" range) as the encryption keys. For example: "0123456aef". • **128-bit** – Input 26 digit Hex values (in the "A-F", "a-f" and "0-9" range) as the encryption keys. For example: "01234567890123456789abcdef".

3.4　Statistics

In the *"Statistics"*, you can get the real time information about the packet transmission and receiving status.
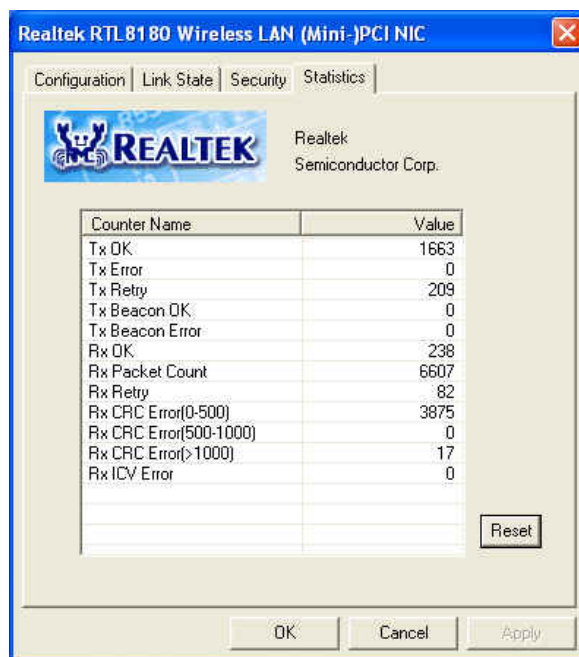
4 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the card.

1. **What is the IEEE 802.11b standard** ？
    The IEEE 802.11b Wireless LAN standard subcommittee which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

2. **What does 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

3. **What is Ad-hoc** ？
    An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

4. **What is Infrastructure** ？
    An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

5. **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.

6. **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.

7. **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, and the specification might be officially released by early 2003.

8. **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 IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

9. **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.

10. **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 feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

11. **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 is, 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.

12. **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).