Wireless 802.11b/g PCI Adapter

EW-7326Ig

User's Manual

Version: 1.0(July, 2008)

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

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 Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

R&TTE Compliance Statement
This equipment complies with all the requirements of DIRECTIVE 1999/5/EC 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, Bulgaria, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia, 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

Please check the declaration of conformity on www.edimax.com

CONTENTS

1. Product Introduction

Thank you for your purchasing Edimax Wireless 802.11b/g PCI Adapter. This PCI adapter is designed to comply with IEEE 802.11b/g Wireless LAN standard and easy to carry with the Mini size. It is suitable for any Desktop computers.

This adapter supports higher data throughput than the IEEE 802.11b/g standard (up to 54Mbps). It supports specific ways to increase the data transfer rate at a time; compress the data and decrease the waiting time to send the next data to the Routers or Access Points. When the adapter is connecting to the Routers or Access Points with the proprietary feature, the wireless network will be more effective.

The power consumption of the Adapter is very low. Furthermore, it also provides several levels of power saving modes allowing user customizes the way of saving the power from his/her portable or handheld devices. It is cost-effective, together with the versatile features; it is the best solution for you to build your wireless network.

1.1. Features
- Complies with IEEE 802.11b/g Standards.
- Supports data transfer rate up to 54Mbps.
- Supports high throughput for multi-media data bandwidth requirement.
- Support 64/128-bit WEP, WPA & WPA2 Encryption.
- Provides 2dBi detachable antenna
- Supports 32-bit PCI interface.
- Supports operating system: Windows OS 98SE/Me/2000/XP/Vista, Mac OS 10.3.x/10.4.x & Linux OS

1.2. Specifications
- Standard: IEEE 802.11b/g
- Interface: 32-bit PCI
- Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g) BPSK, QPSK, CCK (11b)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP Data Encryption, WPA/WPA2 (TKIP with IEEE 802.1x) and AES
- Antenna: External detachable dipole antenna (Connector: RP-SMA connector)
- Drivers: Windows 98SE/Me/2000/XP

- LEDs: Link, TX/RX
- Transmit Power: 17dBm±2dBm
- Power Consumption: TX: 340mA, RX: 320mA
- Dimension: 19(H) x 127(W) x 121(D) mm
- Temperature: 32~131°F (0 ~55°C)
- Humidity: Max. 95% (NonCondensing)
- Certification: FCC, CE

2. 2. Package Contents

Before you starting to use this Wireless PCI Adapter, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- One Wireless PCI Adapter
- One 2dBi Antenna
- One Quick Installation Guide
- One CD-ROM (Including Multi-language QIG, User's Manual and Driver/Utility)

3. Hardware Installation

A. Turn off your computer and remove its cover.

B. Insert the PCI card to an available PCI slot firmly.

C. Secure this card to the rear of the computer chassis and put back the cover.

D. Secure the antenna to the antenna connector of the card.

E. Turn on the computer.

4. Software Installation

This wizard can be run in Windows 2000/XP/XP64/2003/Vista. The following procedures are operated in Windows XP. (Procedures are similar for Windows 2000/XP/XP64/Vista.)

Note1: If you have installed the Wireless PCI Card driver & utility before, please uninstall the old version first.

1. Insert the CD shipped along with the product into your CD-ROM drive. The Windows Vista will popup AutoPlay window, Please select "Install or run program" to execute Autorun.exe program. The Autorun.exe program should be executed automatically. If not, run Autorun.exe manually from "Autorun" folder in the CD.

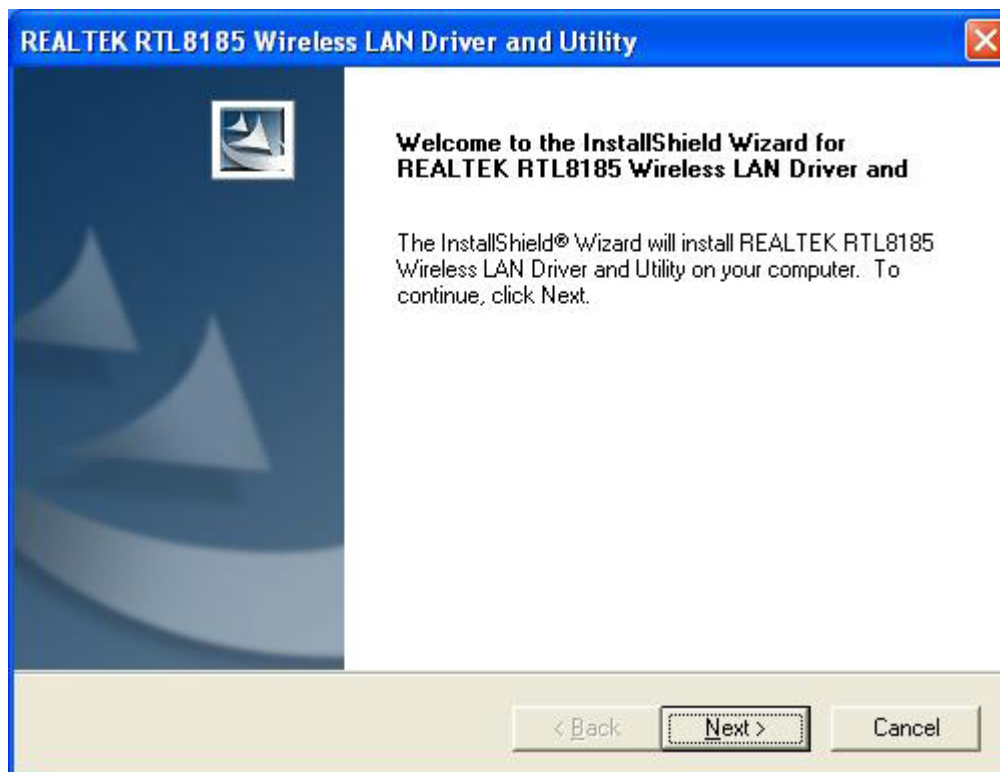2. The follow ing screen will be displayed. Click "Setup Utility" to run the setup wizard.
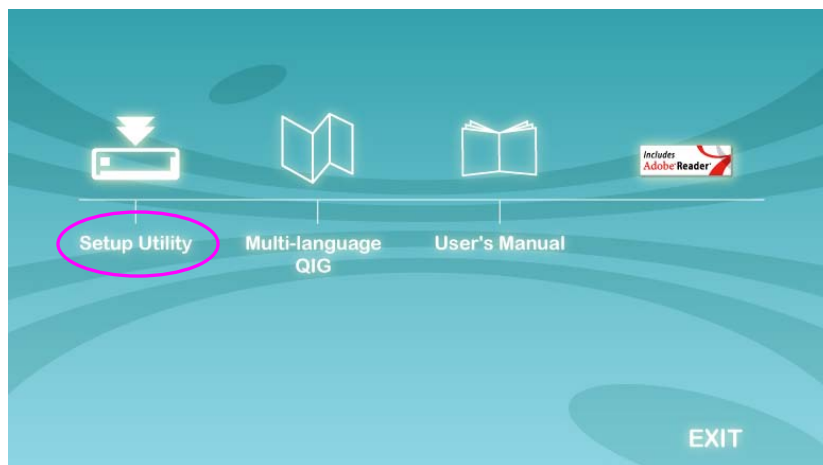
Please select 'Allow' if Windows indicates that 'an unidentified program wants access to your computer'.
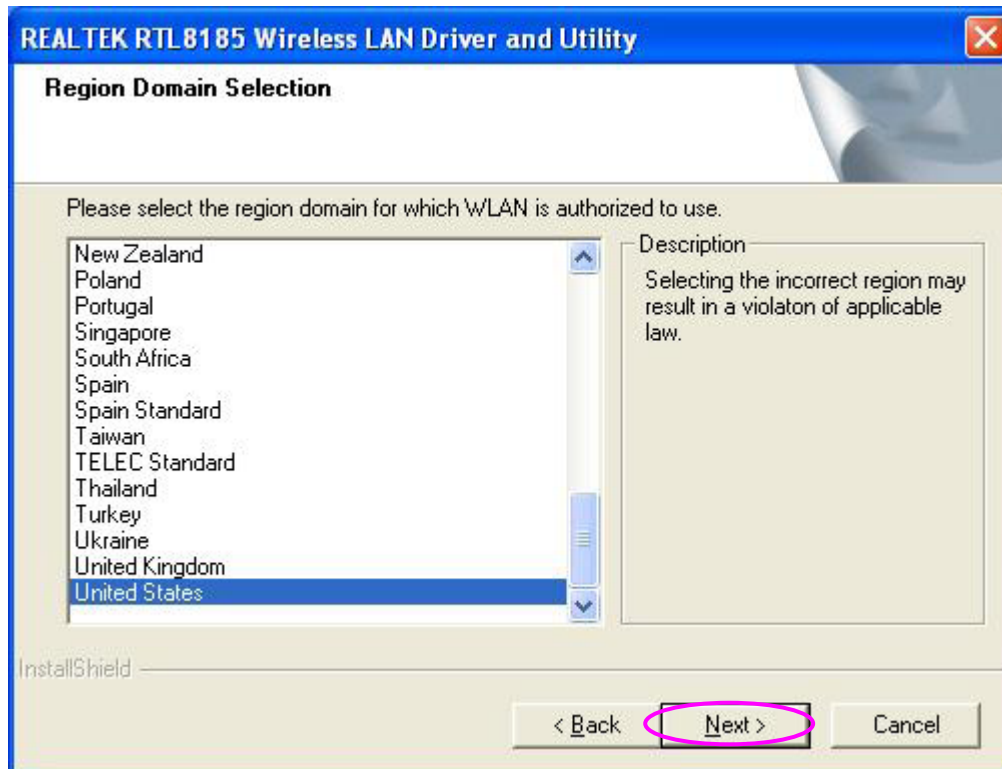
3. Select the Setup Language and click "OK" to proceed.

4. Click "Next" to start installing driver and utility.
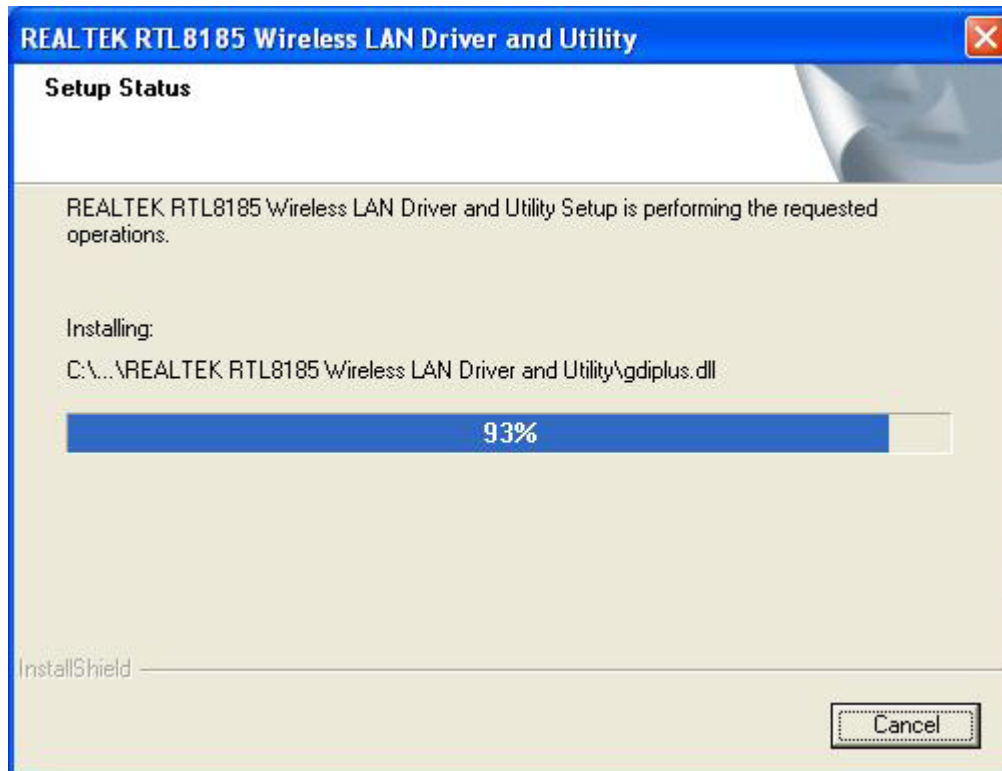
5. Select the Region Domain for which WLAN is authorized to use and click "Next" to continue.

6. Radio regulation warning window. Due to the Radio regulation at different area, different radio law might be applied. Please make sure your region selection is correct.
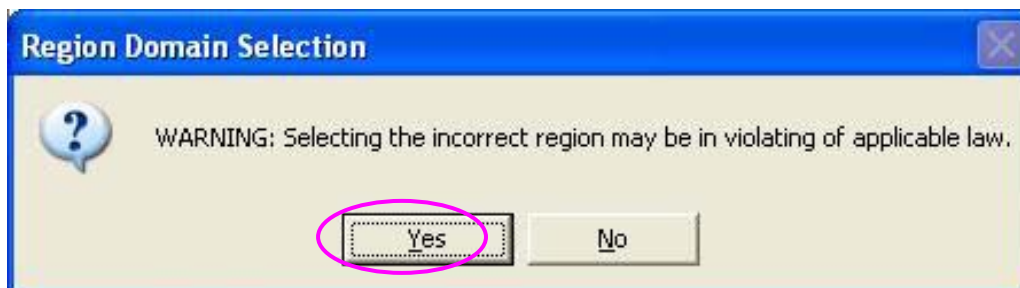
7. The system starts to install the driver and utility.

8. Click "Finish" to complete the driver and utility installation.

5. Connect to Wireless Access Point

Using Configuration Utility to Connect to Wireless Access Point

5.1 Using Realtek Wireless Configuration Utility

1. After installation is complete, wireless configuration utility will be shown an icon at your windows desktop as below. Please click the icon by right mouse key to lunch the configuration utility.
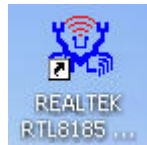
2. Configuration utility will scan for wireless access points automatically, and all found access points will be displayed on "Available Network". Please select an access point you wish to connect, and click 'Add to Profile'. If the wireless access point you want to connect does not show here, please click 'Refresh'
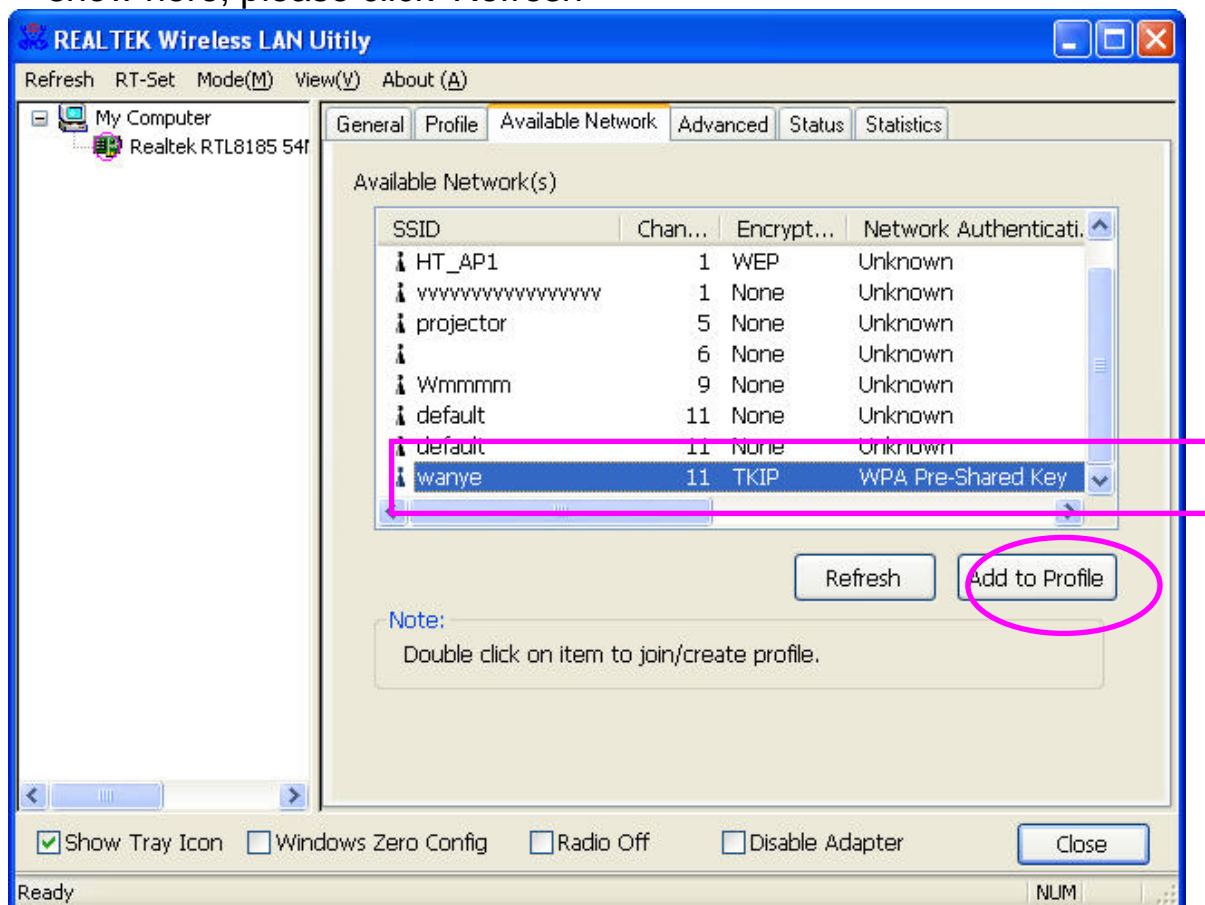
3. If the wireless access point uses encryption, you have to input WEP passphrase or WPA preshared key. Please ask the owner of the wireless access point you want to connect, and input the correct

passphrase / preshared key at "Network key" & "Confirm network key", then click 'OK'.

If the value you inputted here is wrong, you will not be able to connect to wireless access point. Authentication type is selected automatically, please don't change it.

4. The utility will automatically add the access point at Wireless Utility Profile.
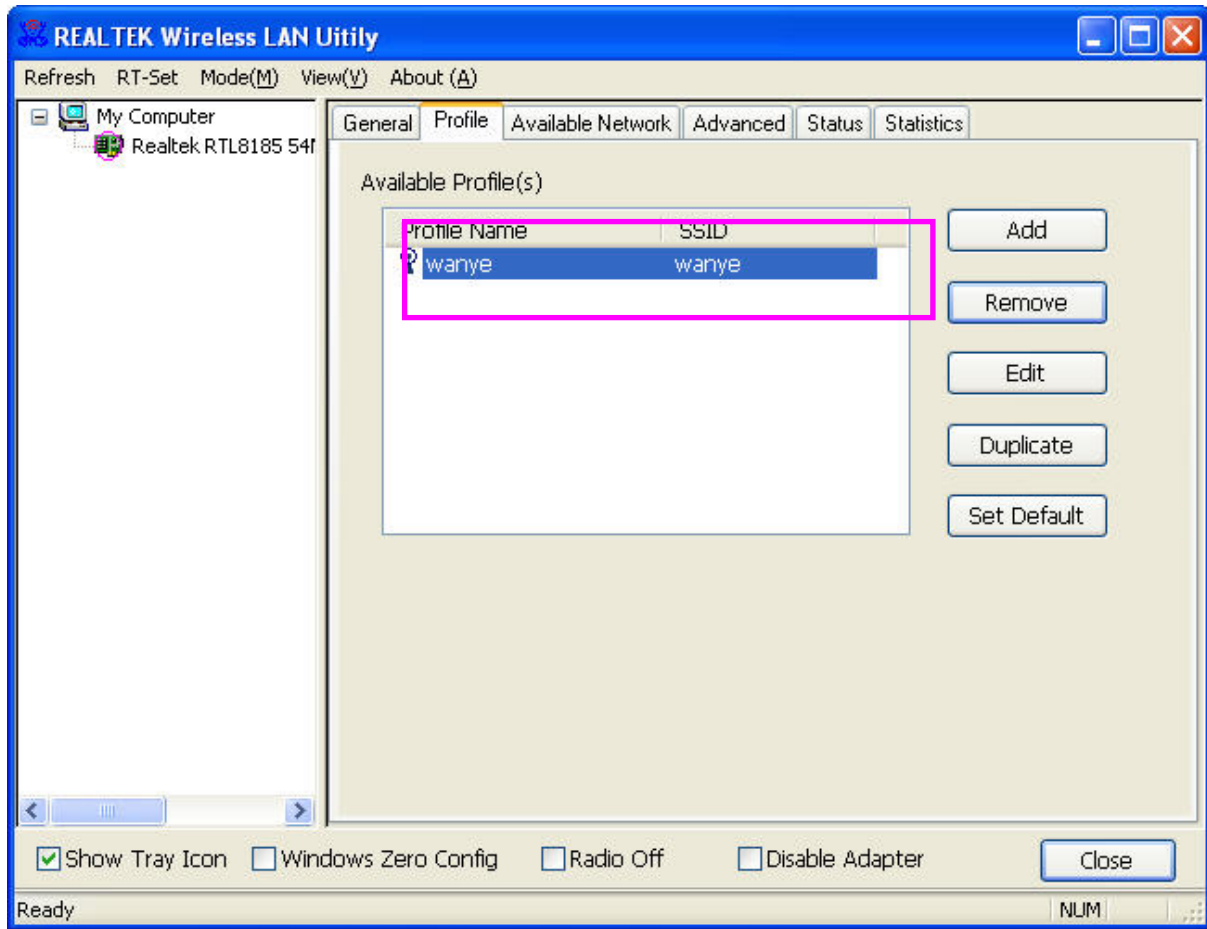
5. If the wireless access point is successfully connected, you'll see a connected icon 📶 displayed at the lower-left corner of wireless configuration utility window and click 'Close' to exit.
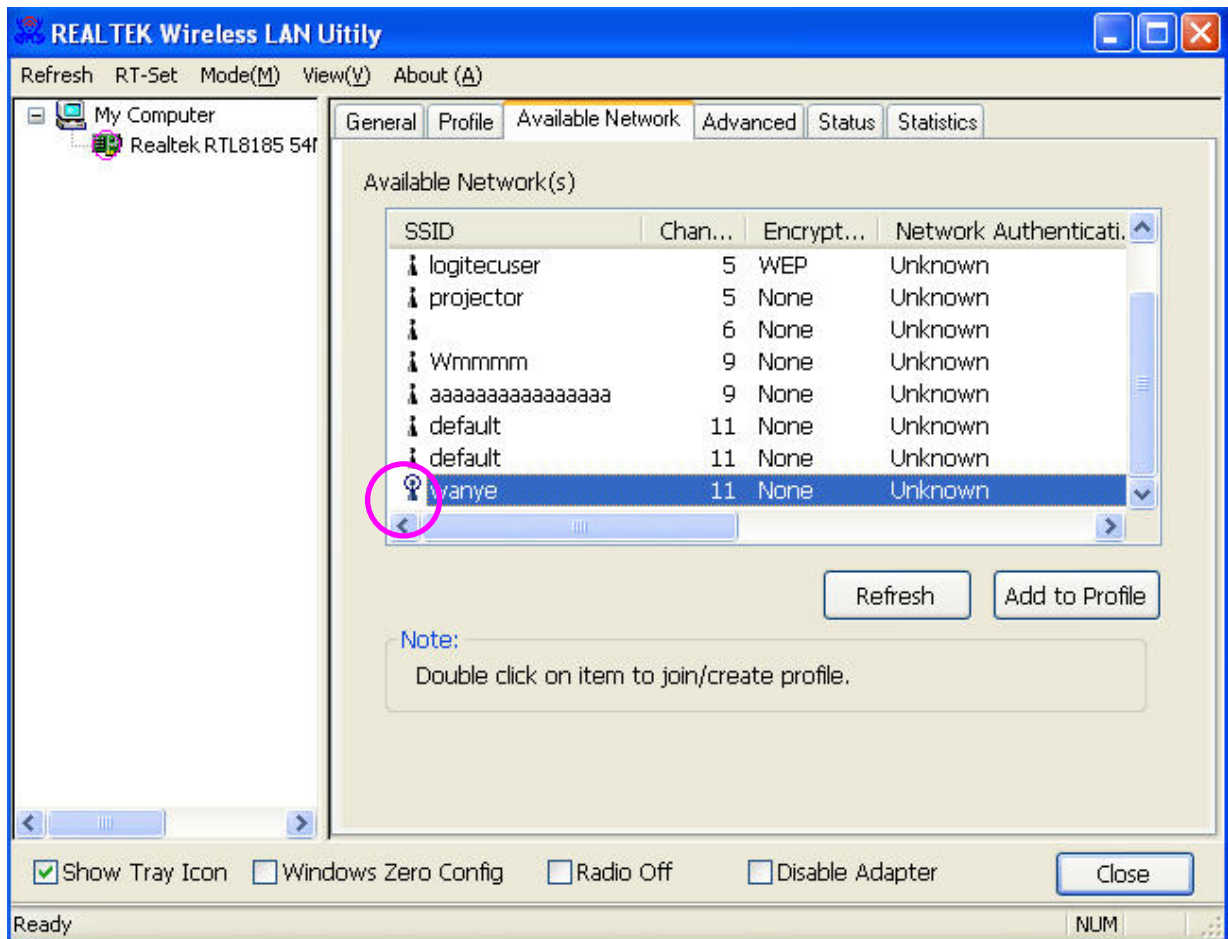
5.2 Using Windows Zero Config

1. After lunch wireless configuration, Please select "Windows Zero Config" and click "OK" to disable the utility of the adapter..
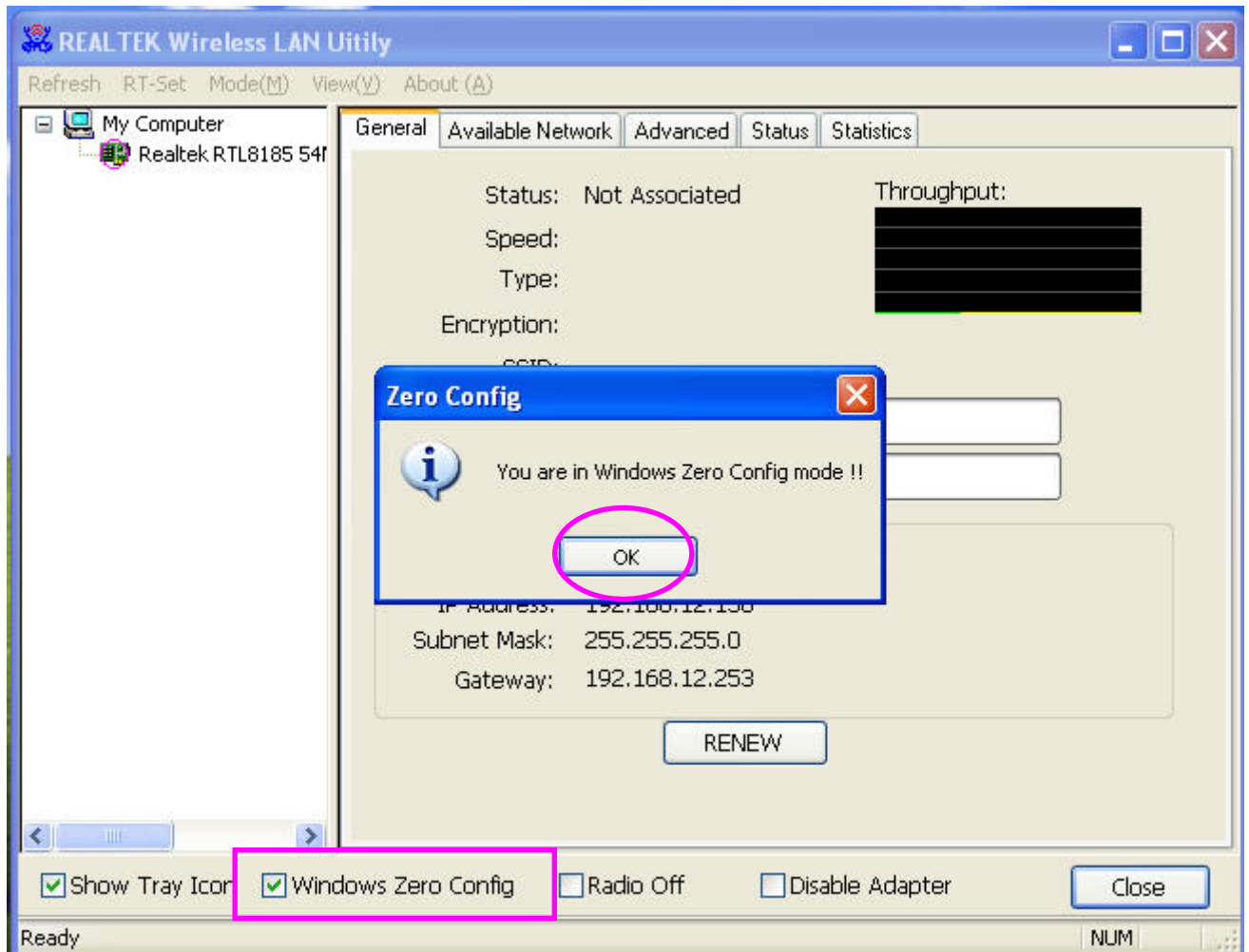
2. Please lunch Windows Zero Config by double-click the wireless connection icon in the lower-left corner on Windows desktop.

3. The Windows Zero Config Panel will pup-up. Please select the wireless access point which you want to connect and click "Connect"
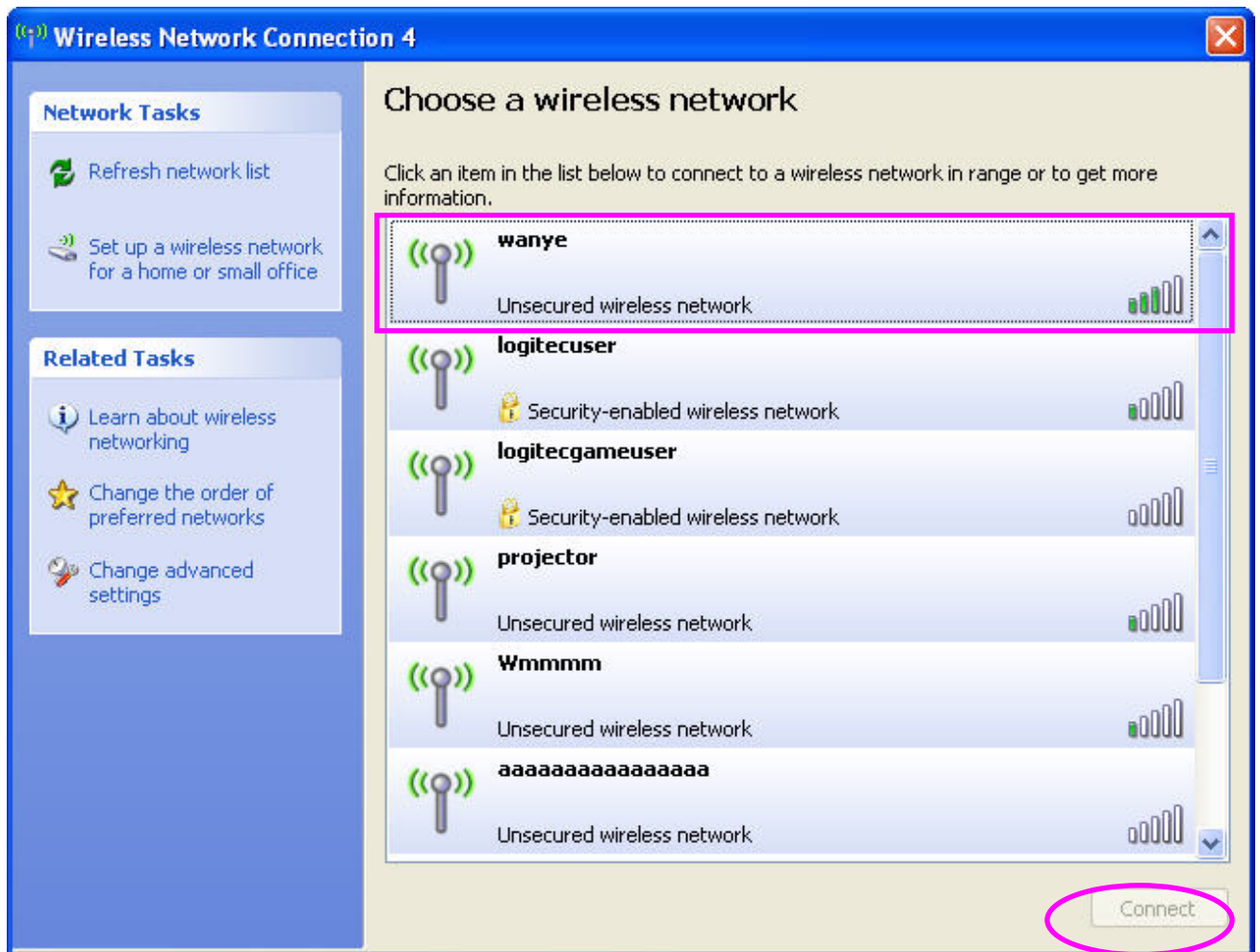
4. If the wireless access point without encryption, there is warning window will pup-up. Please click "Connect Anywhere".
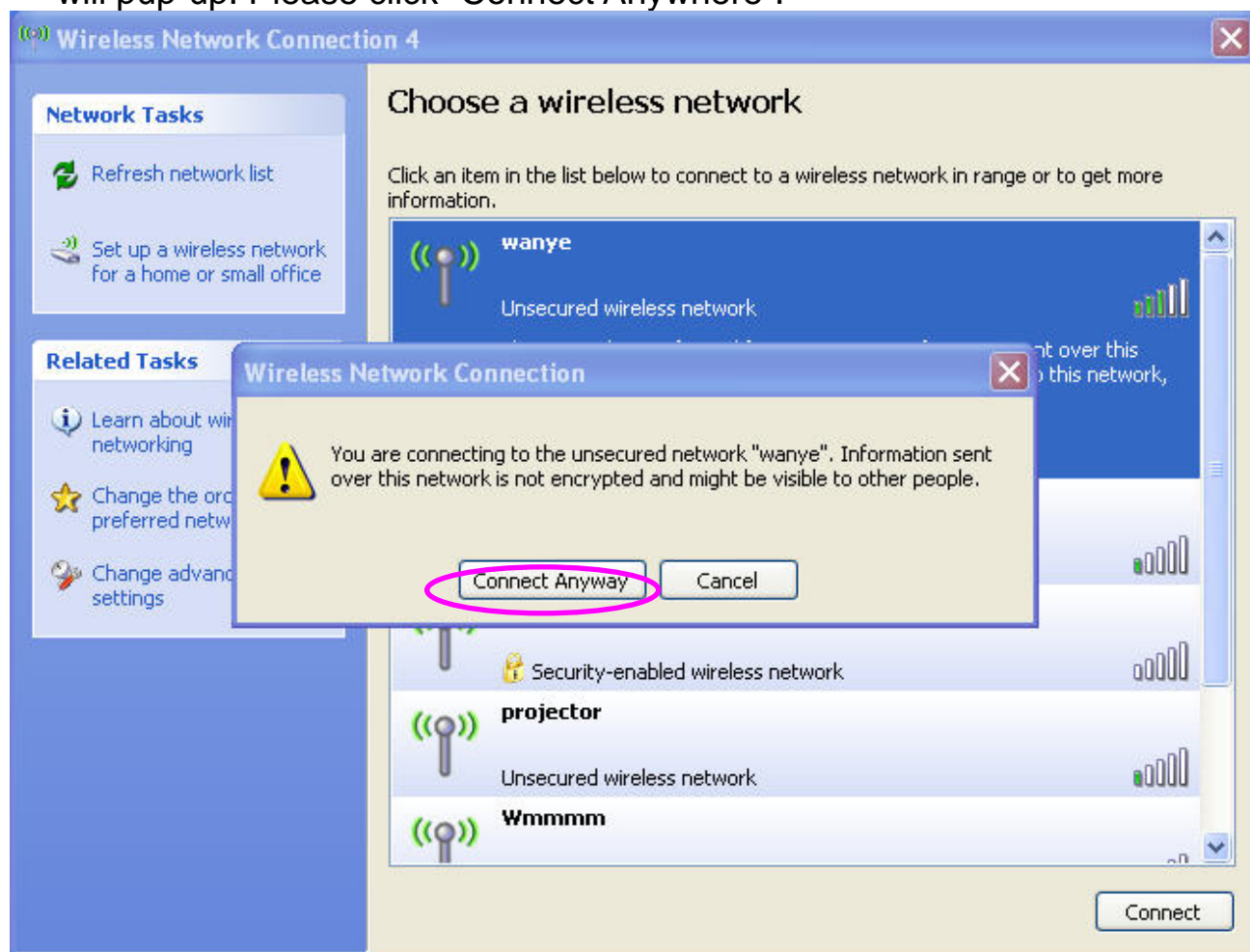
5. When you see the "Connected" shows on the Windows Zero Config window, the wireless is successfully connected.
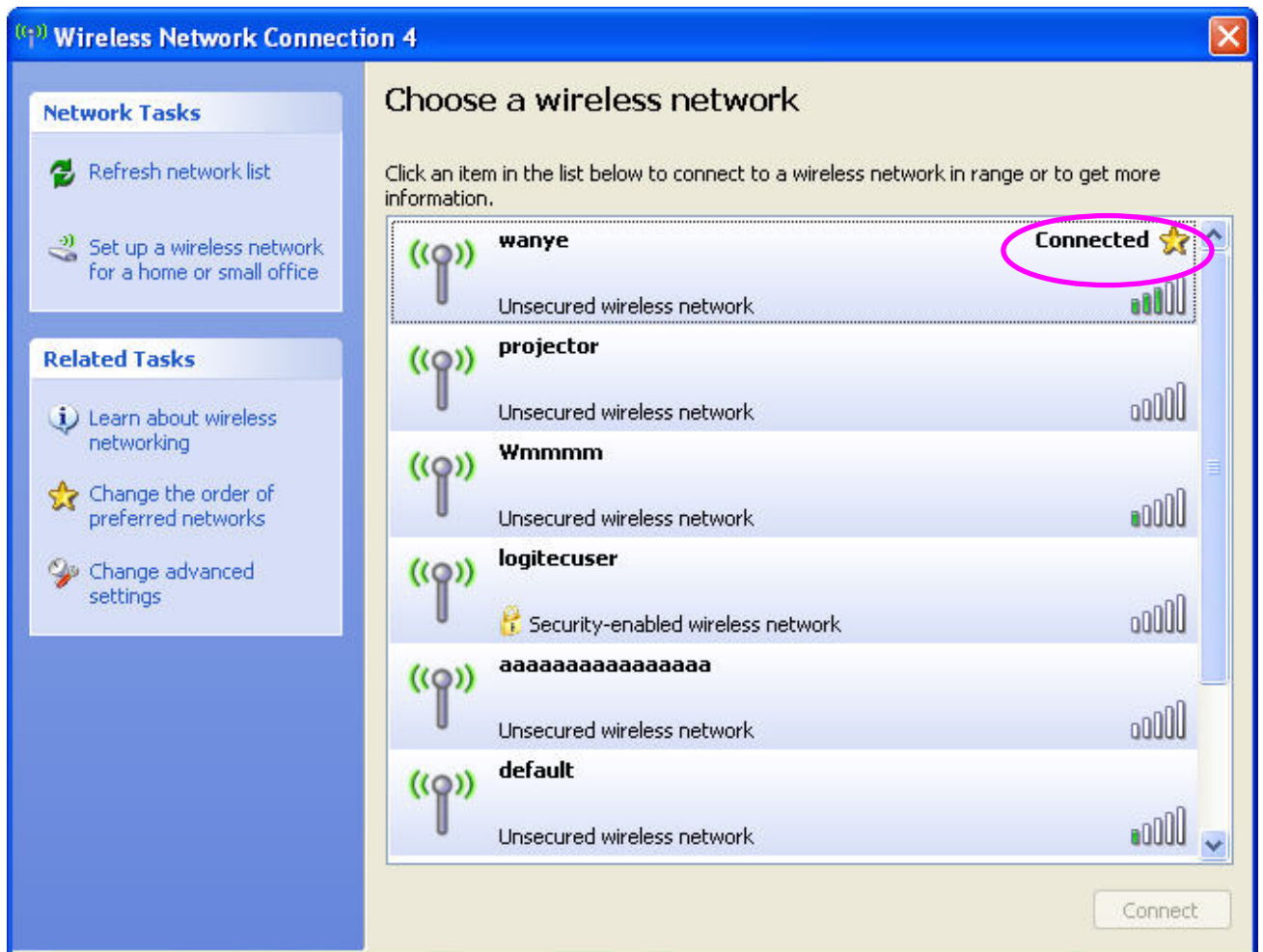
6. Configuration Utility

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.

The Configuration Utility appears as an icon on the system tray and desktop of Windows. You can open it by double-click on the icon.

In the Desktop   *In the System Tray*

Right click the icon in the system tray there are some items for you to operate the configuration utility.

Open Config Utility

Select "Open Config Utility" to open the configuration utility.

RT-Set Wizard

Select "RT-Set Wizard" to open the RT-Set wizard.

About

Select "About" to show the utility information.

Hide

Select "Hide" to hide the utility in the system tray.

6.1. Utility Overview

There are several parts in the utility screen. Please refer to the following table for the description.

Parameter	Description
A	**Refresh** – Refresh card list in the "B" block. **RT-Set** – Open the RT-Set wizard. **Mode** – There are two modes: Station and Access Point. If "Station" is selected, the card works as a wireless card. If "Access Point" is selected, the card will works as a wireless AP. **View** – Enable "Status Bar" and the "D" block in the utility will display the current status of the utility. **About** – To check the version of the utility, select this item.
B	This is a list for you to configure several cards in your PC from the utility.
C	**Show Tray Icon** – To show the icon in the system tray, select the item. **Windows Zero Config** – To configure the card from Windows XP Zero Configuration, check the item. **Radio Off** – This function is for you to turn off or turn on the radio of the card. If the radio is turned off, the card will not work. **Disable Adapter** – This function is for you to disable or enable the card.
D	It is the status bar that displays the current status of the utility. To close it, please disable the "Status Bar" in the "View" item.
E	There are several tabs in the block for you to setup the function of the card. Please refer to the description in the following sections.

6.2. Available Network

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 network with the highest signal strength. From the "Available Network" tab, all the networks nearby will be listed. You can change the connection to another network.
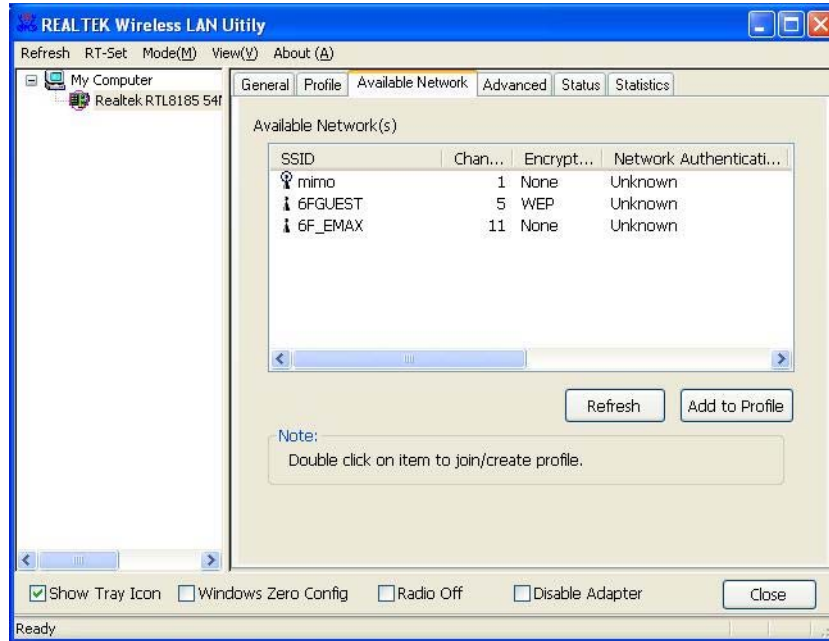
Parameter	Description
Available Network(s)	This list shows all information of the available wireless networks within the range of your card. The information includes SSID, Channel, Encryption, Network Authentication, Signal and etc. If you want to connect to any network on the list, double-click the selected network.
Refresh	Click "Refresh" to update the available networks list. It is recommended that refresh the list while you have changed the connection network.
Add to Profile	A profile stores the setting of a network, so that you can connect to the network quickly. To add the selected network to a profile, click this button.

6.3. General

To check the connection status of the card, select "General". This screen shows the information of Link Speed, Network Type, Encryption Method, SSID, Signal Strength, Link Quality and Network Address of the card.

Parameter	Description
Status	It will show the connection status of the card.
Speed	It shows the current speed
Type	**Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **IBSS** – Select this mode if you want to connect to another wireless stations in the Wireless LAN network without through an Access Point or Router.
Encryption	It displays the encryption setting of the current connection including None, WEP, TKIP or AES.
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.
Signal Strength	It indicates the wireless signal strength.

Parameter	Description
Link Quality	It indicates the wireless link quality.
Network Address	It shows the MAC, IP address and other information of the card.

6.4. Profile

The "Profiles List" is for you to manage the networks you connect to frequently. You are able to Add/Remove/Edit/Duplicate/Set Default to manage a profile.
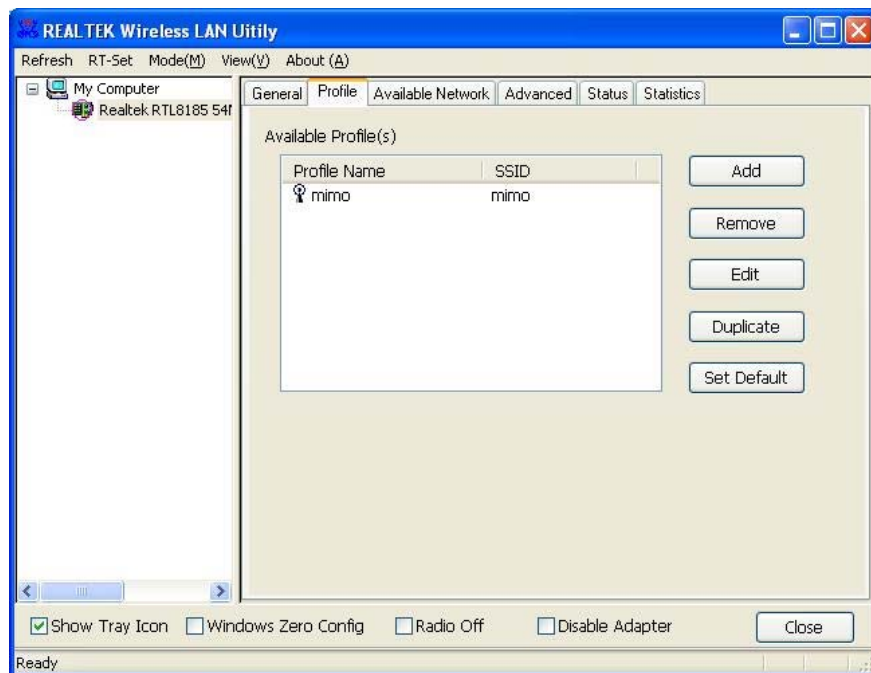
Parameter	Description
Available Profile(s)	This list shows the preferred networks for the wireless connection. You can add, remove, edit, duplicate the preferred networks or set one of the networks as the default connection.
Add/ Remove/ Edit Button	Click these buttons to add/ delete/ edit the selected profiles.
Duplicate	If you like to build up the new profile with the same settings as the current profile, then you can select this feature.
Set Default	To designate a profile as the default network for the connection from the available profiles list, click the button.

6.4.1. Configure the Profile

Parameter	Description
Profile Name	Define a recognizable profile name for you to identify the different networks.
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. You may specify a SSID for the card and then only the device with the same SSID can interconnect to the card.
This is a computer-to-computer (ad hoc) network; wireless access points are not used.	There are two kinds of network type described as follows. **Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **Ad Hoc** – Connect to another wireless card in the Wireless LAN network without through an Access Point or Router. If this item is selected, the card will work in Ad Hoc mode.
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 with the network you are connecting to.

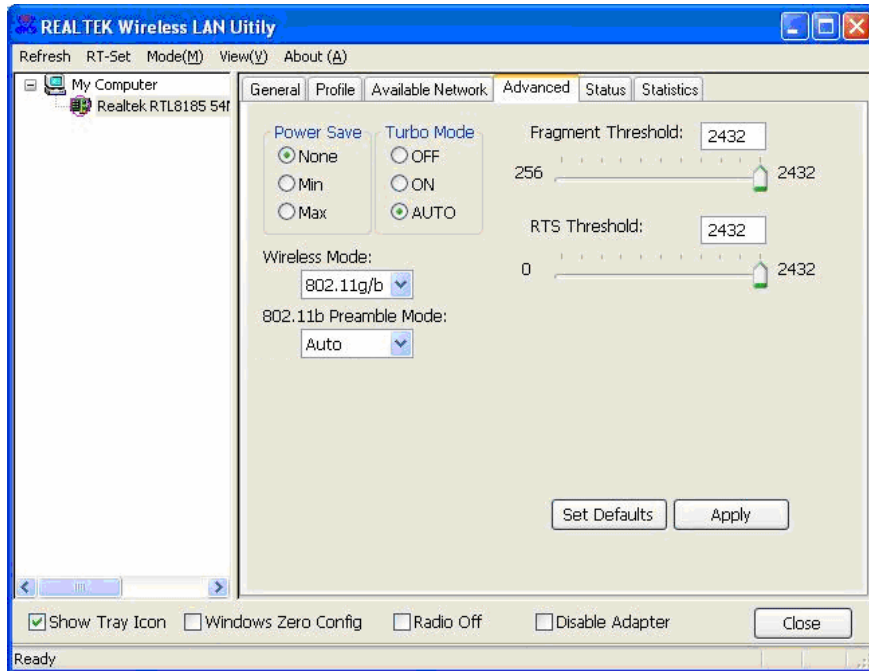| Parameter	Description
Network Authentication	This setting has to be consistent with the wireless networks that the card intends to connect. **Open System** – No authentication is needed among the wireless network. **Shared Key** – Only wireless stations using a shared key (WEP Key identified) are allowed to connecting each other. **WPA 802.1X** – WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure. **WPA-PSK** – It 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, the user manually enters the starting password in their access point or gateway, as well as in each wireless stations in the network. WPA-PSK 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. **WPA2 802.1X** – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP). **WPA2-PSK** – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP). **WEP 802.1X** – It's a special mode for using IEEE 802.1x/EAP technology for authentication and WEP keys for data encryption.

Parameter	Description
Data Encryption	**Disabled** – 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 kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES** – 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. Note: All devices in the network should use the same encryption method to ensure the communication.
ASCII	WEP Key can be ASCII format. Alphanumeric values or signs are allowed to be the WEP key. It is more recognizable for user.
Passphrase	It is a text string with a maximum of 32 alphanumeric characters, for example: "Test". The WEP Key is based upon the Passphrase determined by you. This passphrase may not work with other vendors' products due to possible incompatibility with other vendors' passphrase generators. You must use the same passphrase or WEP key settings for all wireless computers within the network.
Network Key	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 as the encryption keys. For example: "0123456aef". **128-bit** – Input 26-digit Hex values as the encryption keys. For example: "01234567890123456789abcdef".
Confirm Network Key	Enter the same network key to confirm.
Key Index (advanced)	Select one of the four keys to be the data encryption key.

Parameter	Description
EAP Type	**GTC** – GTC is an authentication protocol which allows the exchange of clear text authentication credentials across the network. **TLS** – TLS is the most secure of the EAP protocols but not easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client. After validating the server's certificate, the client presents a client certificate to the server for validation. **LEAP** – LEAP is a pre-EAP, Cisco-proprietary protocol, with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited vendor choice for client, access-point, and server products is not a concern. When you have set up LEAP authentication, you have to enter the user name and password of your computer. **PEAP & TTLS** – PEAP and TTLS are similar and easier than TLS in that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2 and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adaptor supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. The client certificate is optional required for the authentication.
Tunnel	Includes MD5, GTC, TLS, CHAP, MSCHAP, MSCHAP-v2 and PAP.
Username	The certificate username in the RADIUS server.
Identity	User's identity in the RADIUS server.
Password	User's password in the RADIUS server.
Certificate	The certificate for RADIUS server for certification.

6.5. Advanced

The "Advanced" option enables you to configure more advanced settings, for example: Power Save, Turbo Mode, Wireless Mode and etc.

Parameter	Description
Power Save	**None** – The card will always set in active mode.
	Min – Enable the card in the power saving mode when it is idle, but some components of the card are still alive. In this mode, the power consumption is larger than "Max" mode.
	Max – Enable the card in the power saving mode when it is idle.
Turbo Mode	**Off** – Turn off the turbo mode.
	On – Turn on the turbo mode.
	Auto – The card will detect the AP is RTL8186-based AP or not to transmit data in turbo mode automatically.
Wireless Mode	**802.11 b** – 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, you can set the card to this mode.
	802.11 g/b – If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended to setting the card to this mode.

Parameter	Description
802.11b Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless stations. There are three mode including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If "Auto" mode is selected, the card will auto switch the preamble mode depending on the wireless stations that the card is connecting to. Note that the parameter is only active in the Ad Hoc operation mode.
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 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 wireless network. Select a setting within a range of 0 to 2432 bytes. Minor change is recommended.
Set Defaults	Let the setting values return to default.
Apply	Confirm the settings in the "Advanced".

6.6. Status

This screen shows the information of manufacturer, driver version, settings of the wireless network the card is connecting to, linking time and link status. If you don't ensure the status of the card and the network you are connecting, please go to the screen for more details.
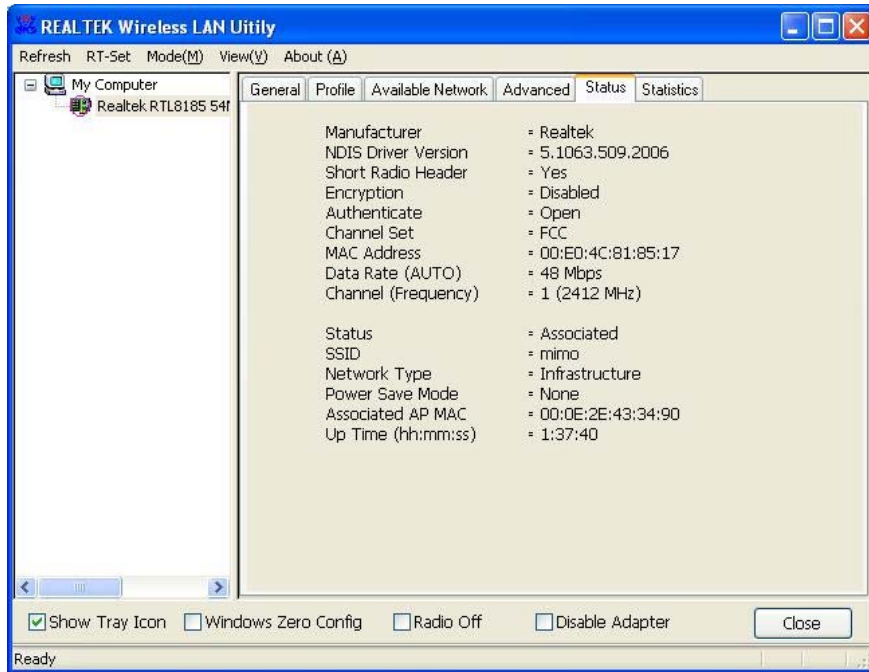
6.7. Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click "Reset".
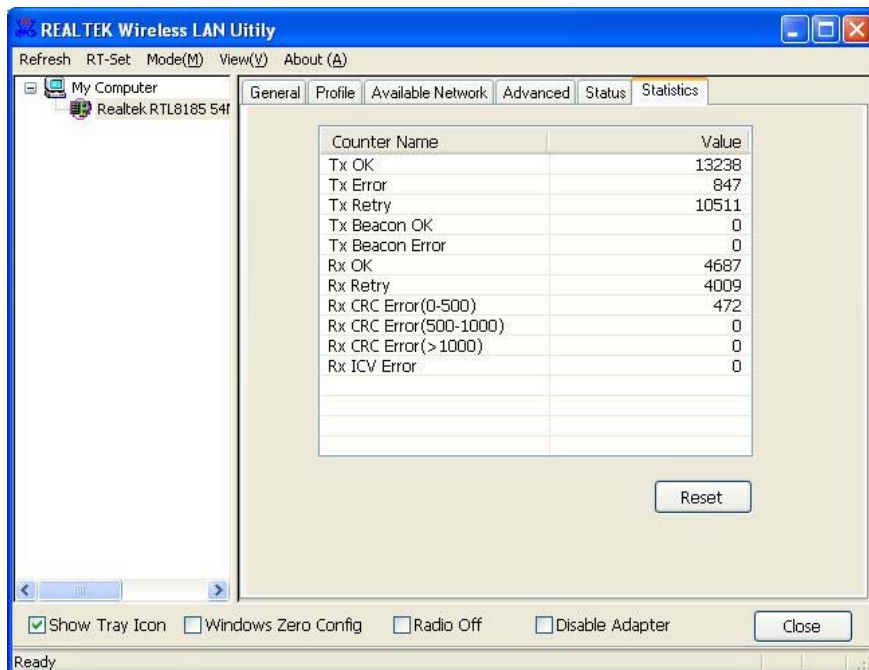
6.8. Software AP

This card can run as a wireless AP. The relative configurations of the AP including channel, SSID, WEP encryption and so on are described as follows.
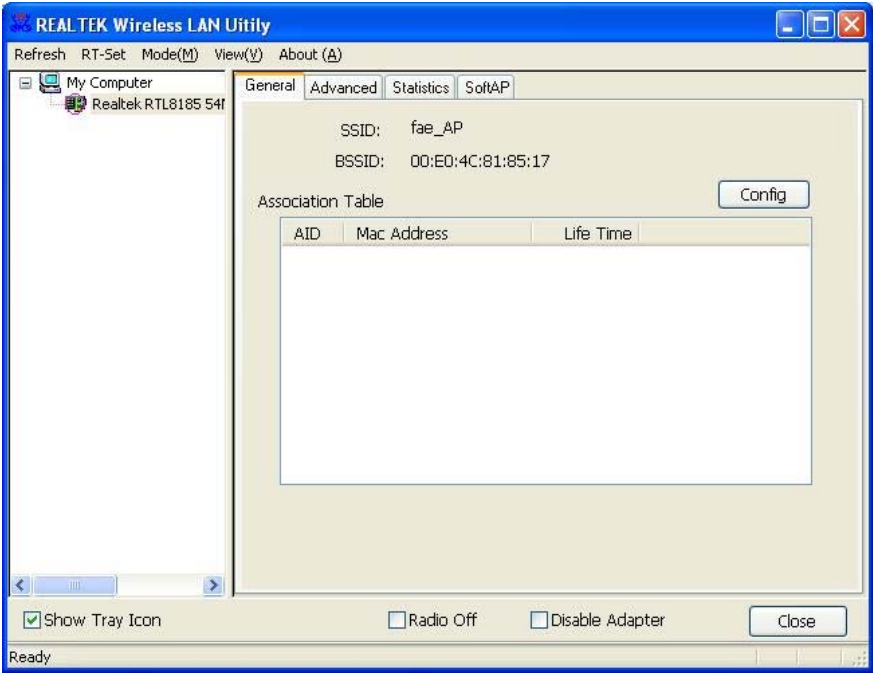

Parameter	Description
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs.
	The default SSID of the AP is "fae_AP". Wireless cards connect to the AP should set up the same SSID as the AP.
BSSID	Display the MAC address of the card.
Associate Table	All the wireless cards connected to the software AP will be displayed in the list.
Config	Click "Config" for setting more configuration of the AP.

6.8.1. AP Properties Setting

Please refer to Section 3.4.1 for the setting of the parameters for AP. Note that Ad Hoc mode is not enabled for AP.
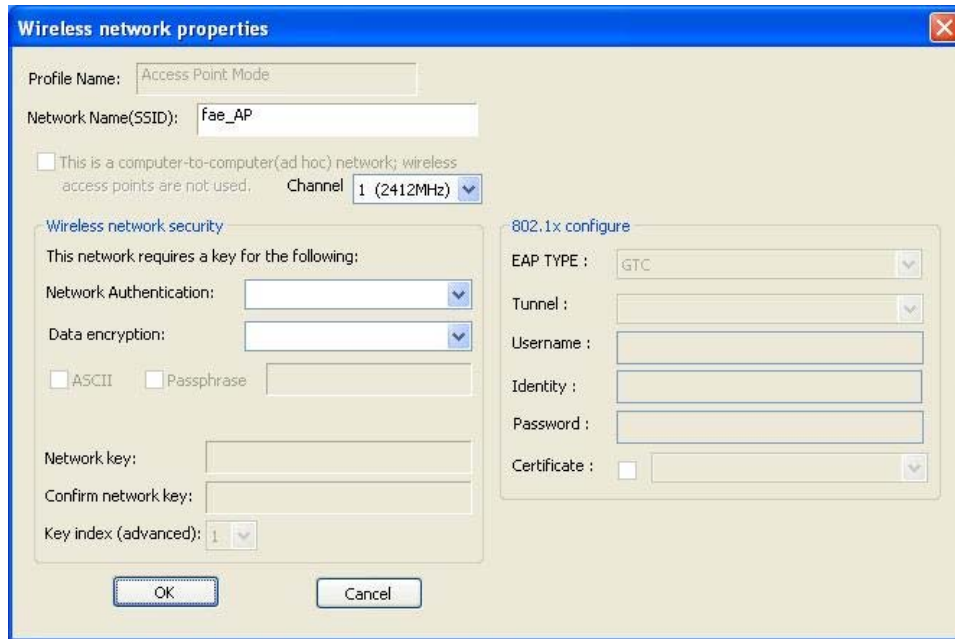
6.8.2. AP Advanced
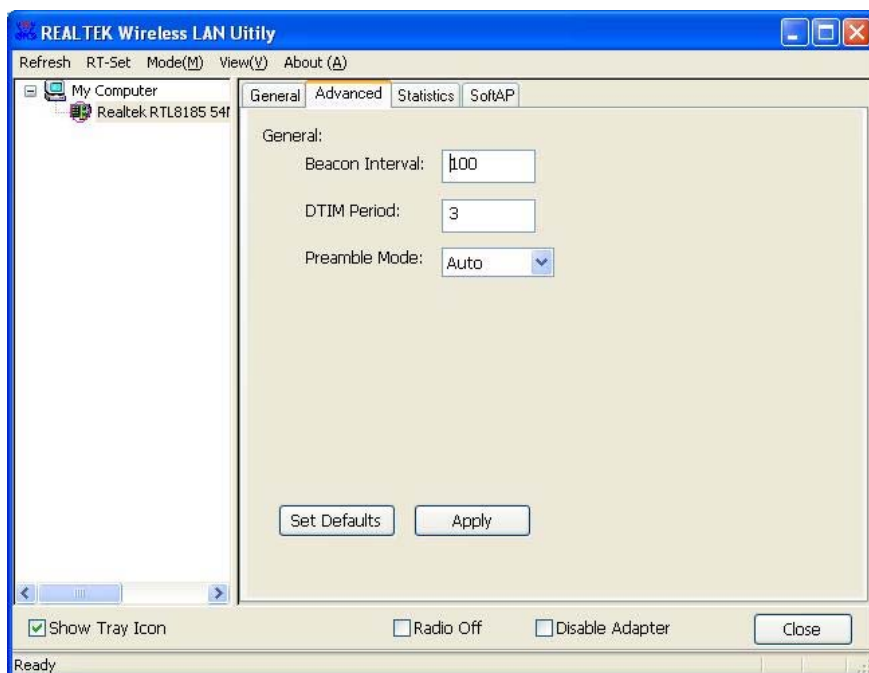
| Parameter	Description
Beacon Interval	Beacon Interval that specifies the duration between beacon packets (milliseconds). The range for the beacon period is between 20-1000 milliseconds with a typical value of 100.
DTIM Period	Determines the interval the Access Point will send its broadcast traffic. Default value is 3 beacons.
Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless stations. There are three mode including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If "Auto" mode is selected, the AP will auto switch the preamble mode depending on the wireless cards.
Set Defaults	Set the setting values return to defaults.
Apply	Confirm the settings in the "Advanced".

6.8.3. AP Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click "Reset".
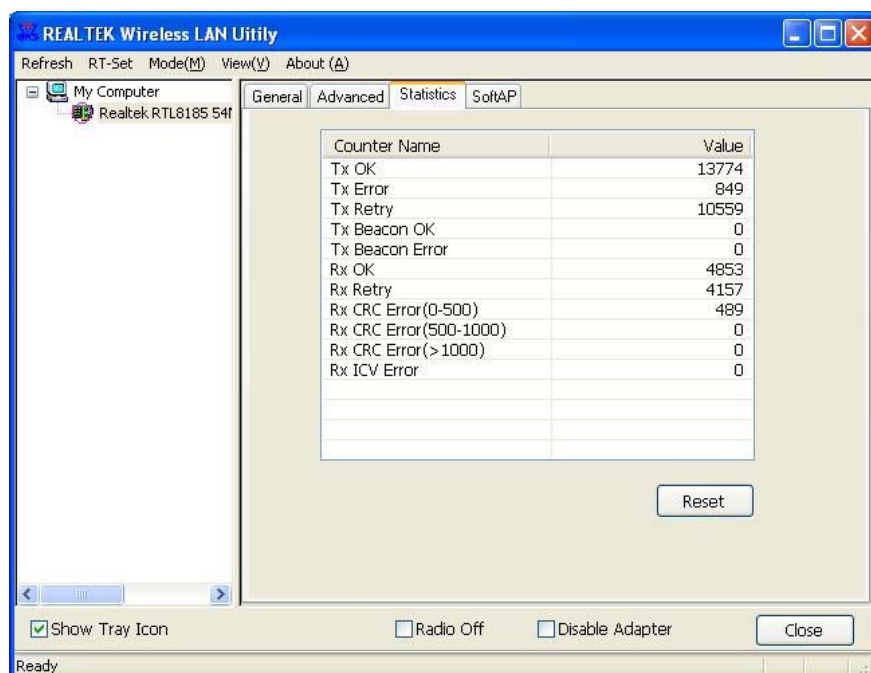
6.8.4. SoftAP

If you want to connect to the internet through this SoftAP, you will need to make a bridge between our SoftAP and your internet connect. Select the internet connection in your SoftAP host machine and press the "Apply" button.
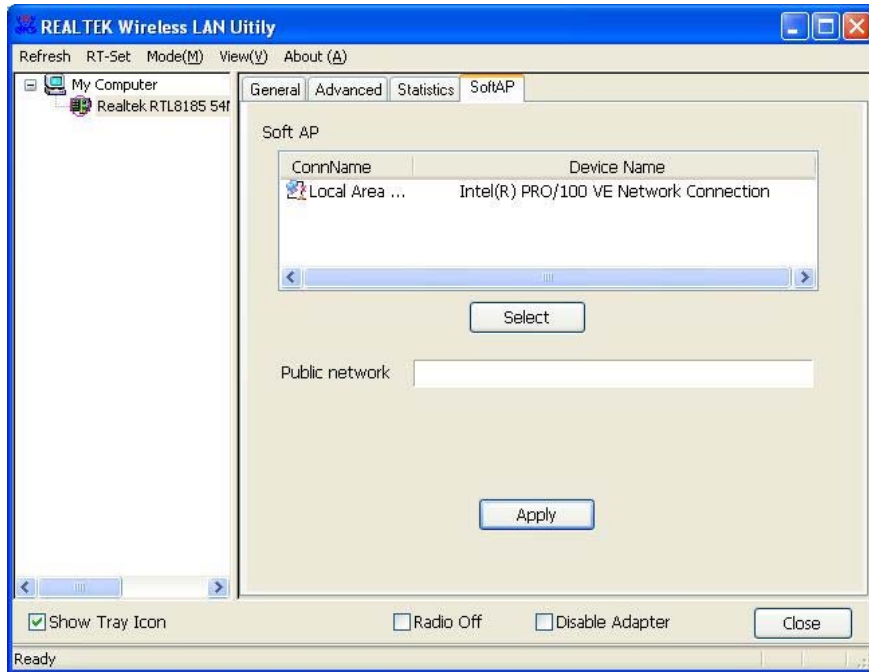
7. RT-Set Wizard

The RT-Set wizard can help users to connect to a wireless LAN or build an Ad-hoc wireless network.

For example, if you want to connect to a wireless LAN in infrastructure mode: A.

Open the RT-Set wizard and choose the Station (infrastructure) mode.

B. The site survey results will show up. Please select the one you'd like to connect to and click the "Next" button.
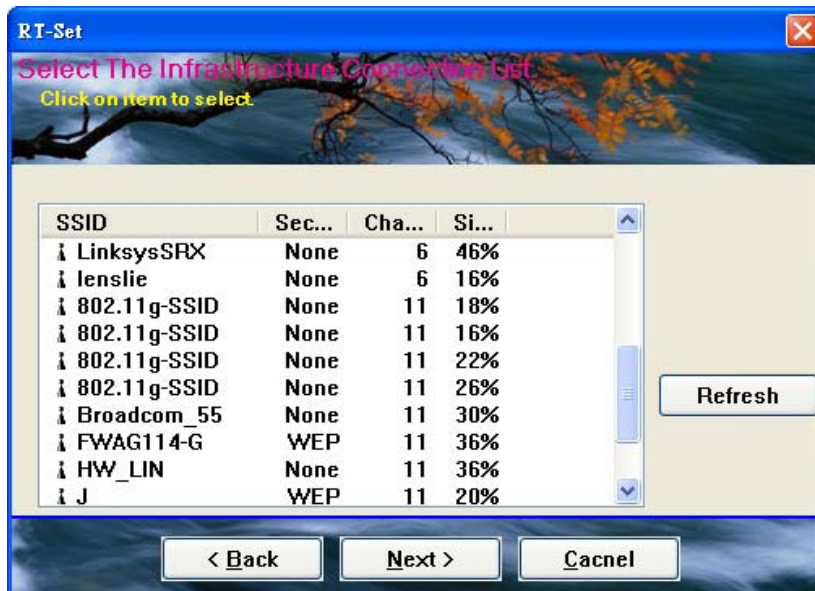
C. In the Wireless network properties dialog, please fill in the security settings for this wireless network you'd like to connect to.
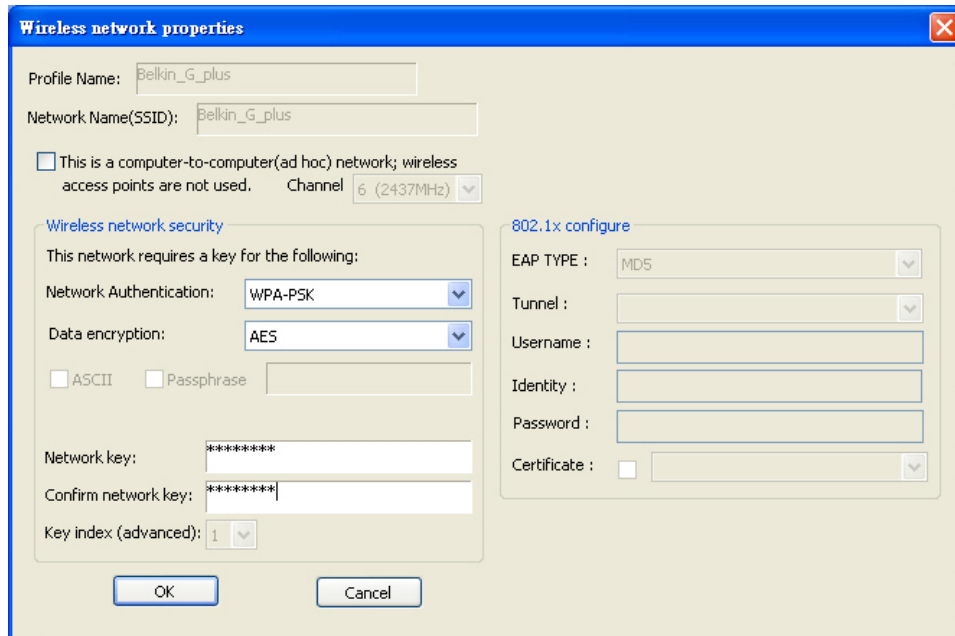
D. Please specify the IP settings for this wireless network and click the "Finish" button.
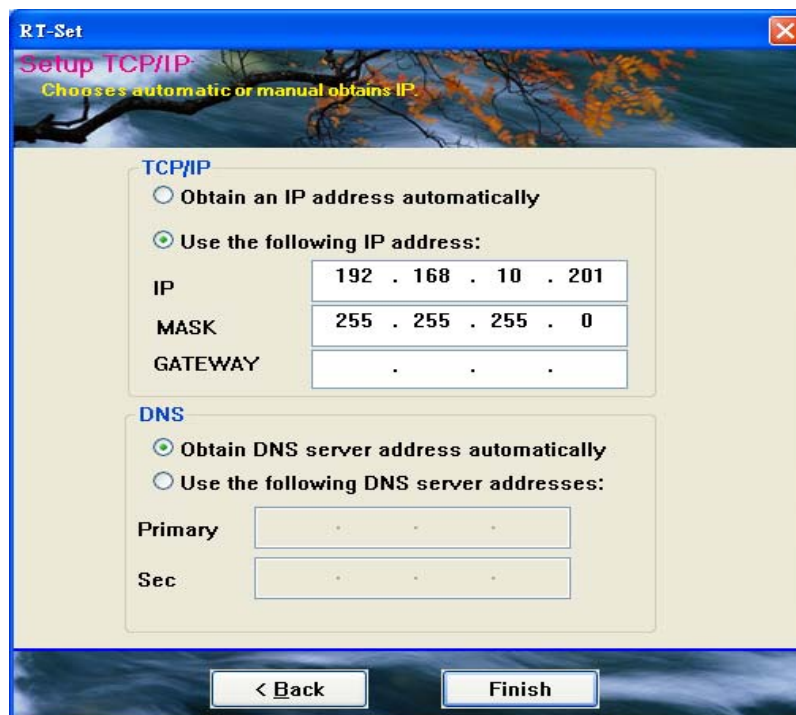
E. Now you can connect to the wireless network successfully.

General	Profile	Available Network	Advanced	Status	Statistics

Status: Associated

Speed: 36 Mbps

Type: Infrastructure

Encryption: None

SSID: HW_LIN

Throughput Tx:0%,Total:0%

Signal Strength: ||||||||||||||||||||||| 66%

Link Quality: ||||||||||||||||||||||||| 76%

Network Address

Mac Address: 00:E0:4C:81:86:36

IP Address: 169.254.122.157

Subnet Mask: 255.255.0.0

Gateway:

RENEW

8. 5 Troubleshooting

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

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, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **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

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

5. **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.

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

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 IEEE 802.11i standard. Compare 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 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.

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 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.

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).