IEEE 802.11n Wireless Series

Wireless 1T1R USB Adapter

User Manual

Version: 2.0
Date: June 20, 2011

FCC Certifications

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
IEEE 802.11b/g or 802.11n operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

CE Mark Warning

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 Class B for ITE, the essential protection requirement of Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility and R&TTE Directive 1999/5/EC to meet the regulation of the radio equipment and telecommunications terminal equipment.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:

Package Contents

The following contents should be found in your box:

- One IEEE 802.11n USB Adapter
- One resource CD, including:
  - REALTEK 11n USB Wireless LAN Driver and Utility
  - User's Manual
  - QIG

Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Conventions:

The "Adapter" mentioned in this user guide stands for Wireless 11n USB Adapter without any explanations.

CONTENTS

Chapter 1 Introduction

Thank you for purchasing this product. Read this chapter to know about your IEEE 802.11n wireless USB Adapter.

1.1 Overview of the product

Comply with 802.11n Standards

The IEEE 802.11n Wireless USB adapter provides users to launch IEEE 802.11n wireless network in the 2.4 GHz band, which is also compatible with IEEE 802.11b/g wireless devices.

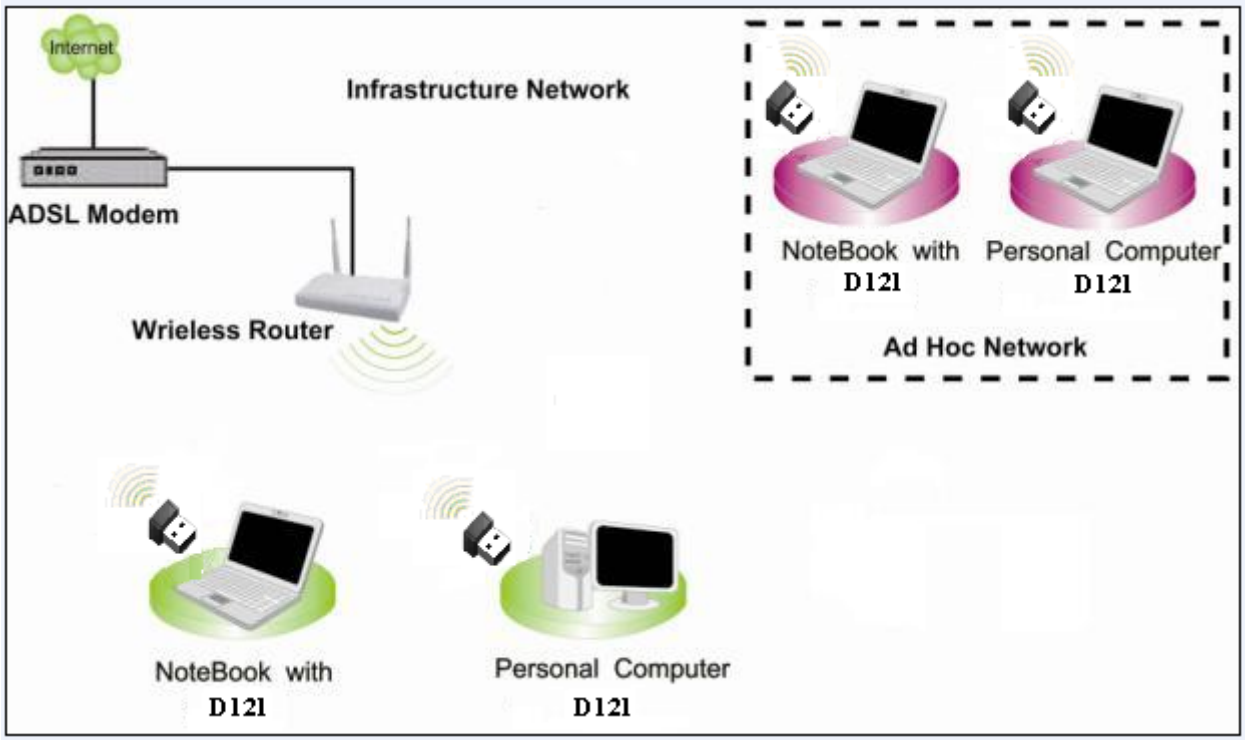
Reliable Coverage

The adapter has internal intelligent antenna providing even better wireless performance, transmission rates, stability and coverage. It includes a convenient utility for scanning available networks and saving preferred networks that users usually connected with. Your wireless communications are protected by up to 128-bit encryption, so your data stays secure.

Easy Installation and Connection

In addition, installation and use are further simplified by living up to USB's Plug and Play installation approach to connecting computer peripherals. You will not need to open the case of your computer, nor will you be required to set IRQ (Interrupt Request). So it is the simplest way to connect your computer to an Ethernet based network.

1.2 Application Diagram



1.3 Features

- Supports QoS Enhancement (WMM, WMM-PS Client mode)
- Supports wireless data encryption with 64/128-bit WPA,WPA2
- Supports frame aggregation, Power saving mechanism, channel management and co-existence
- Transmit Opportunity (TXOP) Short Inter-Frame Space (SIFS) bursting for higher multimedia bandwidth
- Supports auto-installation and diagnostic utilities
- Supports driver for Windows 7, 2003, XP 86, XP 64, Vista 86, Vista 64, Linux, MAC

1.4 LED Status

LED Indications	Status	Working Status
Radio/ACT LED	Blink green	The adapter is Radio on
	Blink green and flashing intermittently	The adapter is already connected but is not transmitting or receiving data
	Blink green and fast flashing	The adapter is activity and transmitting of receiving data.
	Off	The adapter is Radio off

Chapter 2 Installation Guide for Windows

2.1 Hardware Installation

The installation of the adapter is very simple. You could plug the adapter directly to the USB port on your computer. The LED will light up when the adapter is installed successfully and the PC is on.

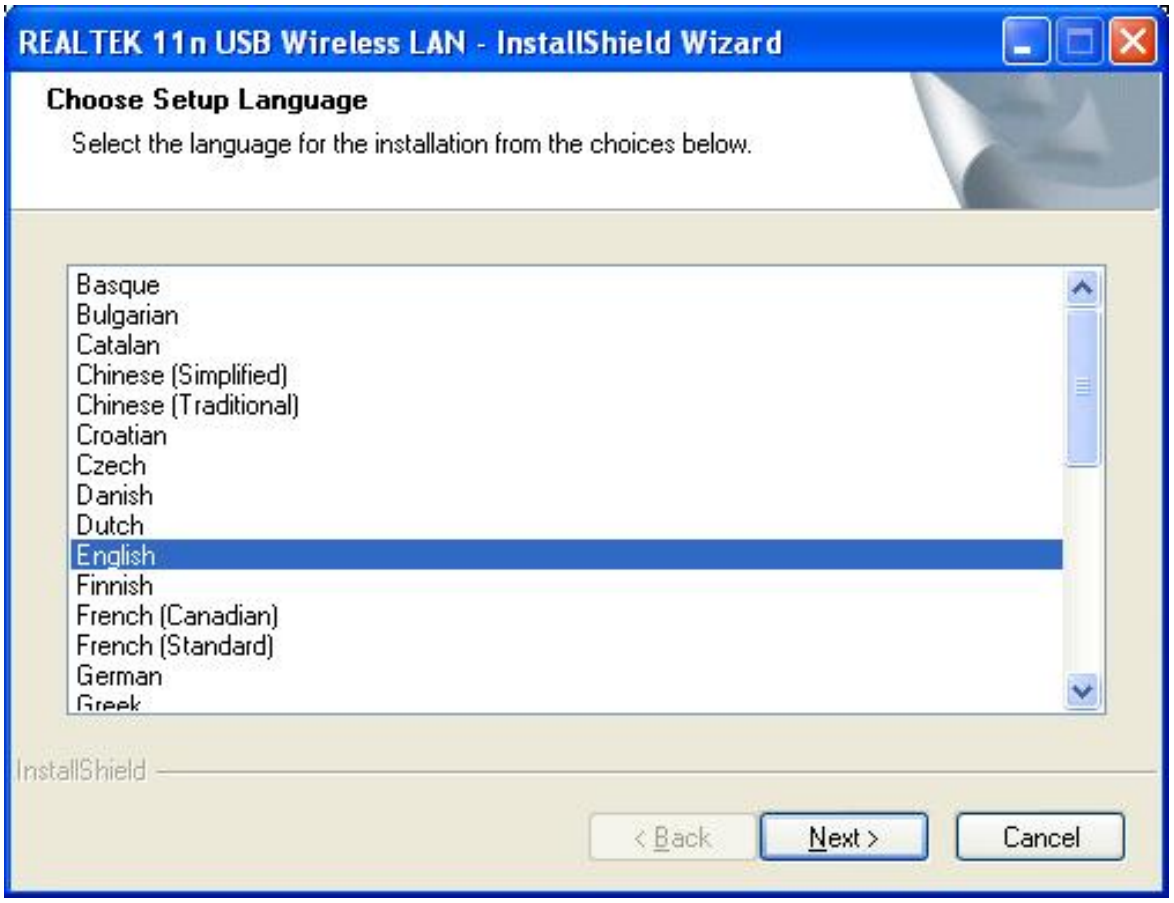
2.2 Software Installation

2.2.1 Overview

The Adapter's Setup Wizard will guide you through the Installation procedure for Windows XP. The Setup Wizard will install the REALTEK 11n USB Wireless LAN Driver and Utility. When you install the hardware prior to before installing the software, the system will prompt "Found New Hardware Wizard", click **Cancel**, and run the Setup Wizard program on the CD-ROM.

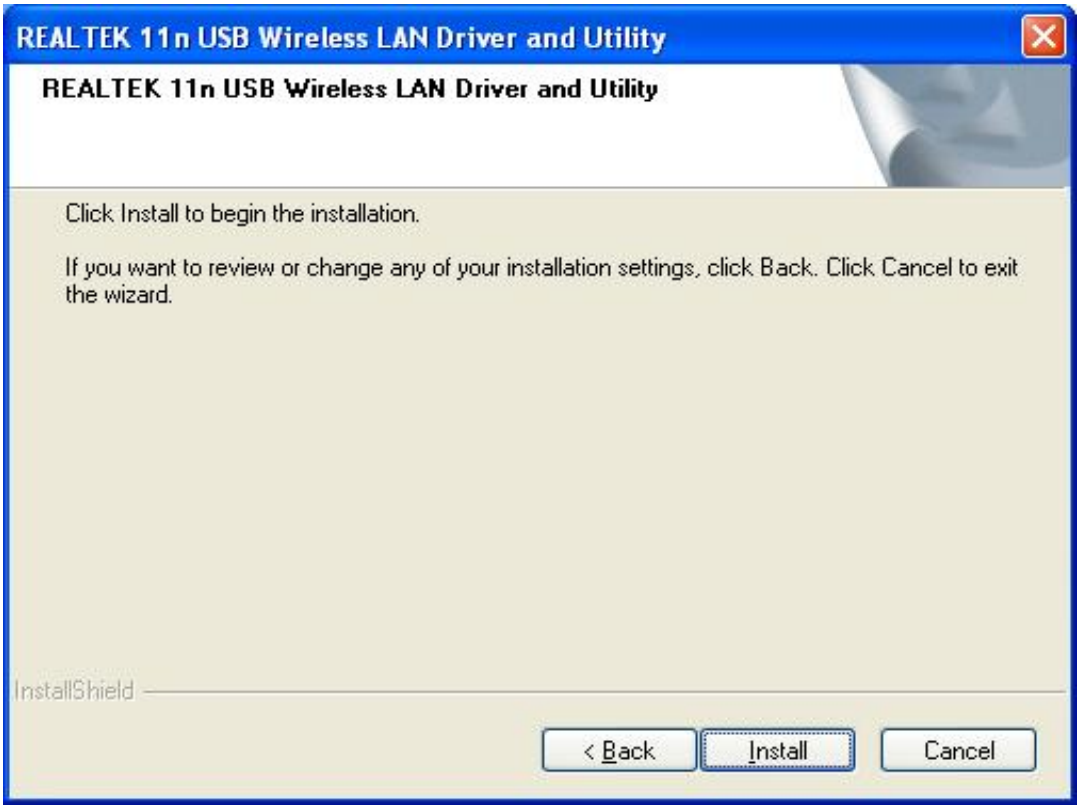
2.2.2 Installation Procedures

1. Insert the CD into your CD-Rom, and find the setup driver in the CD. Then click the setup icon to start the installation.
2. The language-selecting window pops up. Please select the language you use and click "Next".

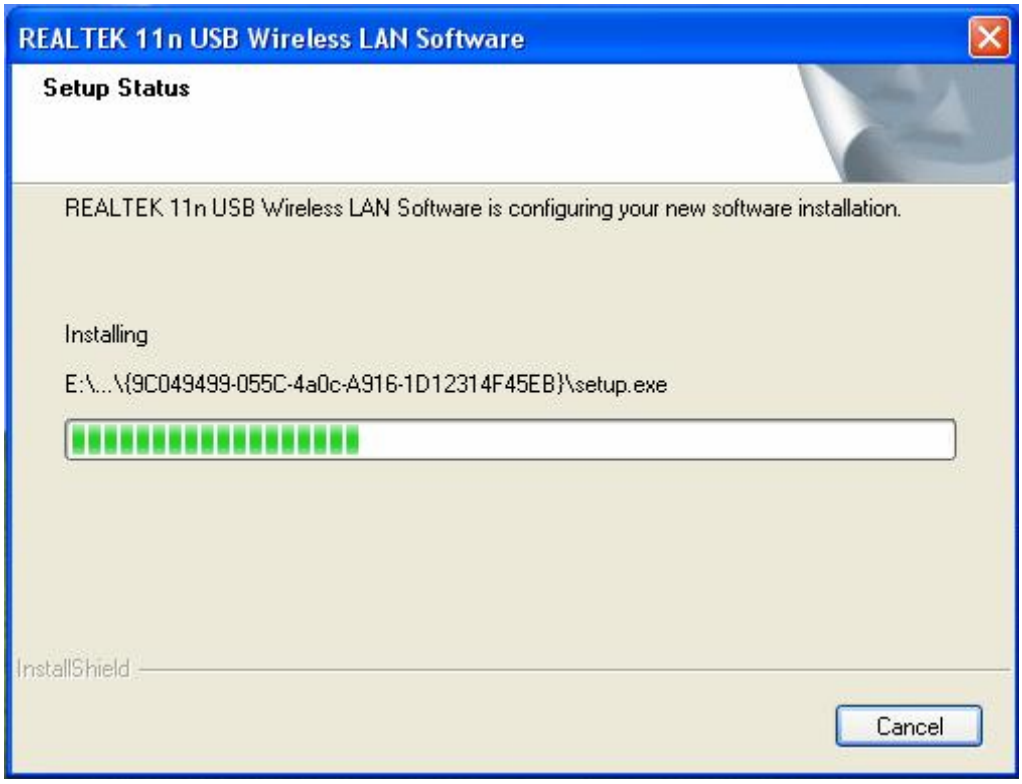


3. The welcome window pops up. Click the “Next” button to proceed.

4. Click the “Install” button to start installing.

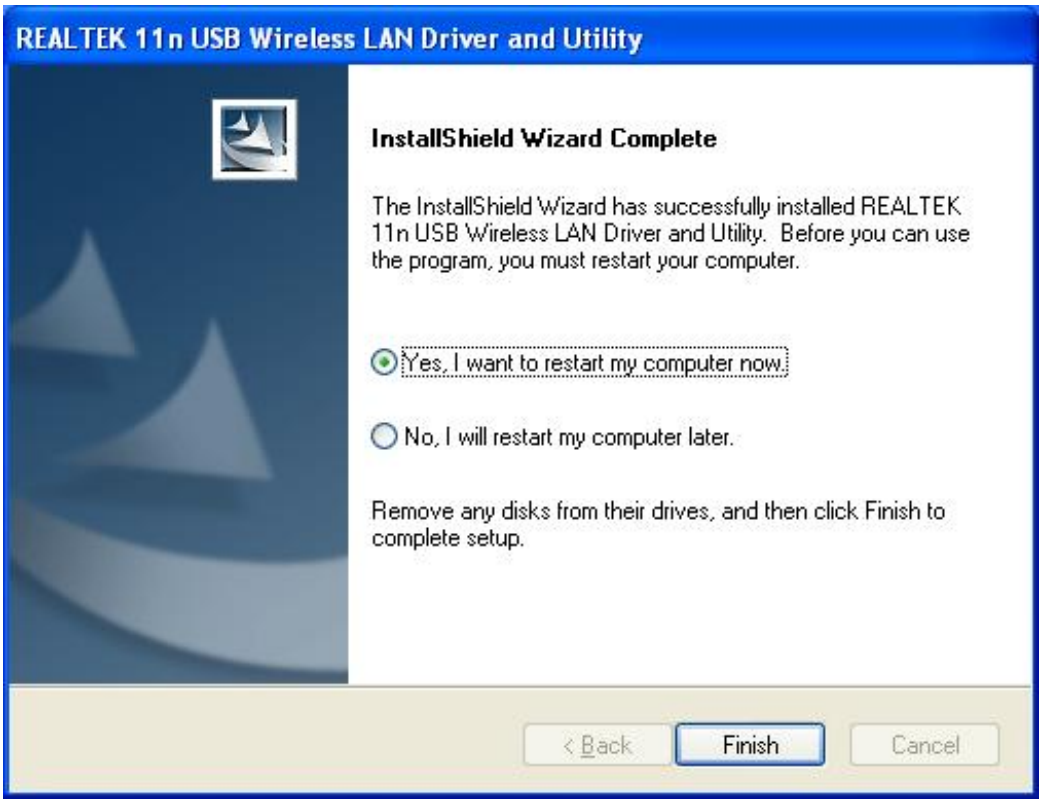


5. Please wait while installation.



6. Please wait again while installation

7. After all the steps above, you will see the screen below, click **Finish** to reboot the system.



Chapter 3 Management Guide

This chapter describes how to configure your Adapter for wireless connectivity on your Wireless Local Area Network (WLAN) and use the data security encryption features.

This User Guide takes Windows XP as the configuration example.

After Installing the Adapter, the Adapter's tray icon will appear in your system tray. It appears at the bottom of the screen, and shows the signal strength using color and the received signal strength indication (RSSI).

 If the icon is purple, there is no connection.

 If the icon is white, the network is dropping off.

 If the icon is green, there is good signal strength.

 If the icon is green, there is excellent signal strength.

3.1 Making a Basic Network Connection

3.1.1 Select a configuration tool

In the following instruction for making a network connection, we use the provided Utility to configure your wireless network settings.

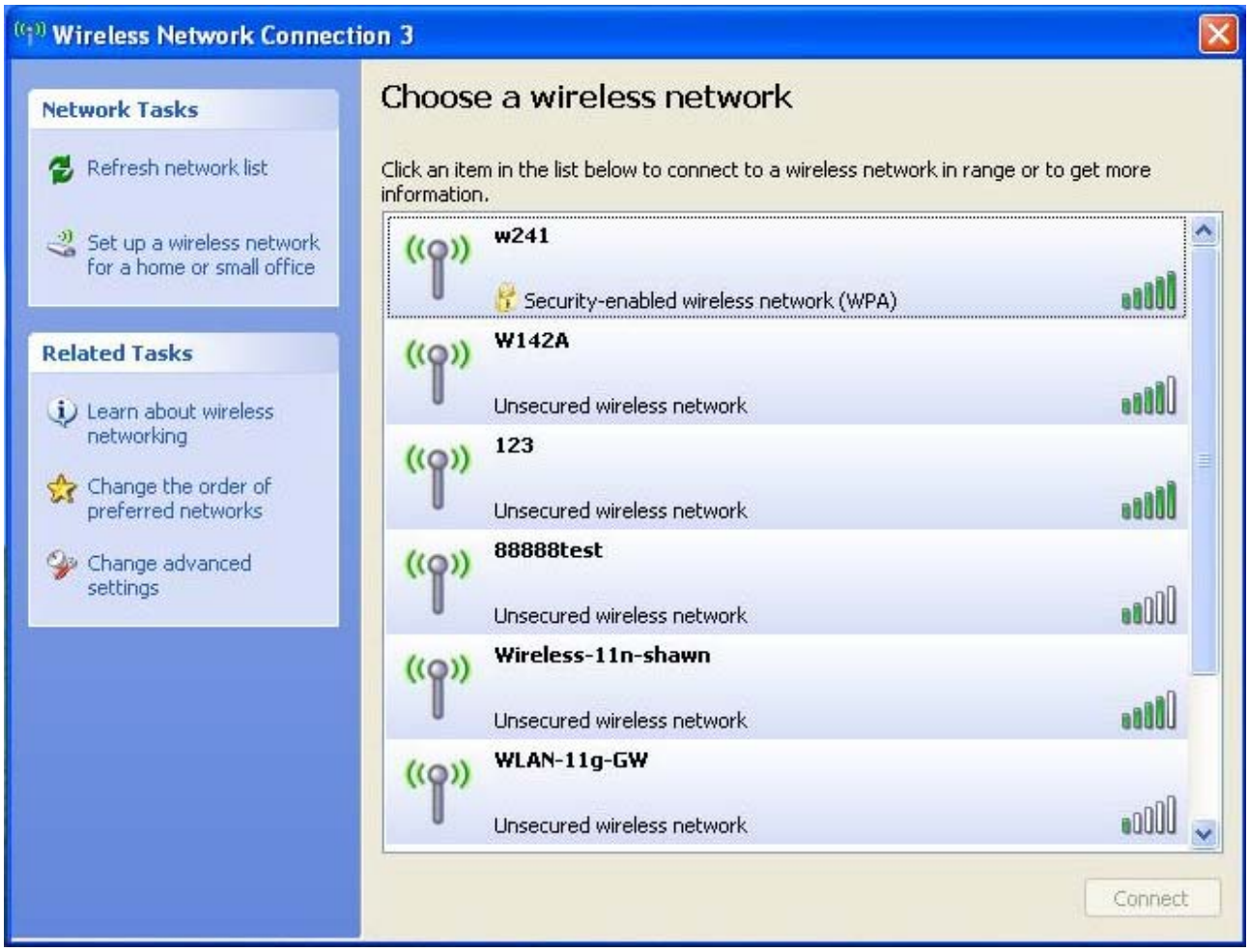
Note:

You could use either the software we provide or Microsoft Zero Configuration tool to configure this adapter.

3.1.2 To connect with Microsoft Zero Configuration tool

After specifying the Microsoft Zero Configuration tool to configure your wireless network, right click on the  icon on system tray. Select "View Available Wireless Networks" to specify your wireless network.

The tool shows the available wireless networks. Select your demanding network to connect with. To connect to a wireless network, please click **Change advanced settings** to be compatible with your wireless network settings.

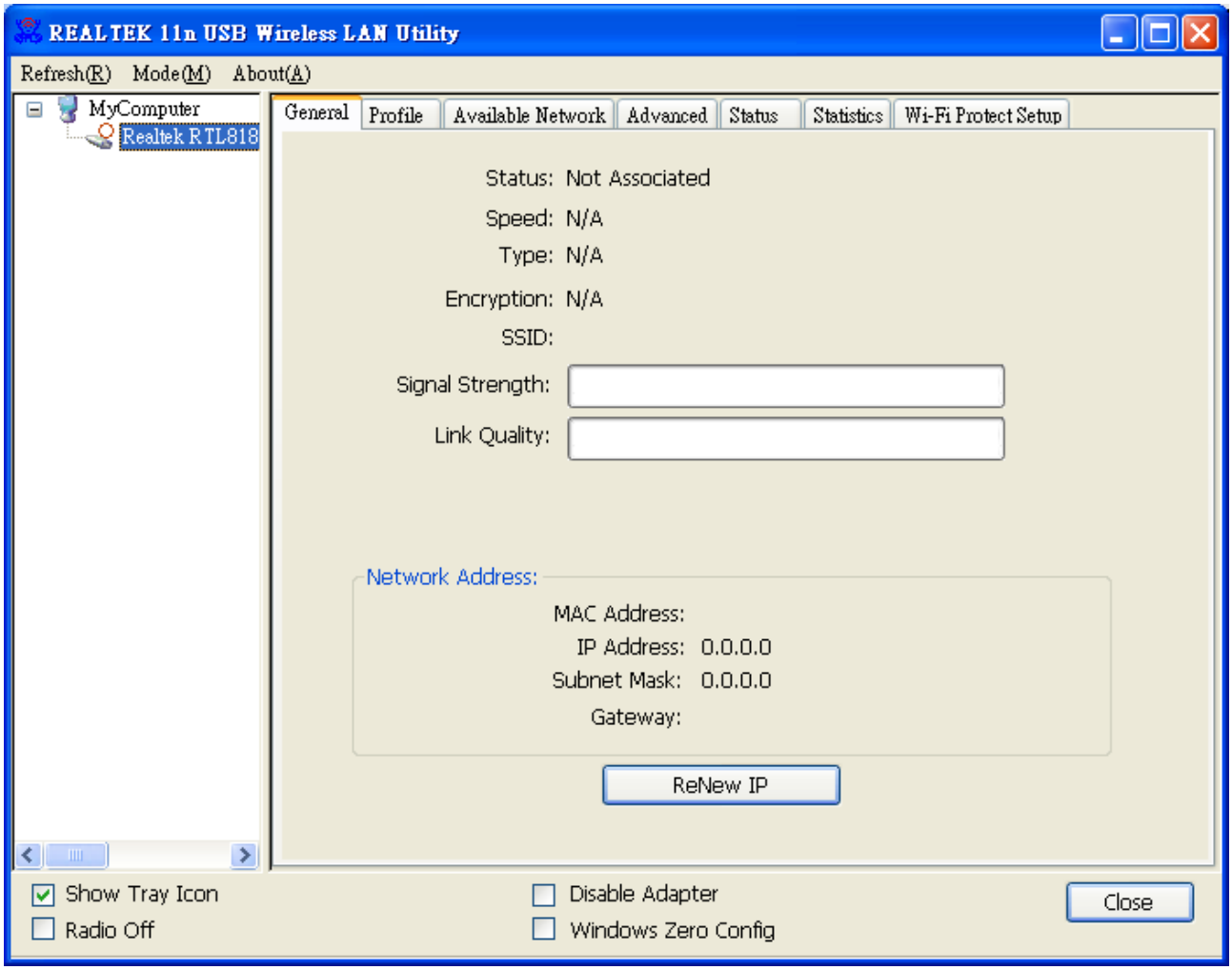

Wireless Network Connection 3
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
w241
Security-enabled wireless network (WPA)
W142A
Unsecured wireless network
123
Unsecured wireless network
88888test
Unsecured wireless network
Wireless-11n-shawn
Unsecured wireless network
WLAN-11g-GW
Unsecured wireless network
Connect

3.2 Introduction to the 802.11n Wireless LAN Utility

Note: The Utility in Linux and Mac are different from the following.

3.2.1 Interfaces

After the driver installation, the icon  will appear on your desktop. Double click this icon and the following interface appears:



1. **Functional Buttons**: on top of the window. You can click each button to access each configuration window.

2. **Configuration Column**: Center of the Utility window. Make your changes for each function in this part.

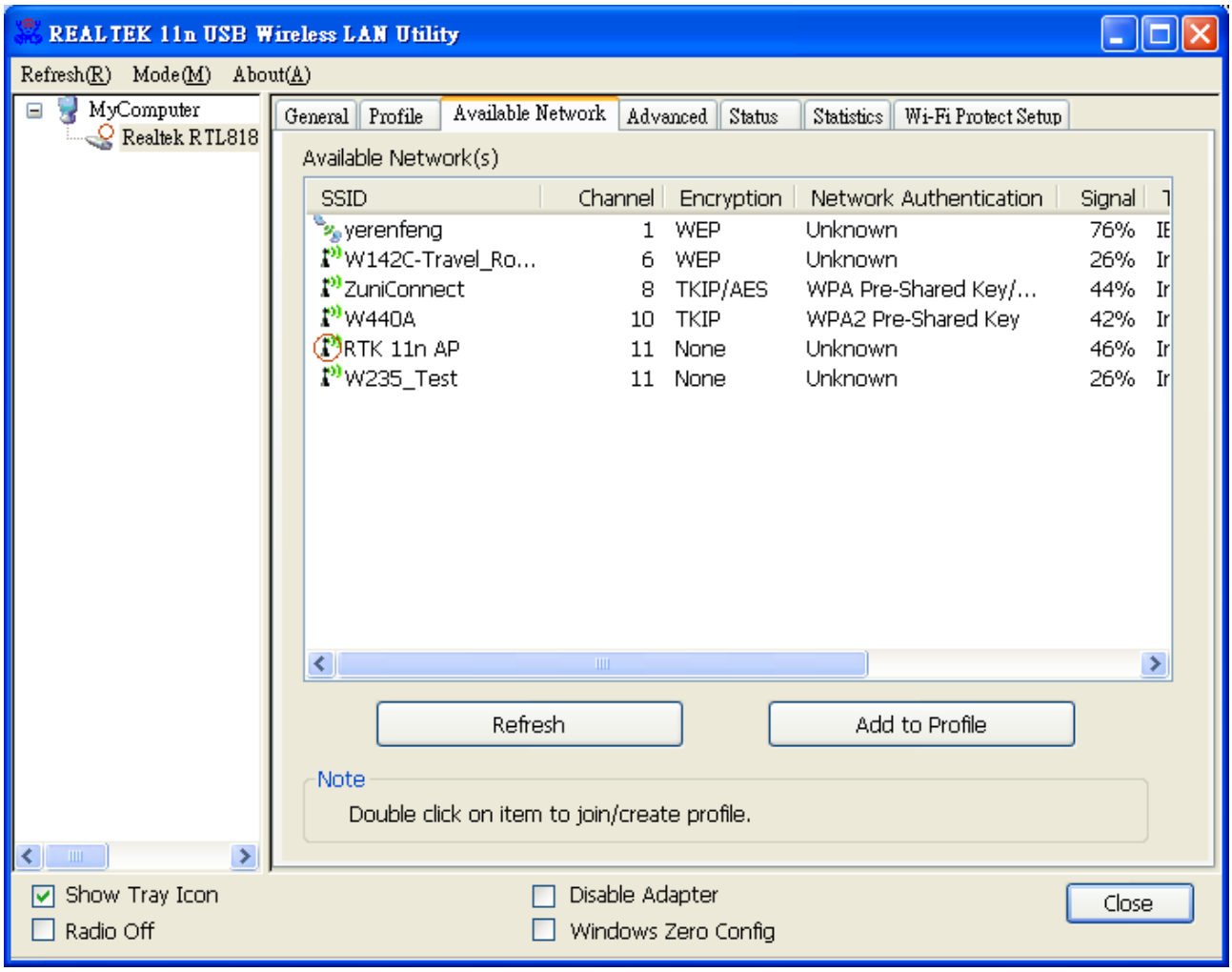
3. **Optional Table**: “Show Tray Icon”, “Disable Adapter”, “Radio off”, “Windows Zero Config”

A. Show Tray Icon---Clicking "Show Tray Icon" and “Close” button, the management GUI will be minimized and stay on the tray icon located at the right bottom corner of Windows. If not, management GUI will shut down by only click "Close" button with unchecked condition.

B. Disable Adapter---Disable this wireless PCI card.
C. Radio off---It can save power while turning off the radio. While the radio is off, the links with other wireless network will be disconnected. User should be aware that while the wireless configuration is in AP mode. Radio Off will cause the sub network belonging to the AP to be disconnected with internet.
D. Windows Zero Config---External Configuration: select this item will enables you to disable the WLAN Station Configuration Utility and indicates that the station driver is to be configured with Windows XP's built-in Zero Configuration Utility. This item is only displayed on windows XP systems.
-

3.2.2 Available Network

This network lists the available wireless networks. The Utility connects to a wireless network with best signal strength automatically. You can refresh the connecting network by clicking on the network name and click the **Refresh** button. In the center of the Utility windows, you will see detail information of each network.



Available Network Information:

Items	Information

SSID	The name of the IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
Channel	Display current channel in use.
Encryption	Shows the encryption mode in use. There are total 4 modes: None, WEP, TKIP and AES.
Network Authentication	Shows the authentication mode in use.
Signal	This percentage shows the strength of the signal.
Type	The type of network and the station currently connected are shown here. The options include : • **Infrastructure -** All wireless clients will connect to an access point or wireless router. • **Ad-Hoc -** Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless adapters.
BSSID	The IEEE MAC address of locally-managed, generating from a 46 random code.
Support Rates	Show current rate

Note:

1) An Infrastructure network contains an Access Point or wireless router. All the wireless devices or clients will connect to the wireless router or access point.

2) An Ad-Hoc network contains only clients, such as laptops with wireless desktop adapters. All the adapters must be in Ad-Hoc mode to communicate.

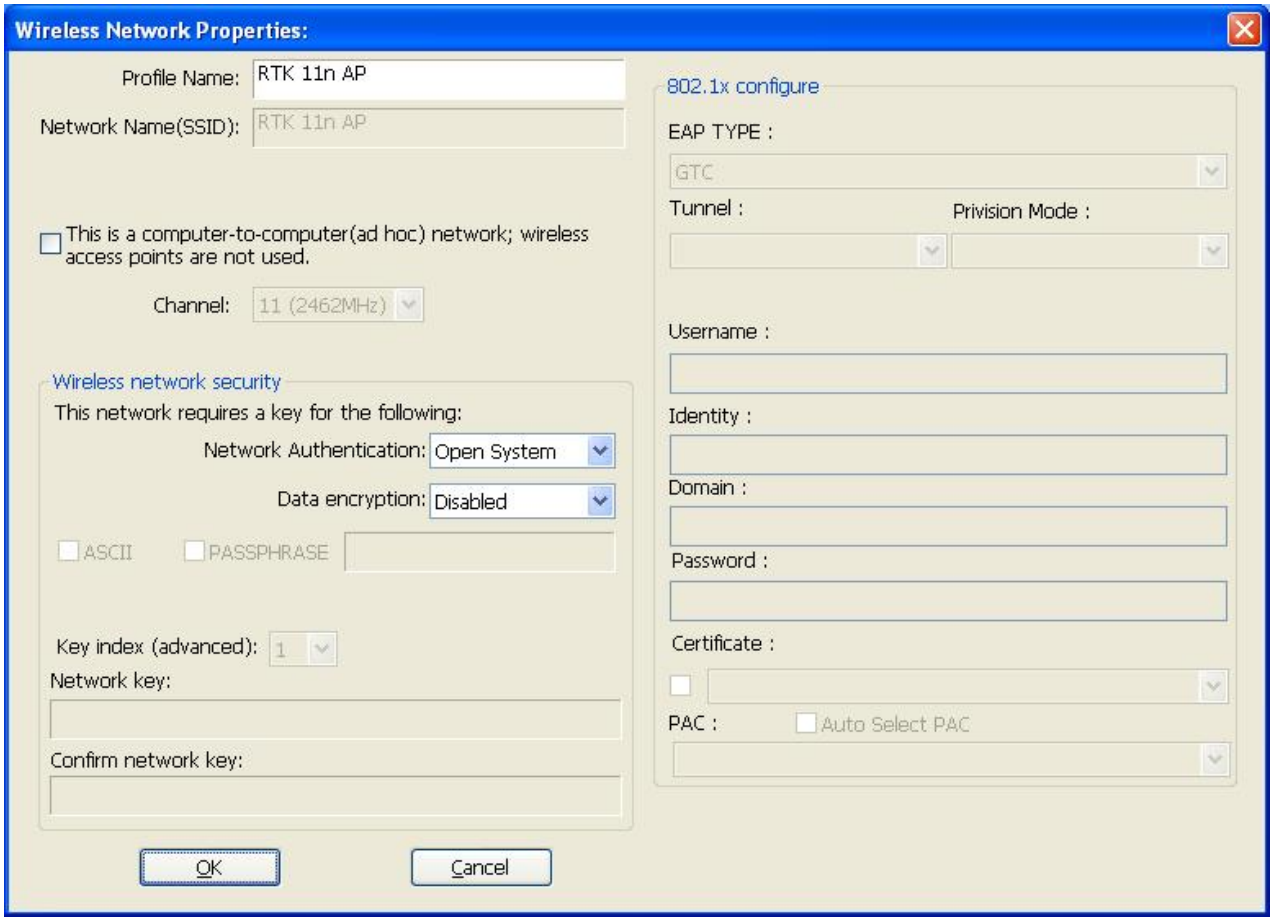
3.2.3 Profile

1. Add a new profile:

(1) Selecting an available network in the "**Available Network**" function then click the **Add to Profile** button., or double click the network name. You could also add a new profile quickly by clicking the **Add** button in the "**Profile**" function.

Note: If the network you add to profile is not encrypted, "Unsecured network" window will pop up, then Click "OK".

(2) It displays “Wireless Network Properties” dialog box. This profile page allows users to save different wireless settings, which helps users to get access to wireless networks at home, office or other wireless network environments quickly.



In this dialog box, there are some items:

Items	Information
Profile Name	Identifies the configuration profile .This name must be unique. Note that the profile names are not case-sensitive. (You can enter the Profile name by “Add”, but you could only use the default name by “Add to profile”.
Network Name(SSID)	The IEEE 802.11n wireless network name, using default name defined by system. This field has a maximum limit of 32 characters.

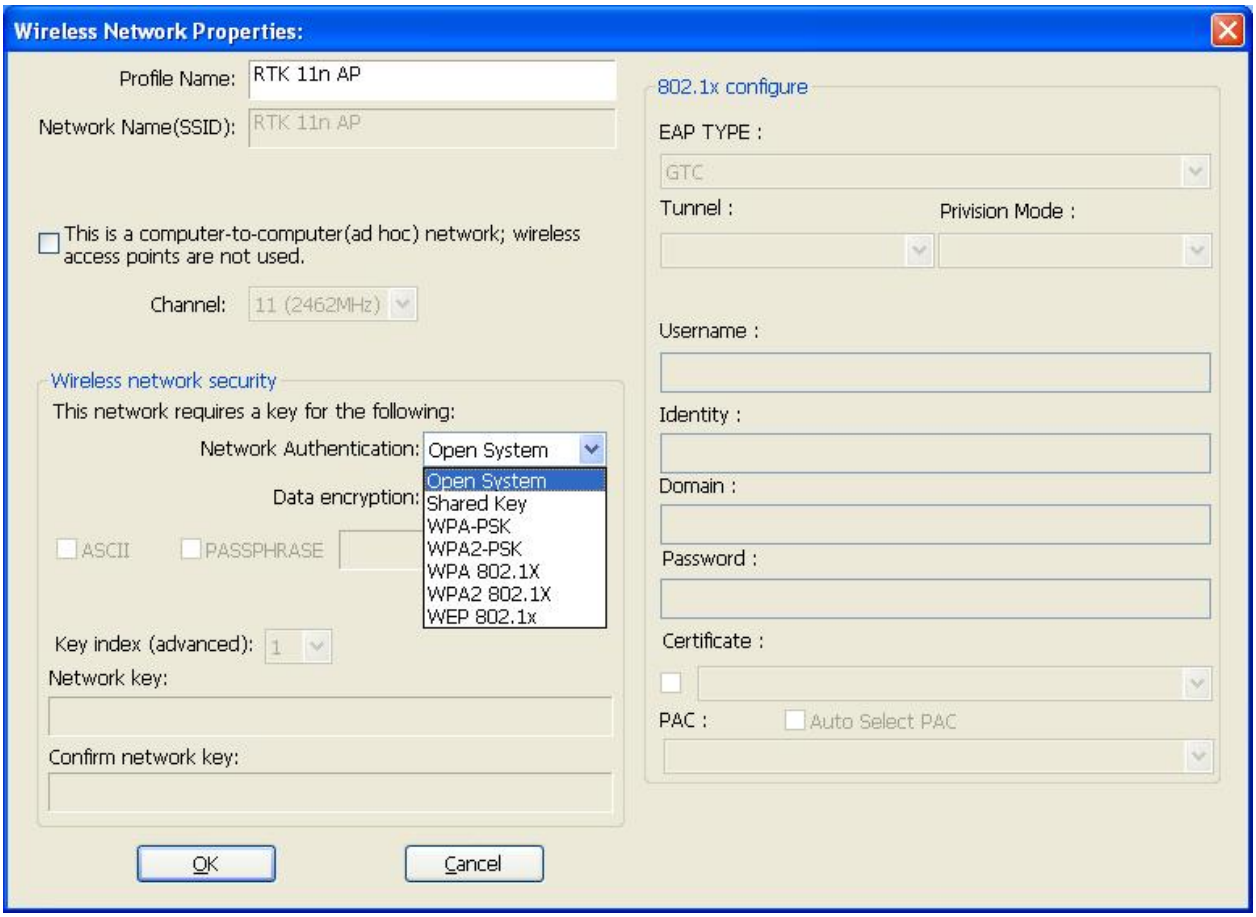
(3) Channel (Country Region Code): six countries to choose. Country channel list:

Country	Channel Range	Country	Channel Range
SPAIN	CH1 ~ CH11	FRANCE	CH1 ~ CH13
CANADA	CH1 ~ CH11	JAPAN	CH1 ~ CH14
ETSI	CH1 ~ CH13	ISRAEL	CH1 ~ CH13

(4) Wireless Network Security

A. Network Authentication

There are 7 types supported: Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X, WEP 802.1X. Please select a type from the drop down list. Select the Security tab in the screen above. To define the security mode, select the desired security mode as follows.



- **Open System:** enable an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match.
- **Shared-key:** only allows the adapter to associate with access points that have the same WEP key.
- **802.1x:** This item appears while the environment is set to an open authentication with WEP encryption. The section is also available in WPA and WPA2 authentication types.

- **Preshared Key (PSK):** This is the shared secret between AP and STA. For WPA-PSK, WPA2-PSK and WPA-NONE authentication mode, this field must be filled with characters longer than 8 and less than 32 lengths. The following dialog appears if you have input invalid values.
- **WEP Key:** Only available when using WEP encryption algorithm. The key must match AP's key. Only using the same cryptographic key to access the computer, the internet can storage, and decryption the information from other computer.

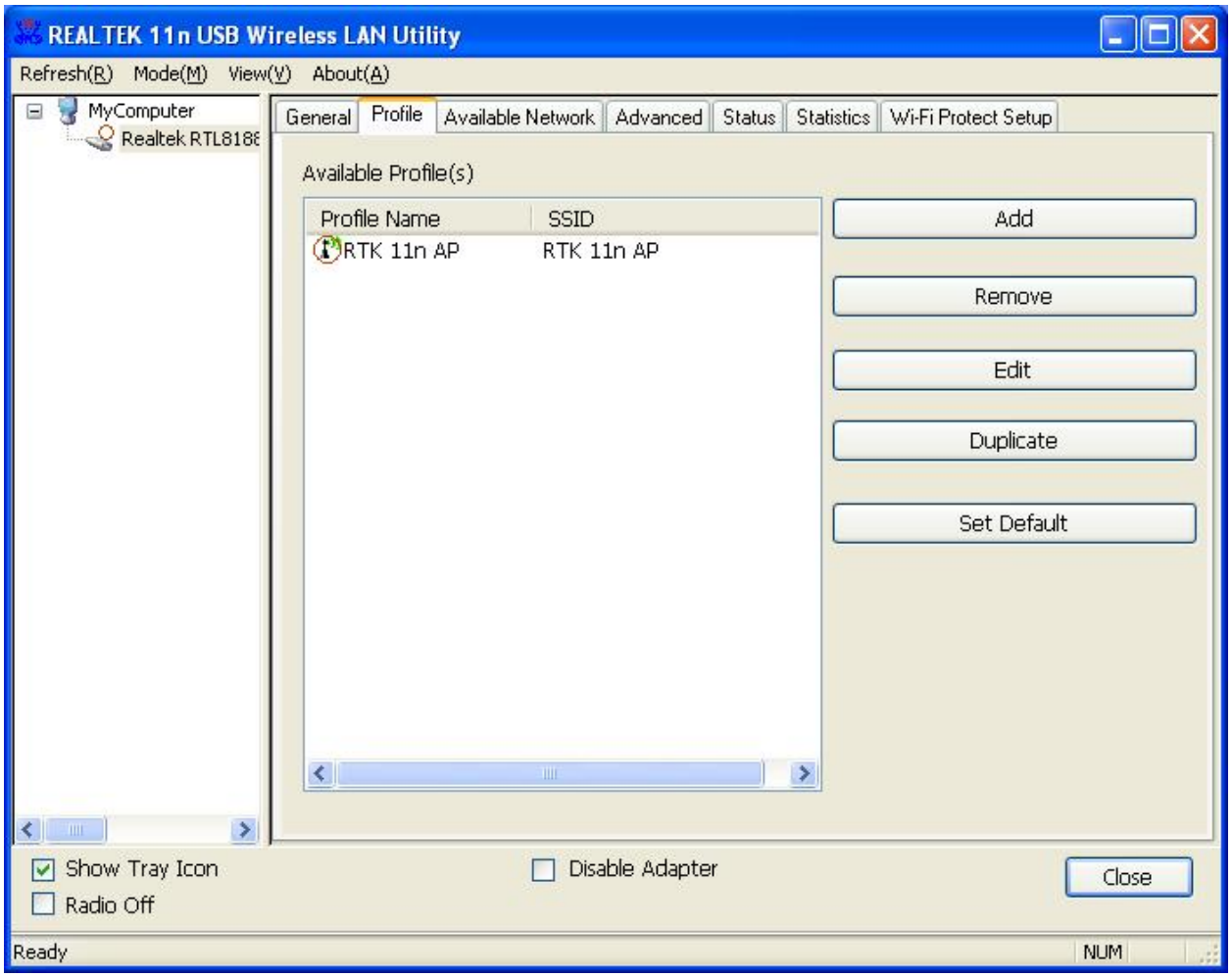
B. Data Encryption:

<table>
<tr><td>Data encryption</td><td>There are 4 types supported: Disabled, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open System</td><td>Disabled, WEP</td></tr>
<tr><td>Shared Key , WEP 802.1X</td><td>WEP</td></tr>
<tr><td>WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X</td><td>TKIP, AES</td></tr>
</table></td></tr>
</table>

Note: Select different Security Options, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

- **TKIP:** "Temporary Key Integration communication Protocol", it provide each packet's key mixture, message integration and key reconstruction mechanism. TKIP can use with personal or the enterprise network validation.
- **AES:** “Advanced Encryption Standard”, it is a new method that the wireless transmission of privacy protection. AES encryption methods is more careful than TKIP.

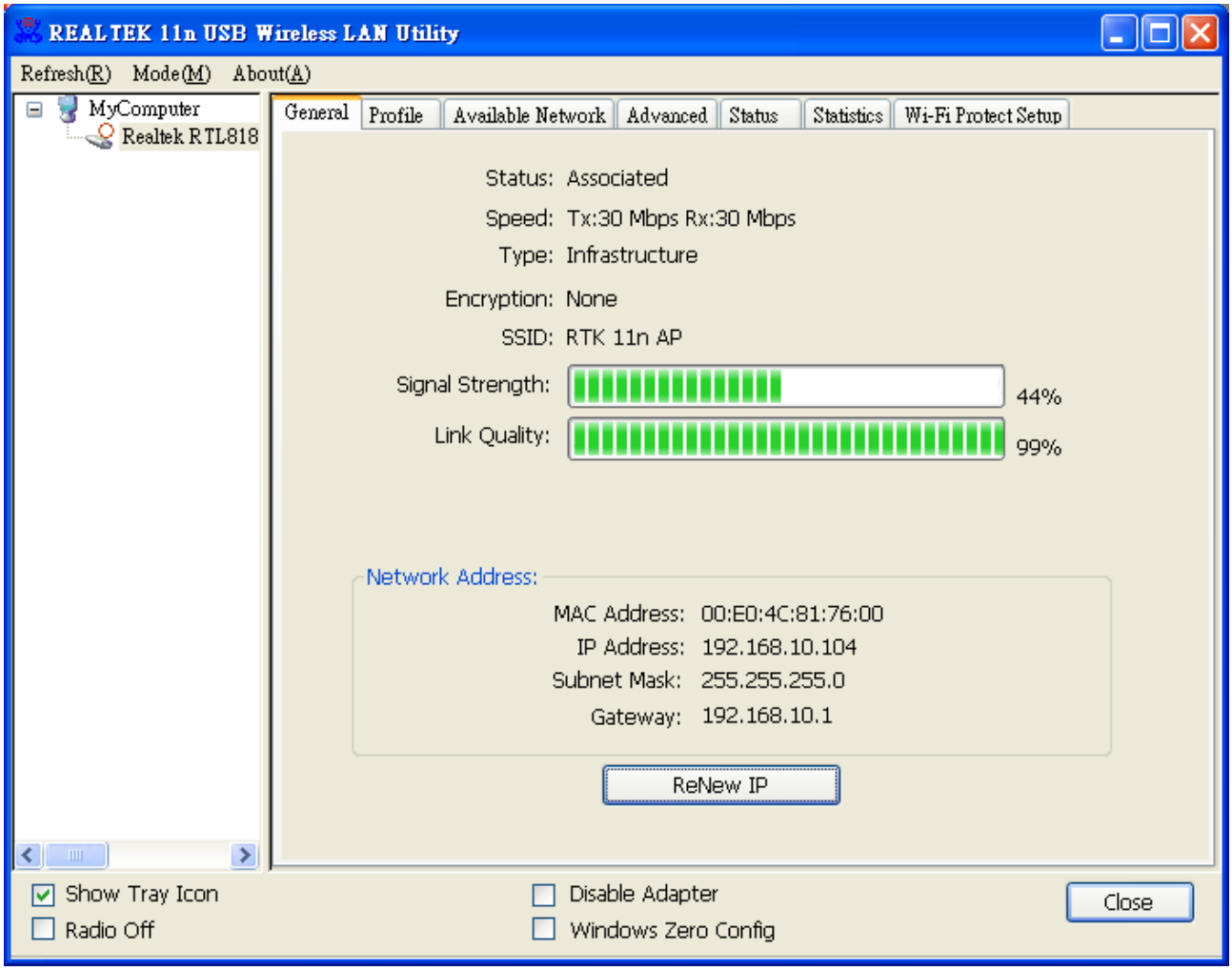
(5) Finish the configuration, then click “OK”, that network has been added to the profile.



Profile List: The list shows all the profiles you have added before.

Buttons: You can click on these buttons to **Add** a new profile, **Remove**, **Edit**, **Duplicate** or **Set Default** an old profile.

3.2.4 General



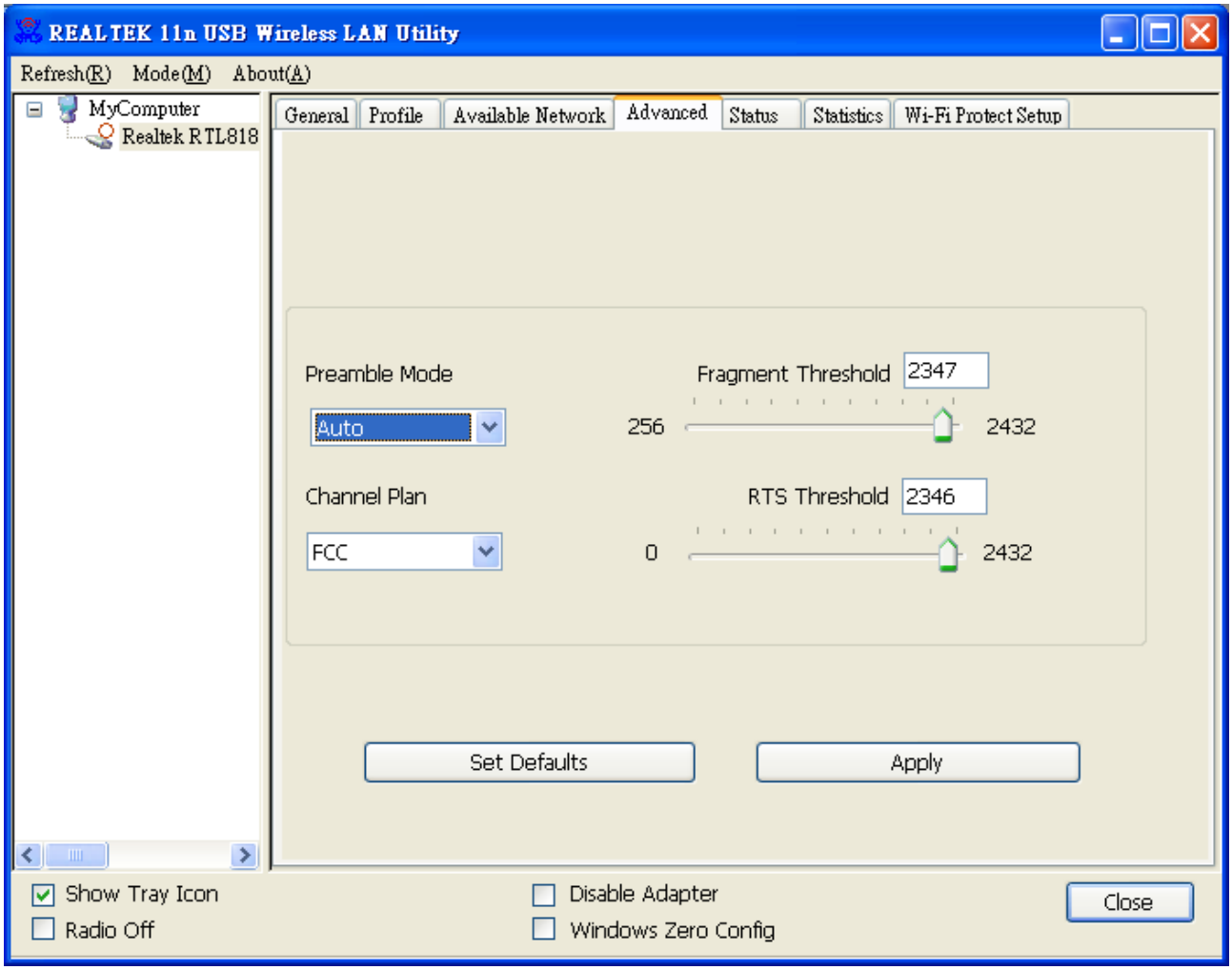
In this window, there are some items as following:

Items	Information
Status	Currently connection status.
Speed	Show current transmit rate and receive rate.
Type	Network type in use.
Encryption	Encryption type in use.
SSID	The name of the IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
Signal Strength	Receive signal strength.
Link Quality	Display connection quality based on signal strength.
Network Address	A. MAC Address: The MAC address of the wireless network adapter. B. IP Address: IP address of current connection.

	C. Subnet Mask: Subnet mask of current connection. D. Gateway: Gateway of current connection.

3.2.5 Advanced

This screen below allows you to make advanced configuration for the profile. Please refer to the following chart for definitions of each item.



1. Preamble Mode

The length of CRC blocks in the frames during the wireless communication. Select the options from the drop list : (1) Long (2)Short (3)Auto.

2. Channel Plan

The selected Channel: FCC, IC, ETSI, Spain, France, MKK, MKK1, Israel, TELEC, Default.

(Note: The choose between channels function is not allowed in USA.)

3. Threshold

(1) Fragment Threshold

This value should remain at its default setting of 2347. If you experience a high packet error rate,

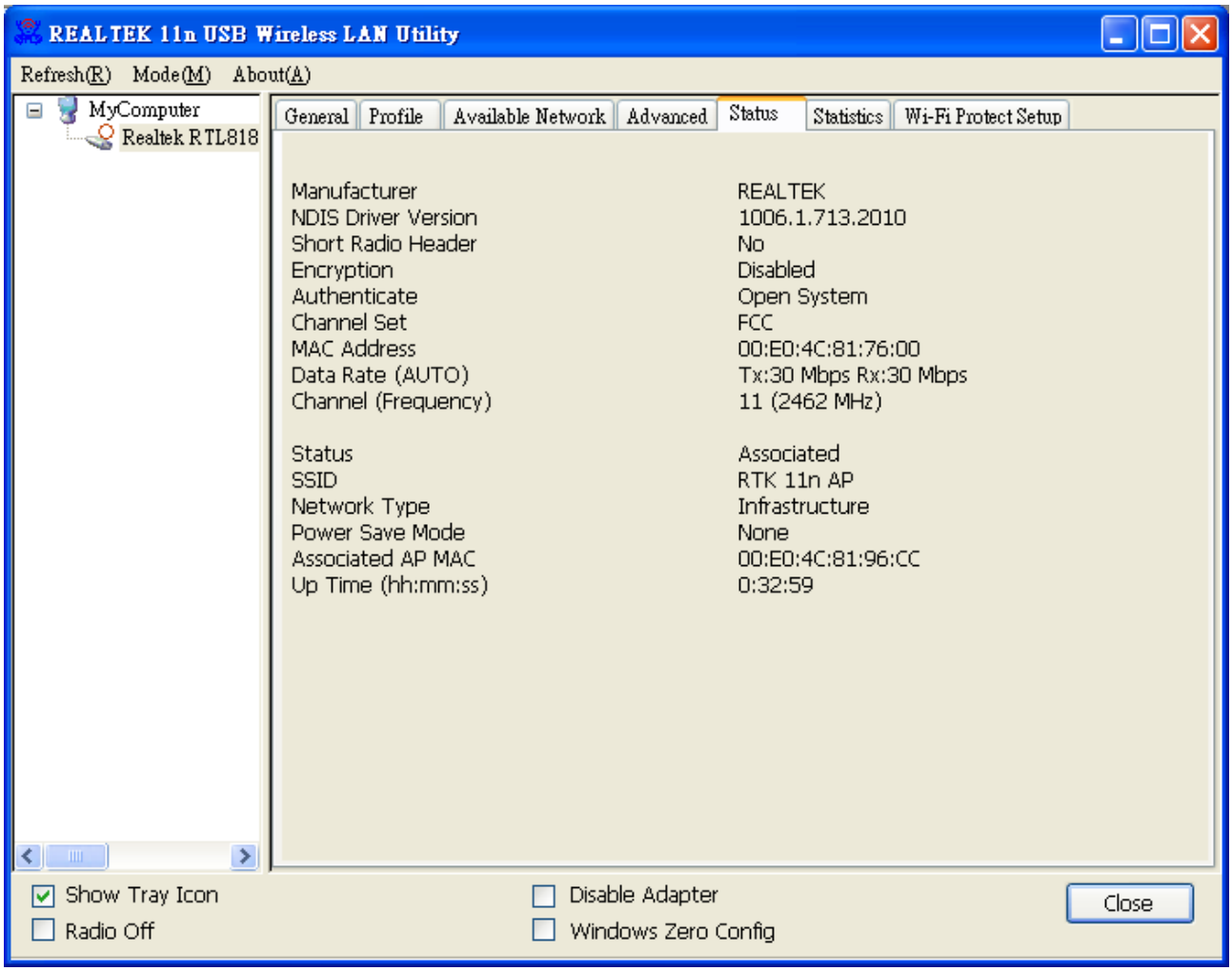
you may slightly increase your fragmentation threshold within the value range of 256 to 2432. Setting the fragmentation threshold too low may result in poor performance.

(2) RTS Threshold

Request To Send threshold. This value should remain at its default setting of 2346. If you encounter inconsistent data flow, only minor modifications to the value range between 0 and 2432 are recommended.

3.2.6 Status

The Status tab contains general information about the program and its operations. The current Status tab needn't any configurations.



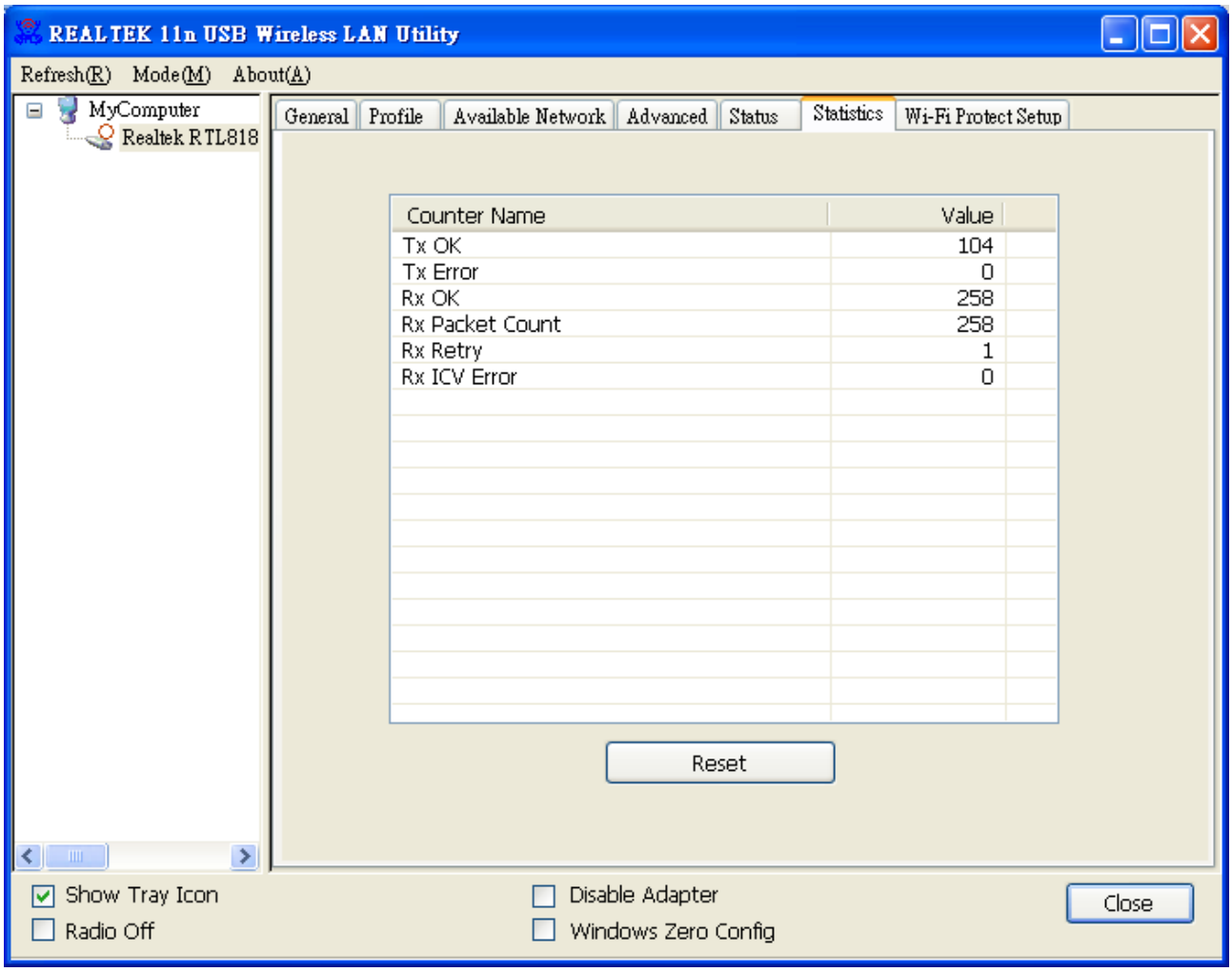
The following table describes the items found on the Status screen.

Items	Information
Manufacturer	The name of manufacturing this product.
NDIS Driver Version	The version of Network Driver Interface Specification.

Encryption	Here displays the encryption type the device is using.
Authenticate	This shows whether the server based authentication is used.
Channel Set	Appears the country you use.
MAC Address	The MAC address of the wireless network adapter.
Data Rate(Auto)	Show current transmit rate and receive rate.
Channel Frequency	Shows the channel in use (1~14).
Status	Current connection status.
SSID	The SSID of the wireless system.
Network Type	The type of network and the station currently connected are shown here. The options include : Infrastructure, Ad Hoc
Power Save Mode	The power save mode have three mode, as follows : • **Max -** Selects maximum mode to let the access point buffer incoming messages for the Adapter. The Adapter will detect the access point if any messages are waiting periodically. • **Min –** Min mode uses minimum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets. • N**one -** Turns power saving off, thus powering up the Wireless USB Adapter continuously for a short message response time.
Associated AP MAC	The MAC Address of associated AP.
Up Time	Record life time.

3.2.7 Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates the MIB counters into a format easier for user to understand. It show receiving and transmitting statistical information about the following receiving and transmitting diagnostics for frames received by or transmitted to the wireless network adapter.

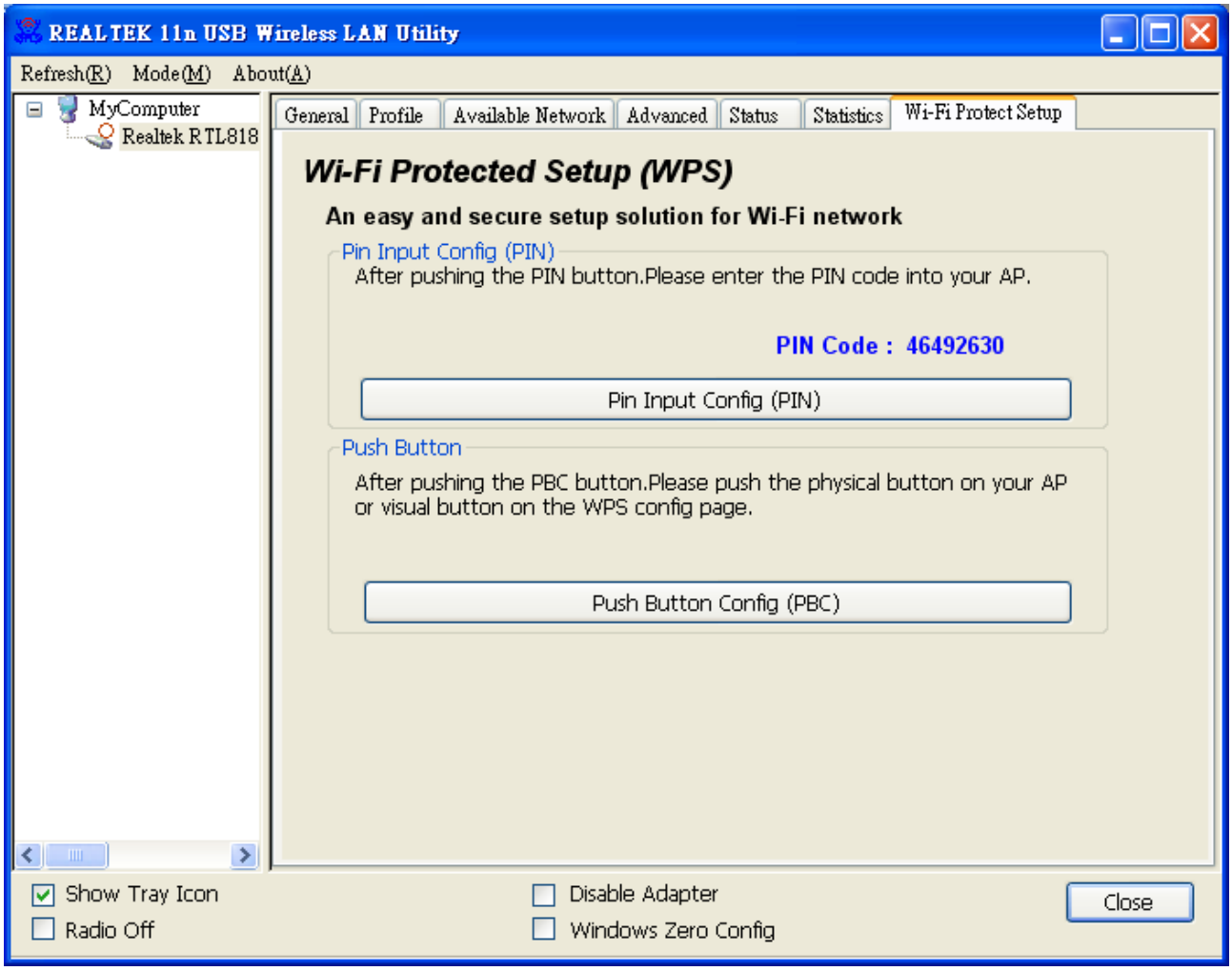


Items	Information
TX OK	Successfully transmitted frames numbers.
TX Error	Frames numbers transmitting with error.
RX OK	Successfully received frames numbers.
Rx Packet Count	The packets of receiving frames.
RX Retry	Frames numbers re-receiving.
RX ICV Error	Integrity Check Value receiving with error.
Reset Counter	Reset counters to zero.

3.2.8 Wi-Fi Protect Setup

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This adapter supports the configuration setup using PIN configuration method or PBC configuration method. If the wireless card supports Wi-Fi Protected

Setup (WPS), you can establish a wireless connection between wireless card and router using either Push Button Configuration (PBC) method or PIN method.



Here we will introduce two ways to configure the QSS

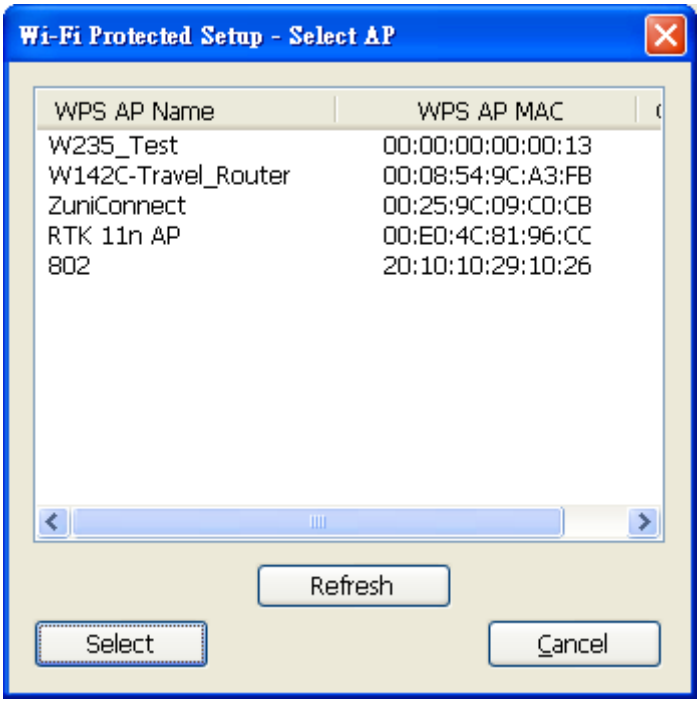
(QSS is known as rapid security settings, by pressing the wireless router and wireless card on the QSS button to automatically set up WPA2 secure connection level without the router or network adapter management software to conduct the cumbersome interface settings, greatly simplifying the operation of the wireless security settings.)

Pin Code: 8-digit numbers. It is randomly generated from system

1. PIN method

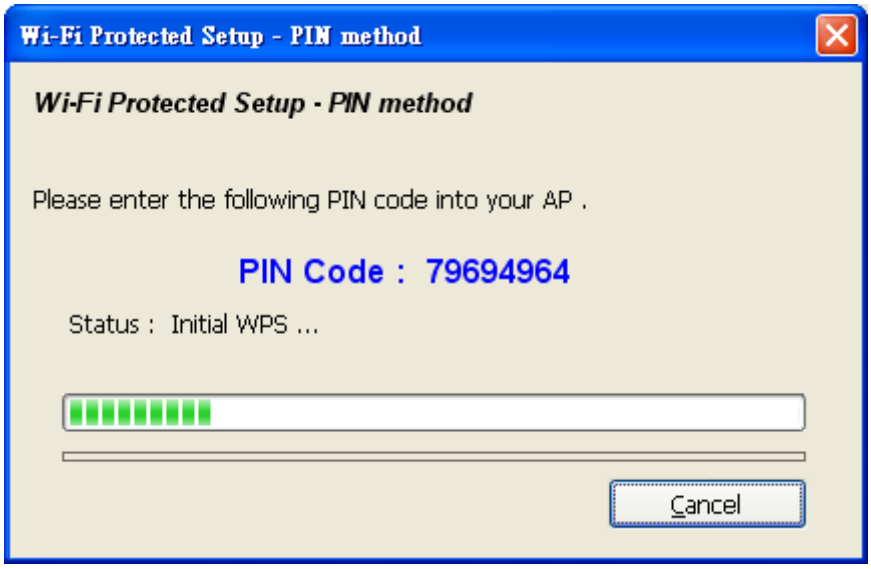
Click the button “Pin Input Config (PIN)”, and then come to the following figure.

Click the button “Yes”, you can select one of the AP.



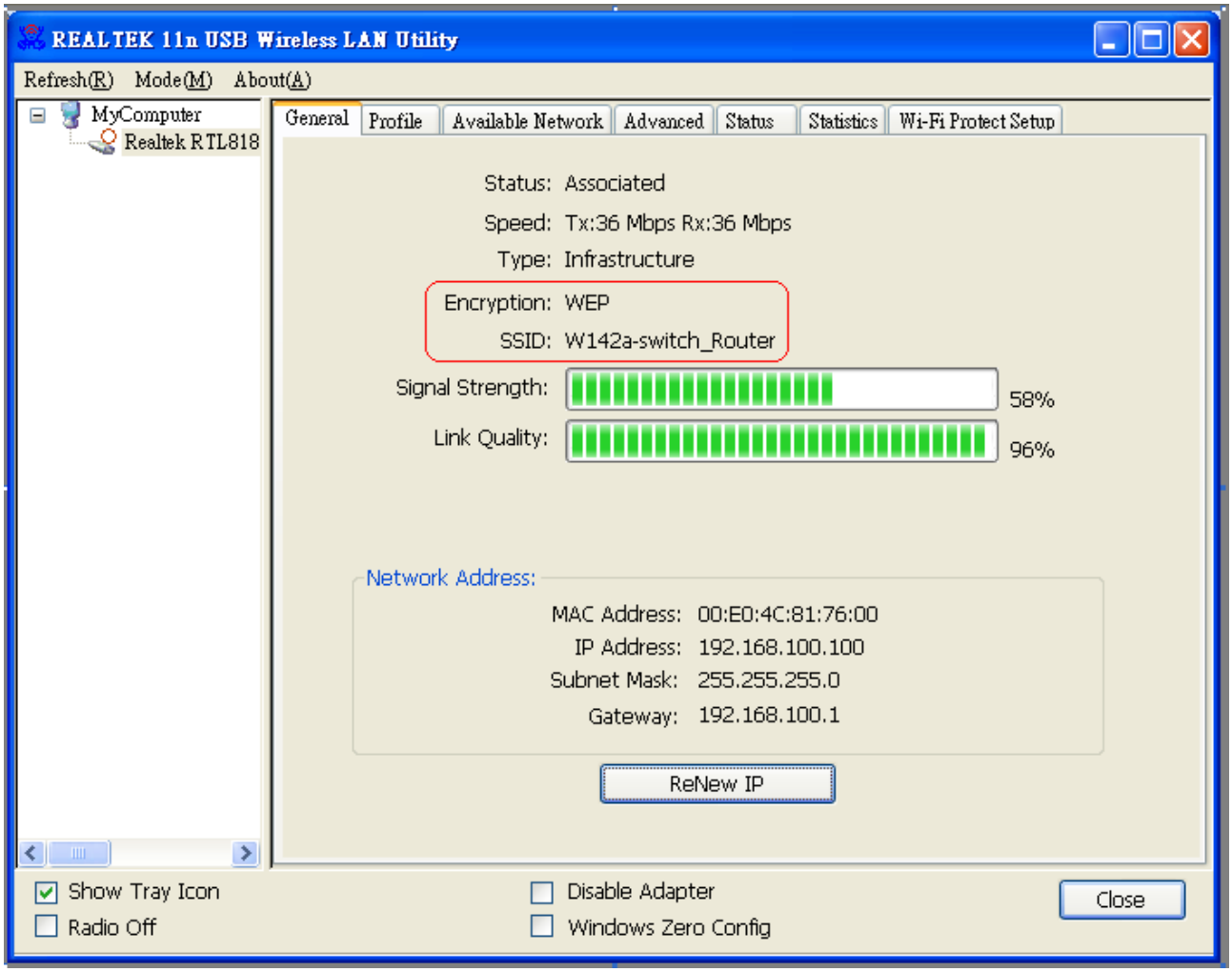
When the following interface pops up, double click the Internet WEB browser icon on your desktop screen. Type the IP address of you selected Router/AP into the URL and press “Enter”, and then you can enter the configuration.

Please enter the WPS (Wi-Fi) configuration page, type the PIN code of adapter and click confirm button to build WPS connection.



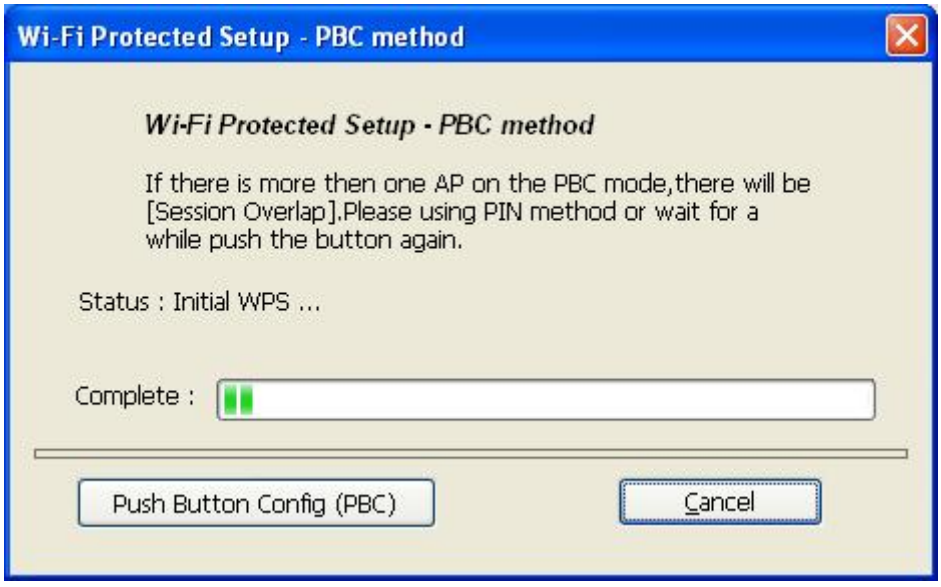
+

When the “General” window appears, WPS is configured successfully.

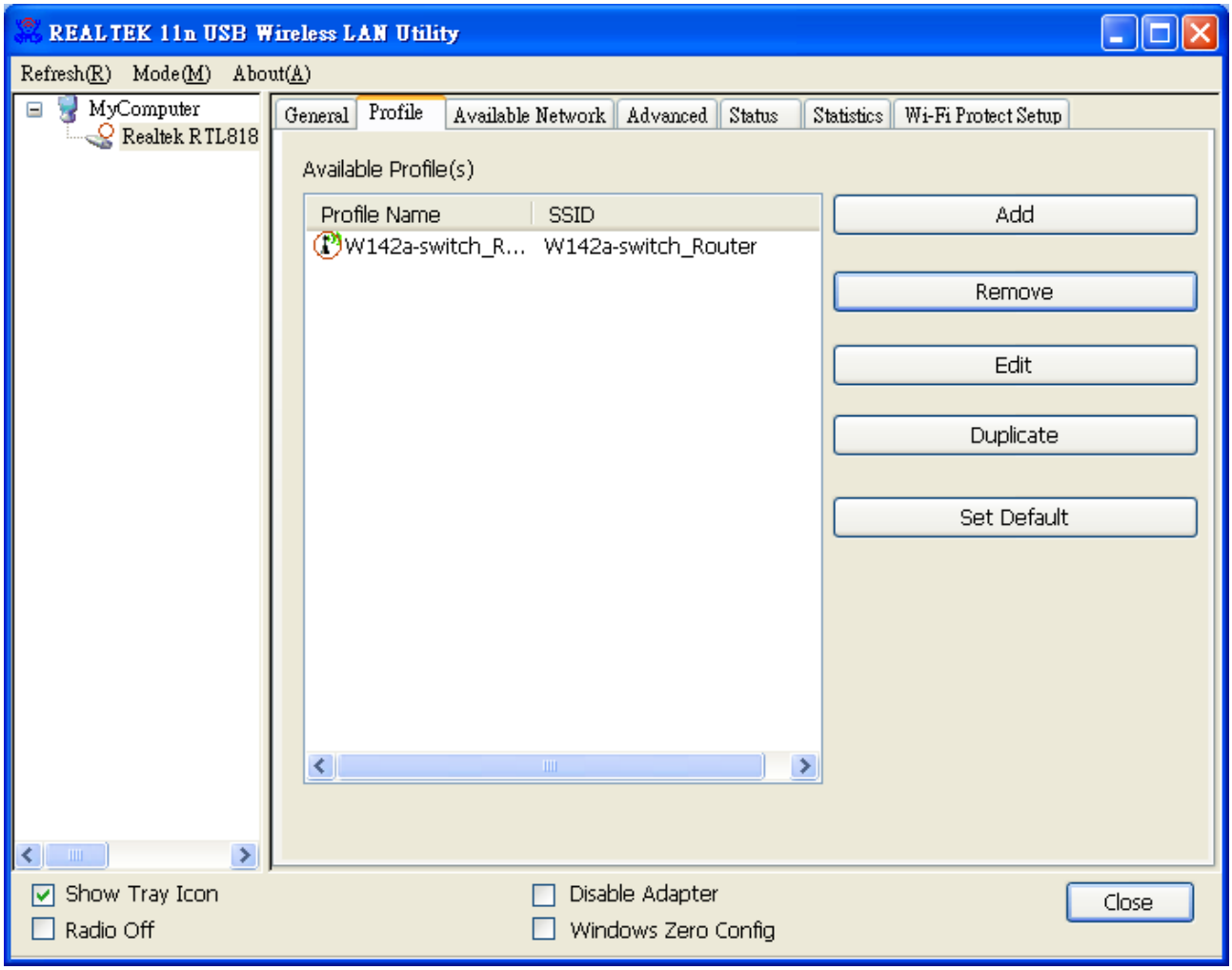


2. PBC (Push Button Configuration) method

After pushing the PBC button, please push the physical button on your AP or visual button on the WPS config page, then come to the following figure.



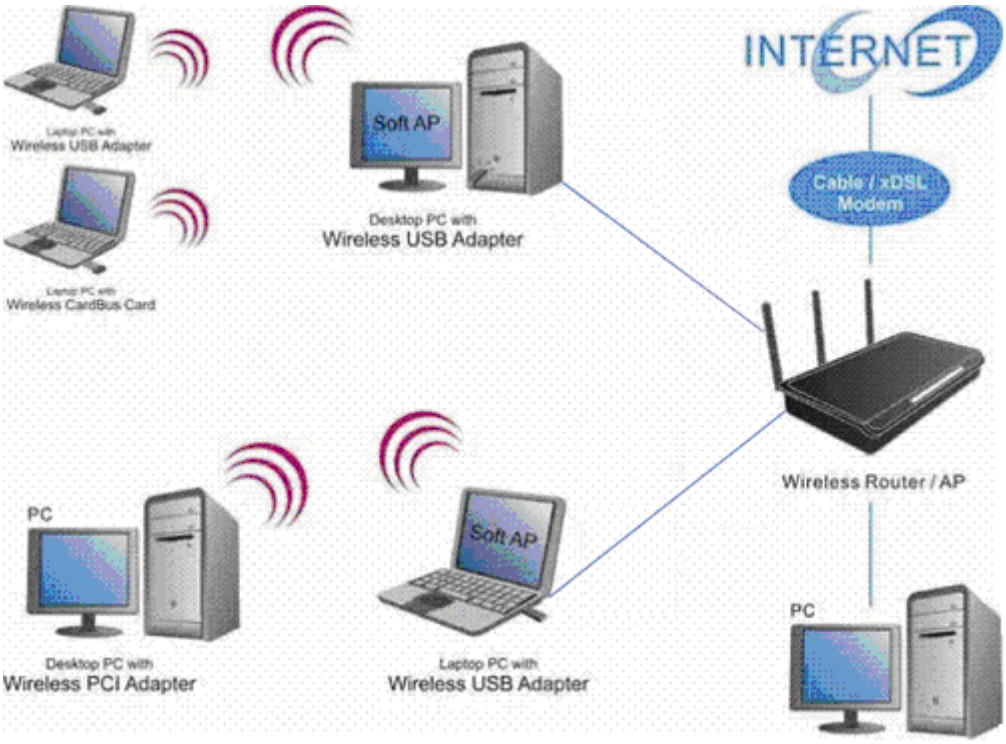
When WPS is configured successfully, the available profile(s) is changed.



3.3 AP mode management guide for Windows XP

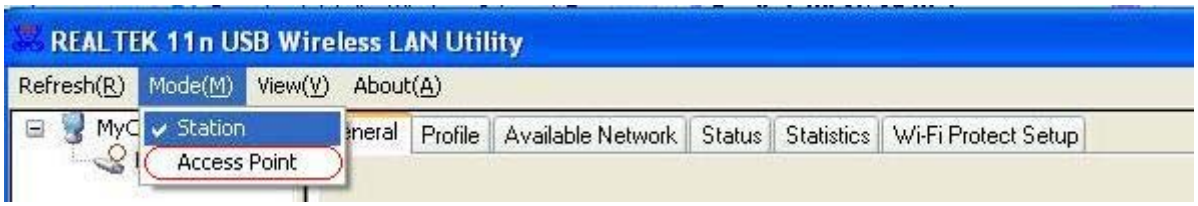
If you wish to share the Internet access with the wireless stations in your environment, you can configure this wireless adapter as a software access point (Soft AP). In this mode, this wireless adapter becomes the wireless access point that provides local area network and Internet access for your wireless stations.

3.3.1 Software Access Point (Soft AP) Application

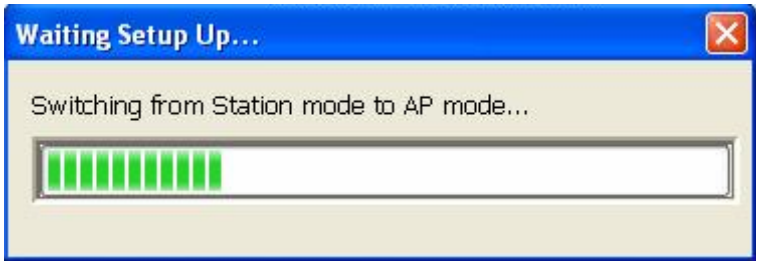


3.3.2 General

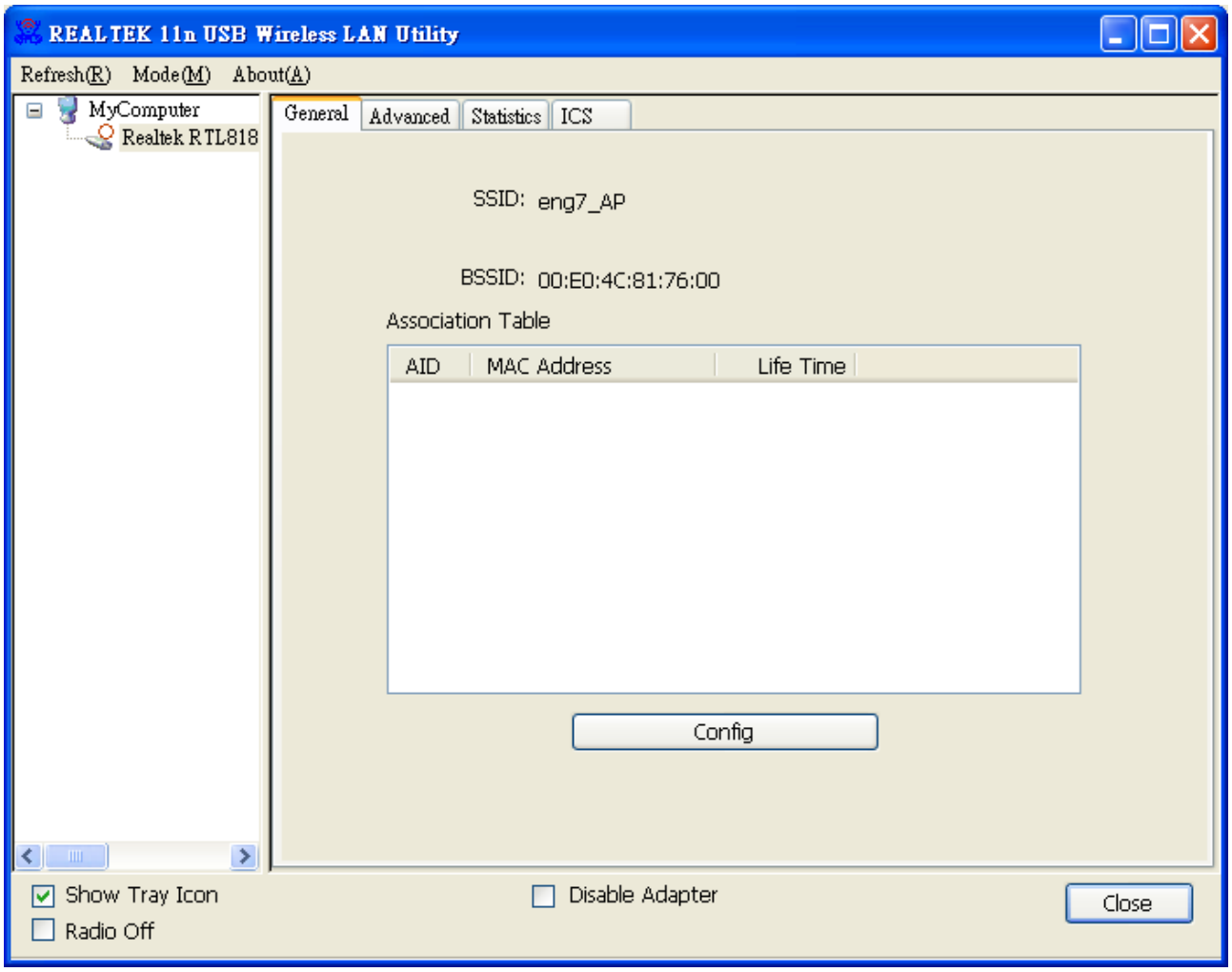
To use this adapter as an access point, please click the “Mode” on **Functional menu** and select **“Access Point”**.



Then switch from station mode to AP:



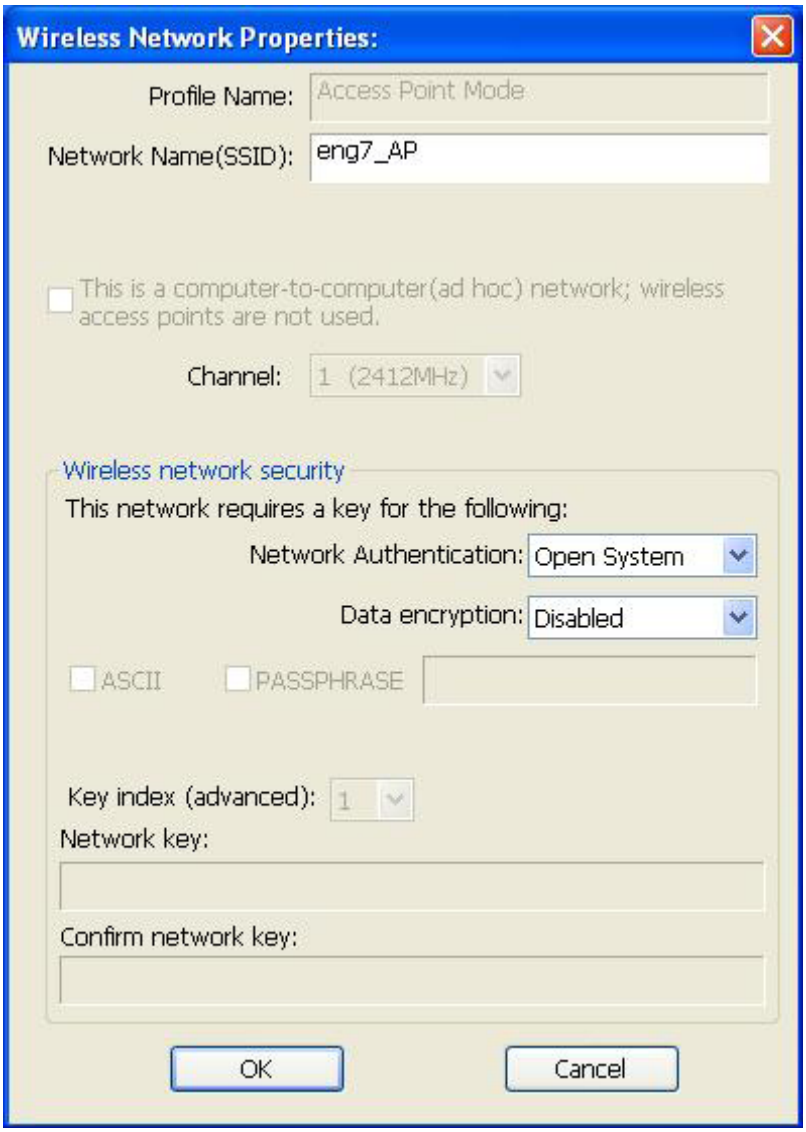
At the same time, you will find that the icon on the system tray is changed.



Please refer to the following information about this AP-mode utility.

Items	Information
SSID	AP name of user type.
BSSID	The IEEE MAC address of locally-managed, generating from a 46 random code.
AID	Raise value by current connection.
MAC Address	The station MAC address of current connection.
Life Time (mm:ss)	Record life time.

Click the “Config” button, then you can configure the wireless network properties. This page provides overall configuration to this adapter.



SSID: AP name of user type.

Channel: Manually force the AP using the channel. System default is channel 1.

Security Setting: Authentication mode and encryption algorithm used within the AP. System default is no authentication and encryption.

Cancel: Cancel the above changes.

OK: Apply the above changes.

A. Network Authentication

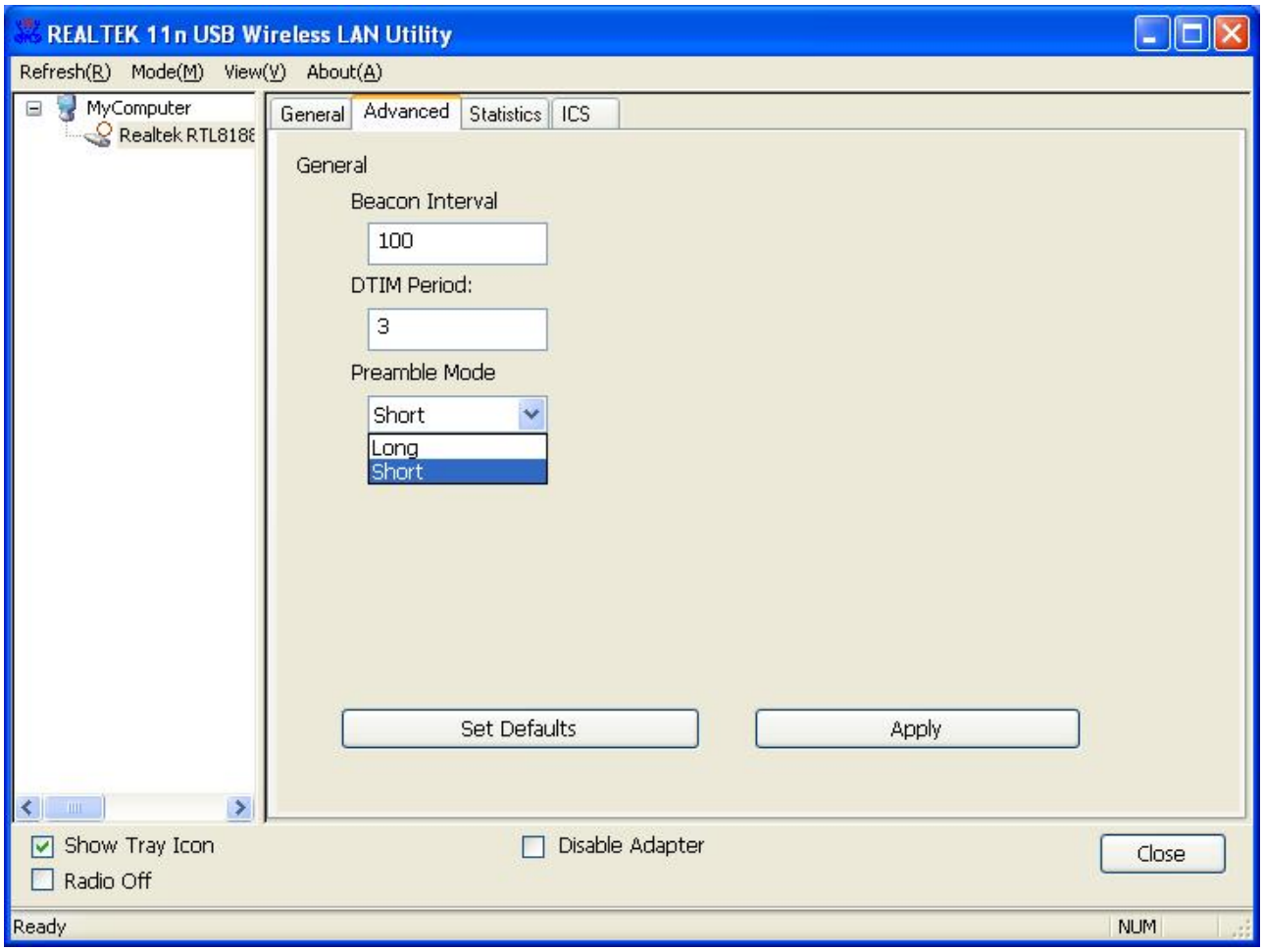
Select the Security tab in the screen above. To define the security mode, select the desired security mode as follows. There are 4 types supported: Open System, Shared Key, WPA-PSK, WPA2-PSK. Please select a type from the drop down list.

B. Data Encryption:

<table>
<tr><td>Data encryption</td><td>There are 4 types supported: Disabled, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open System</td><td>Disabled, WEP</td></tr>
<tr><td>Shared Key , WEP 802.1X</td><td>WEP</td></tr>
<tr><td>WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X</td><td>TKIP, AES</td></tr>
</table>
</td></tr>
</table>

Note: Select different Security Options, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

3.3.3 Advanced

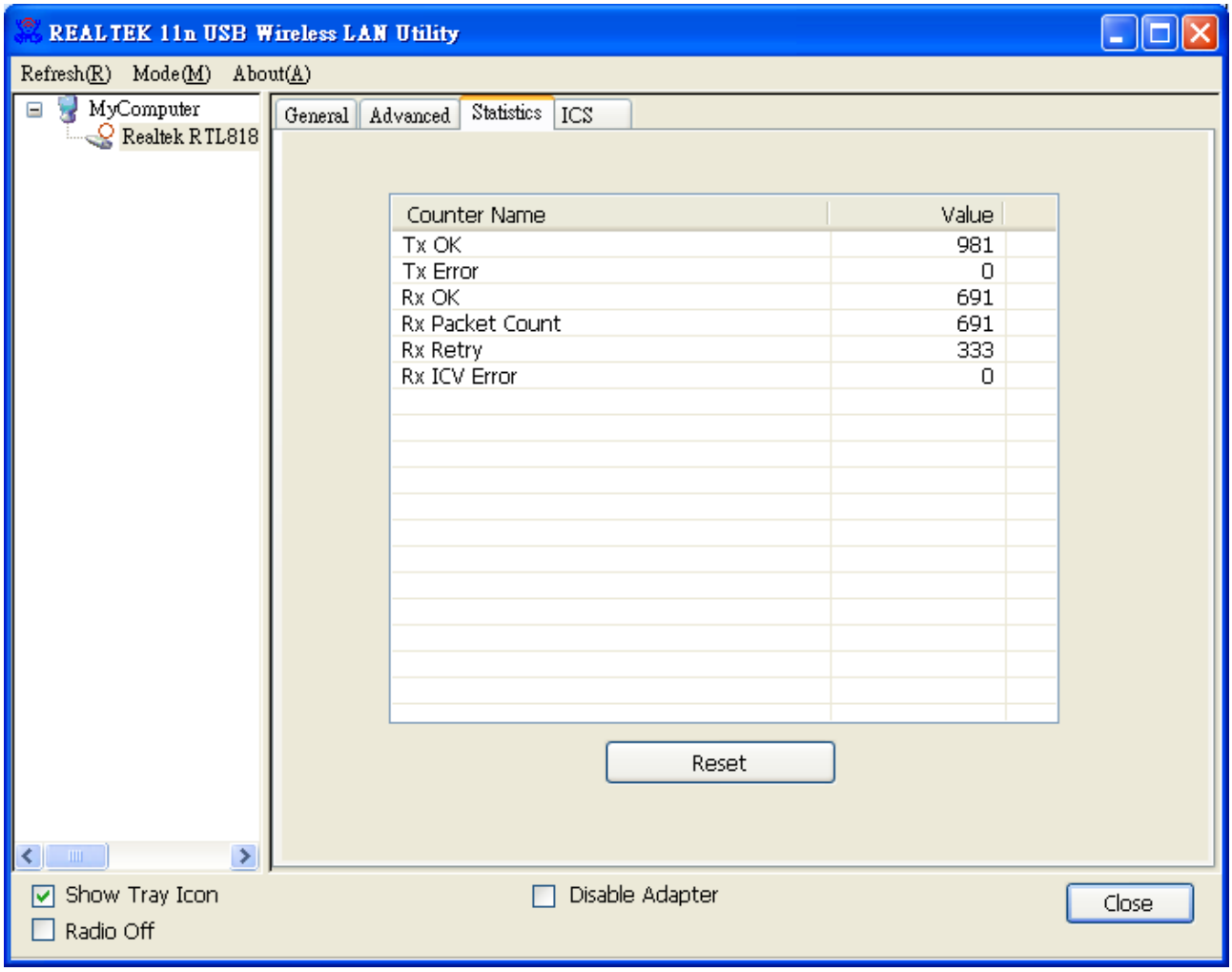


Items	Information

Beacon Interval	Beacon frequency spacing.
DTIM Period	Delay transmission indicator map (DTIM) is enabled for power management of the client. If any client power management is enabled, the DTIM should be retained for 1 (the default). Support this parameter range from 1 to 255.
Preamble Mode	Select the options from the drop list,(Long / Short).
Set Defaults	Setting the default value of General.
Apply	Apply the above changes.

3.3.4 Statistics

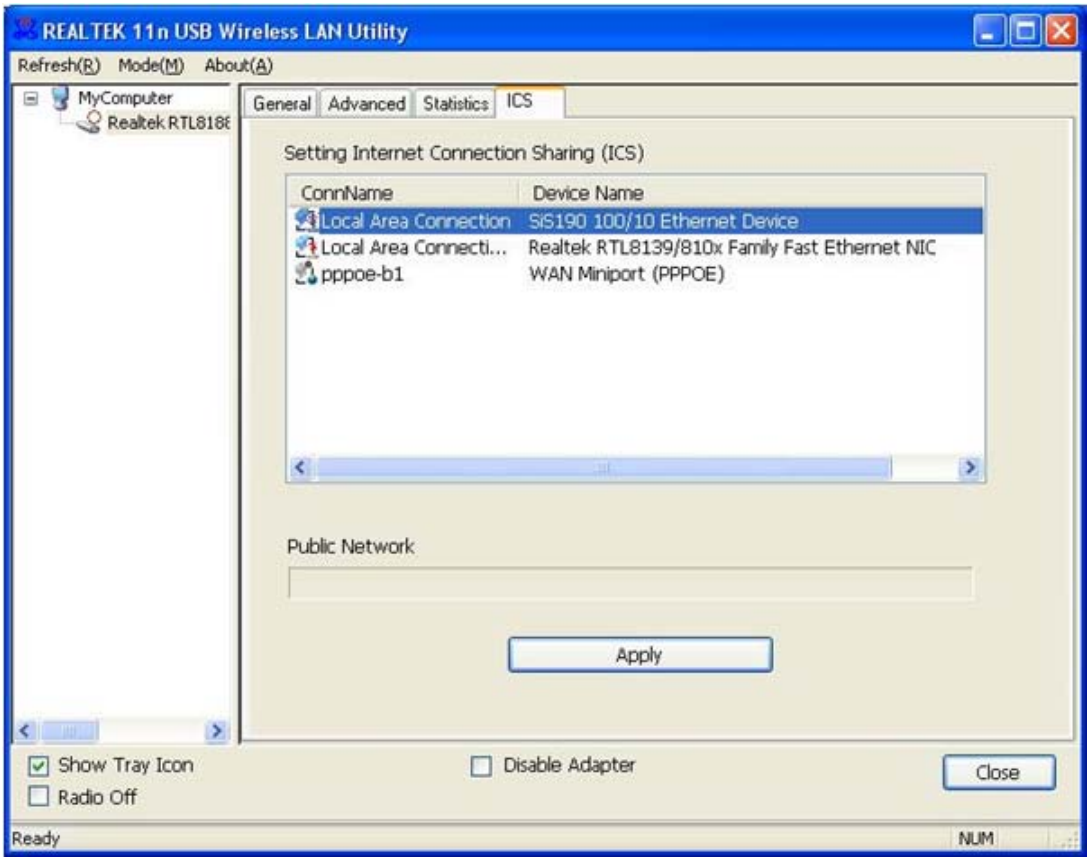
Statistics page displays the detail counter information based on 802.11 MIB counters.



Items	Information
TX OK	Successfully transmitted frames numbers.
TX Error	Frames numbers transmitting with error.

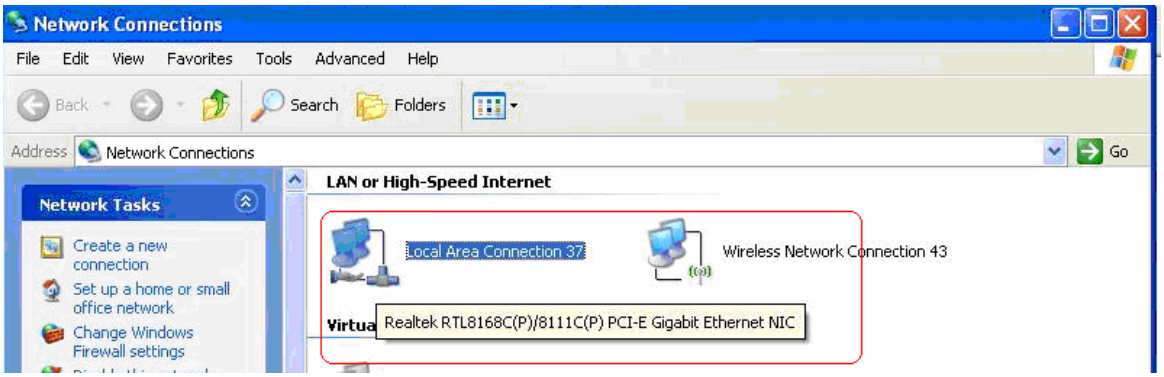
RX OK	Successfully received frames numbers.
Rx Packet Count	The packets of receiving frames.
RX Retry	Frames numbers re-receiving.
RX ICV Error	Integrity Check Value receiving with error.
Reset Counter	Reset counters to zero.

3.3.5 ICS



In this function, you can set the device sharing with Internet. Click the button “Apply”, and then Prompt box pops up.

Select “OK”. When the connection is successful, you will find that the tray “Local Area Connection” has been changed.


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
LAN or High-Speed Internet
Local Area Connection 37
Wireless Network Connection 43
Realtek RTL8168C(P)/8111C(P) PCI-E Gigabit Ethernet NIC

Chapter 4 Introduction for Vista user

4.1 Hardware Installation

The installation of the Adapter is very simple. You could plug the Adapter directly to the USB port on your computer. The LED will light up when the Adapter is installed successfully and the PC is on.

4.2 Software Installation

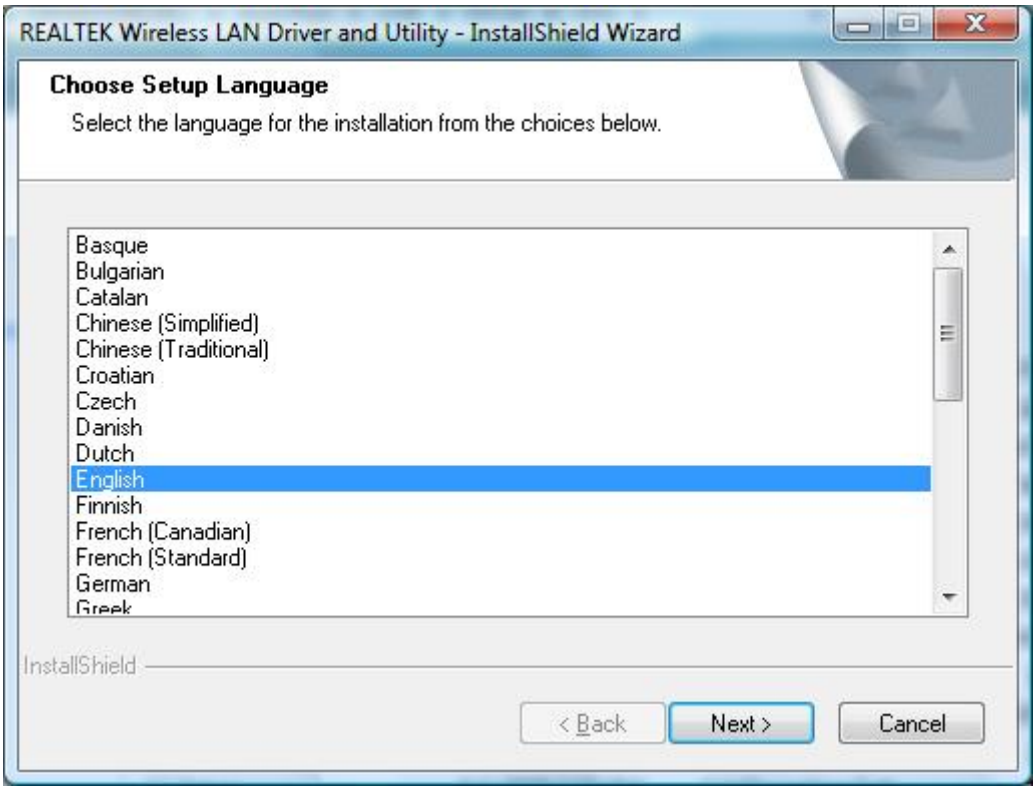
4.2.1 Overview

The Adapter's Setup Wizard will guide you through the Installation procedure for Vista. The Setup Wizard will install the REALTEK 11n USB Wireless LAN Driver and Utility. When you install the hardware prior to before installing the software, the system will prompt "Found New Hardware Wizard", click **Cancel**, and run the Setup Wizard program on the CD-ROM.

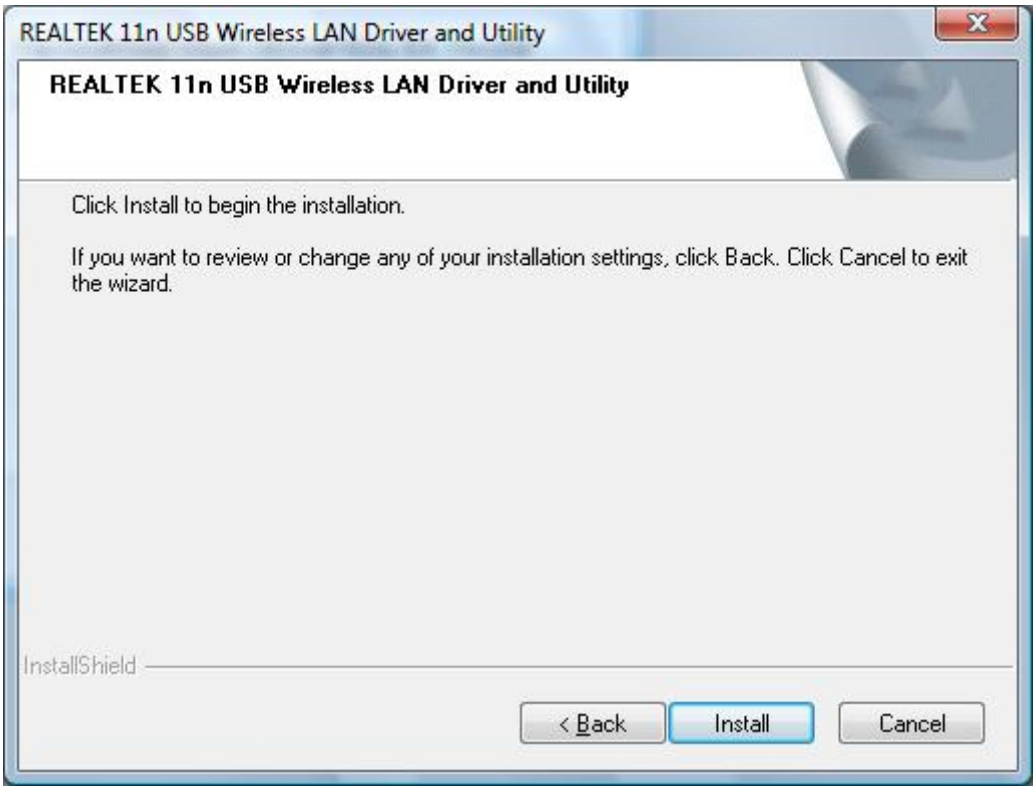
4.2.2 Installation Procedures

1. Insert the CD into your CD-Rom, and find the setup driver in the CD. Then click the setup icon to start the installation.

2. The language-selecting window pops up. Please select the language you use and click "Next".

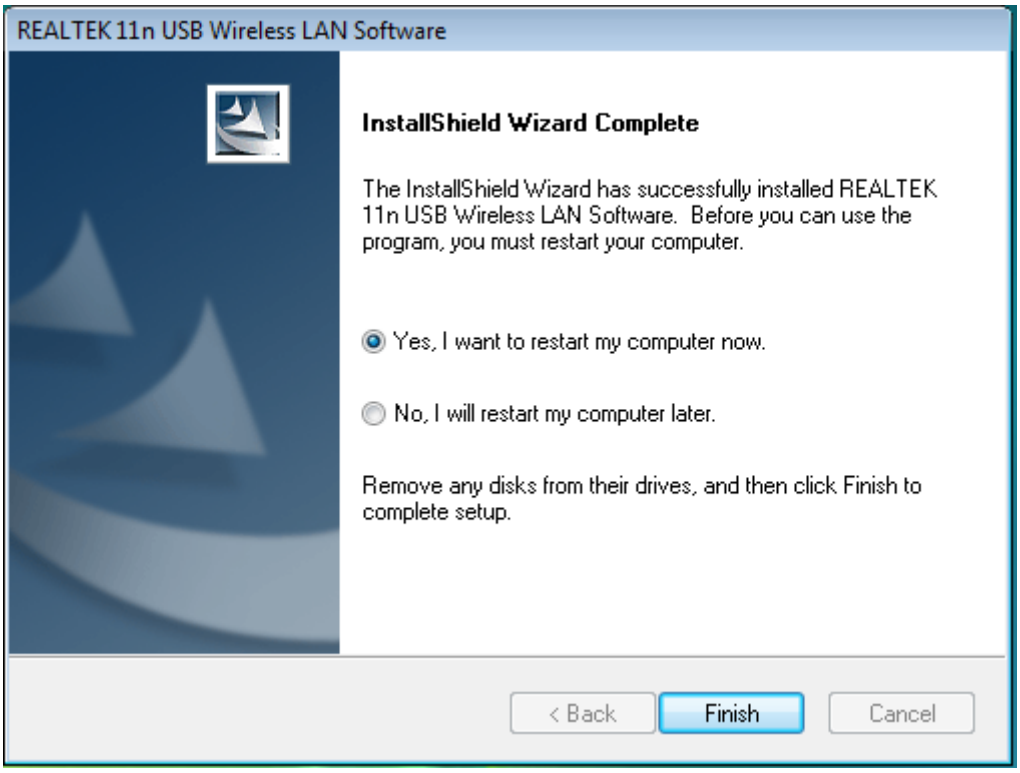


3. The welcome window pops up. Click the "Next" button to proceed.



4. Please wait again while installation

5. After all the steps above, you will see the screen below, Select “Yes” or “No” to reboot the system, then click Finish.



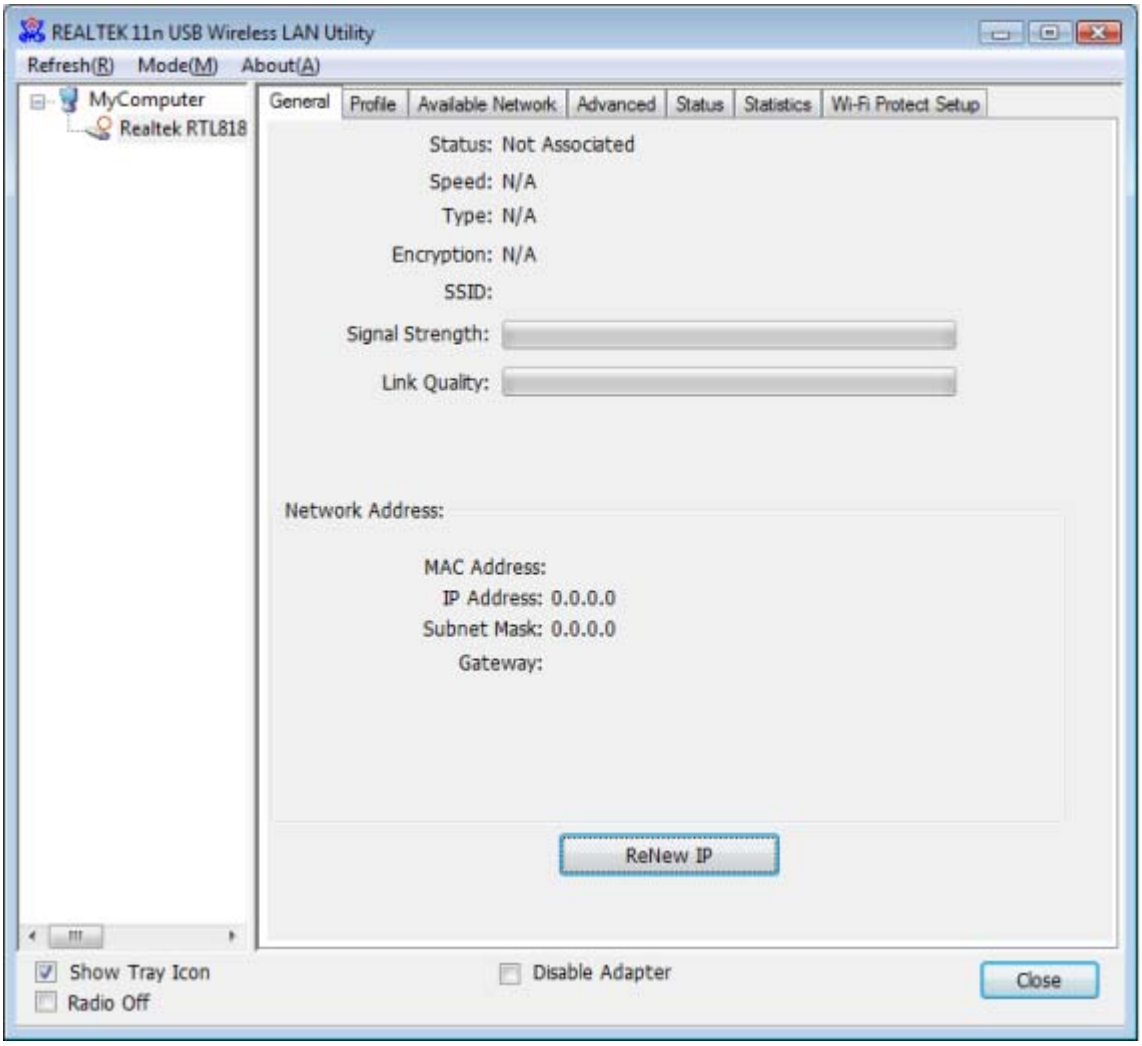
4.3 Management Guide

This chapter describes how to configure your Adapter for wireless connectivity on your Wireless Local Area Network (WLAN) and use the data security encryption features.

After Installing the Adapter, the Adapter's tray icon will appear in your system tray. It appears at the bottom of the screen, and shows the signal strength using color and the received signal strength indication (RSSI).

4.3.1 Interfaces

After the driver installation, the icon  will appear on your desktop. Double click this icon and the following interface appears:



Note:

1. **Functional Buttons** : on top of the window. You can click each button to access each configuration window.

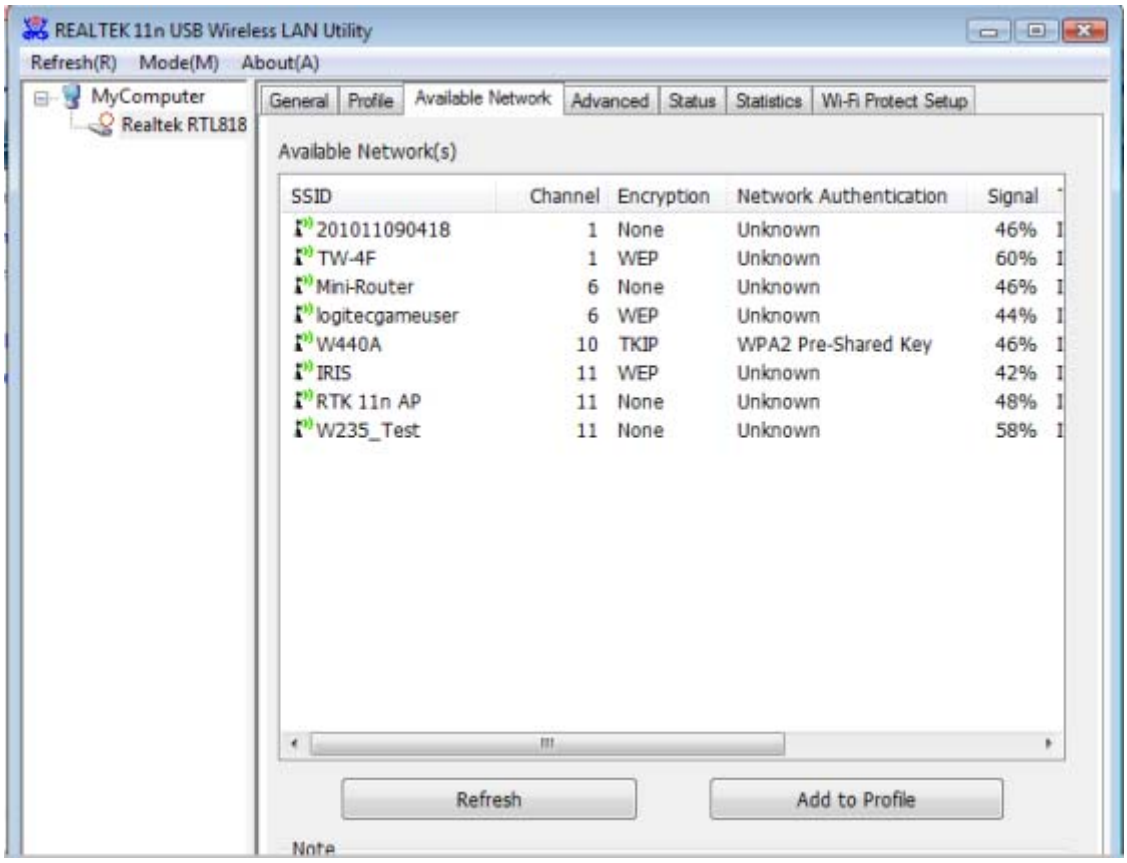
2. **Configuration Column** : Center of the Utility window. Make your changes for each function in this part.

3. **Optional Table** : “Show Tray Icon”, ”Disable Adapter”, ”Radio off”,.

4.3.2 Available Network

This network lists the available wireless networks. The Utility connects to a wireless network with best signal strength automatically. You can refresh the connecting network by clicking on the network name and click the **Refresh** button. In the center of the Utility windows, you will see detail

information of each network.



Available Network Information:

Items	Information
SSID	The name of the IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
Channel	Display current channel in use.
Encryption	Shows the encryption mode in use. There are total 4 modes: None, WEP, TKIP and AES.
Network Authentication	Shows the authentication mode in use.
Signal	This percentage shows the strength of the signal.
Type	The type of network and the station currently connected are shown here. The options include : Infrastructure & Ad-Hoc
BSSID	The IEEE MAC address of locally-managed, generating from a 46 random code.

Support Rates	Show current rate.

Note:

1) An Infrastructure network contains an Access Point or wireless router. All the wireless devices or clients will connect to the wireless router or access point.

2) An Ad-Hoc network contains only clients, such as laptops with wireless desktop adapters. All the adapters must be in Ad-Hoc mode to communicate.

4.3.3 Profile

1. Add a new profile:

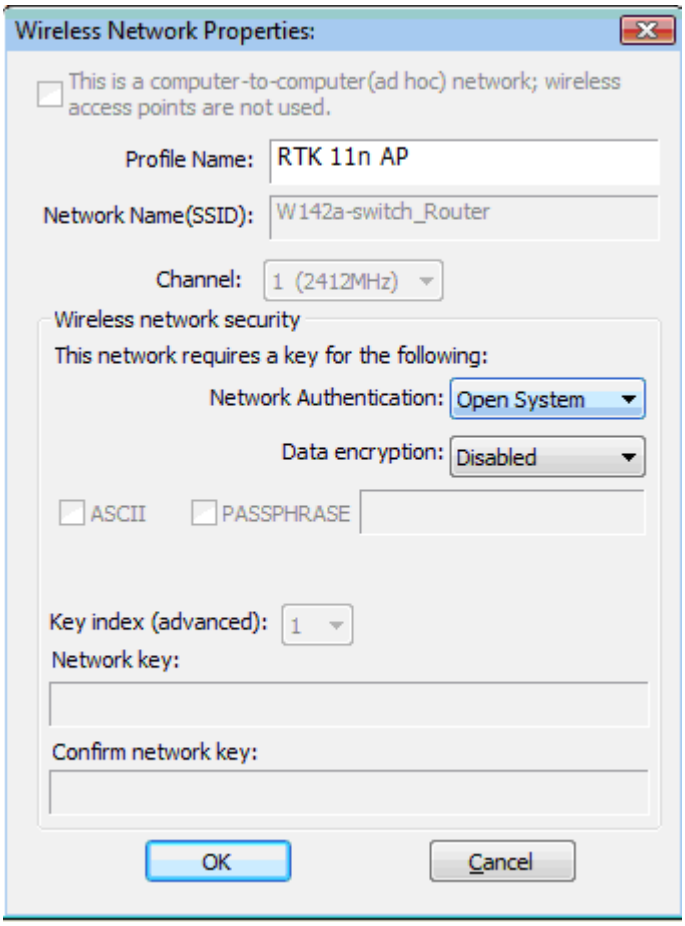
(1) Selecting an available network in the "**Available Network**" function then click the **Add to Profile** button, or double click the network name. You could also add a new profile quickly by clicking the **Add** button in the "**Profile**" function.

Note: If the network you add to profile is not encrypted, "Unsecured network" window will pop up, then Click "OK".

(2) It displays "Wireless Network Properties" dialog box. This profile page allows users to save different wireless settings, which helps users to get access to wireless networks at home, office or other wireless network environments quickly.

In the following dialog box, there are some items:

Items	Information
Profile Name	Identifies the configuration profile .This name must be unique. Note that the profile names are not case-sensitive.
Network Name(SSID)	The IEEE 802.11n wireless network name, using default name defined by system. This field has a maximum limit of 32 characters.



(3). Channel (Country Region Code): six countries to choose. Country channel list:

Country	Channel Range	Country	Channel Range
SPAIN	CH1 ~ CH11	FRANCE	CH1 ~ CH13
CANADA	CH1 ~ CH11	JAPAN	CH1 ~ CH14
ETSI	CH1 ~ CH13	ISRAEL	CH1 ~ CH13

(4) Wireless Network Security

A. Network Authentication

Select the Security tab in the screen above. To define the security mode, select the desired security mode as follows. There are 7 types supported: Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X, WEP 802.1X, Please select a type from the drop down list

- **Open System:** enable an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match.
- **Shared-key:** only allows the adapter to associate with access points that have the same WEP key.
- **802.1x:** This item appears while the environment is set to an Open authentication with WEP encryption. Mark the checkbox to make the section available. The section is also available in WPA and WPA2 authentication types.
- **Preshared Key(PSK):** This is the shared secret between AP and STA. For WPA-PSK, WPA2-PSK and WPA-NONE authentication mode, this field must be filled with characters longer than 8 and less than 32 lengths. The following dialog appears if you have input invalid values.
- **WEP Key:** Only available when using WEP encryption algorithm. The key must match AP's key. Only using the same cryptographic key to access the computer, the internet can storage, and decryption the information from other computer.

B. Data Encryption:

<table>
<tr><td>Data encryption</td><td>There are 4 types supported: Disabled, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open System</td><td>Disabled, WEP</td></tr>
<tr><td>Shared Key , WEP 802.1X</td><td>WEP</td></tr>
<tr><td>WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X</td><td>TKIP, AES</td></tr>
</table></td></tr>
</table>

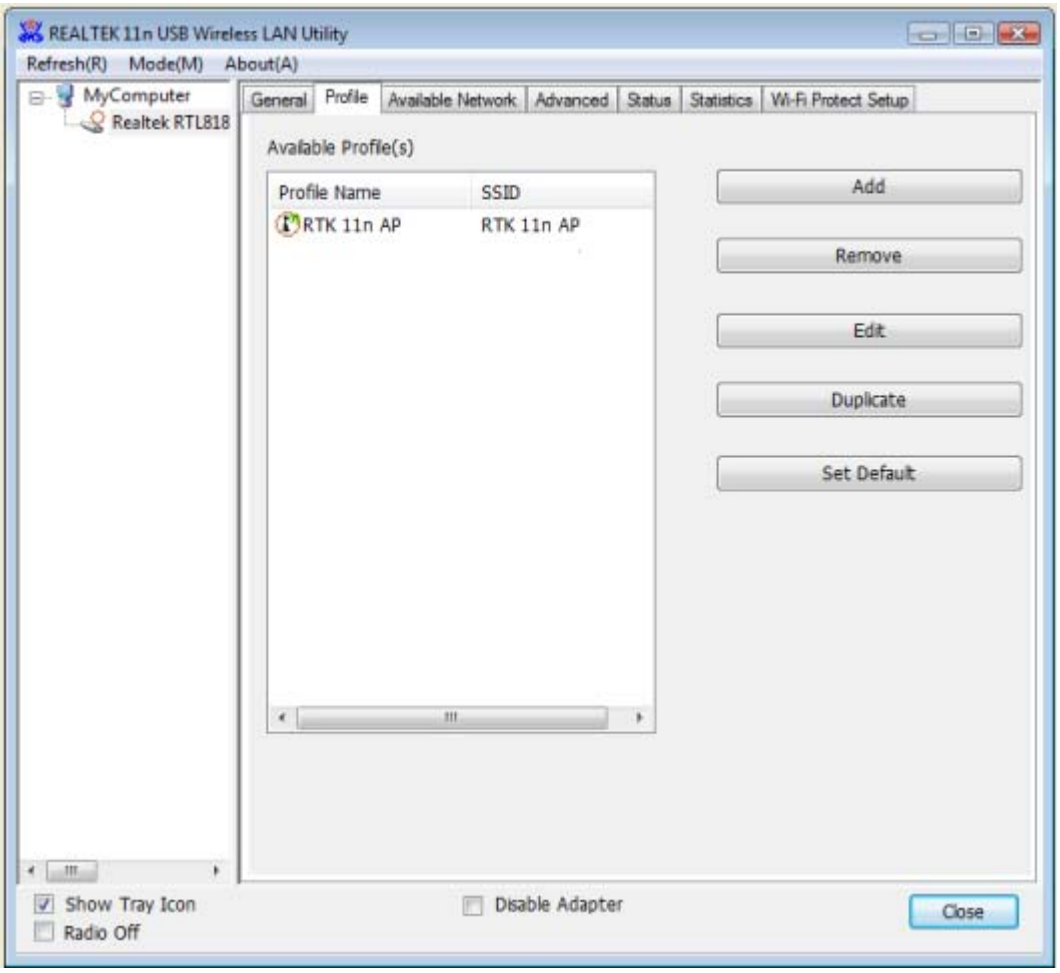
Note: Select different Security Options, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

- **TKIP:** "Temporary Key Integration communication Protocol", it provide each packet's key

mixture, message integration and key reconstruction mechanism. TKIP can use with personal or the enterprise network validation.

- **AES:** “Advanced Encryption Standard”, It is a new method that the wireless transmission of privacy protection. AES encryption methods provides more careful than TKIP.

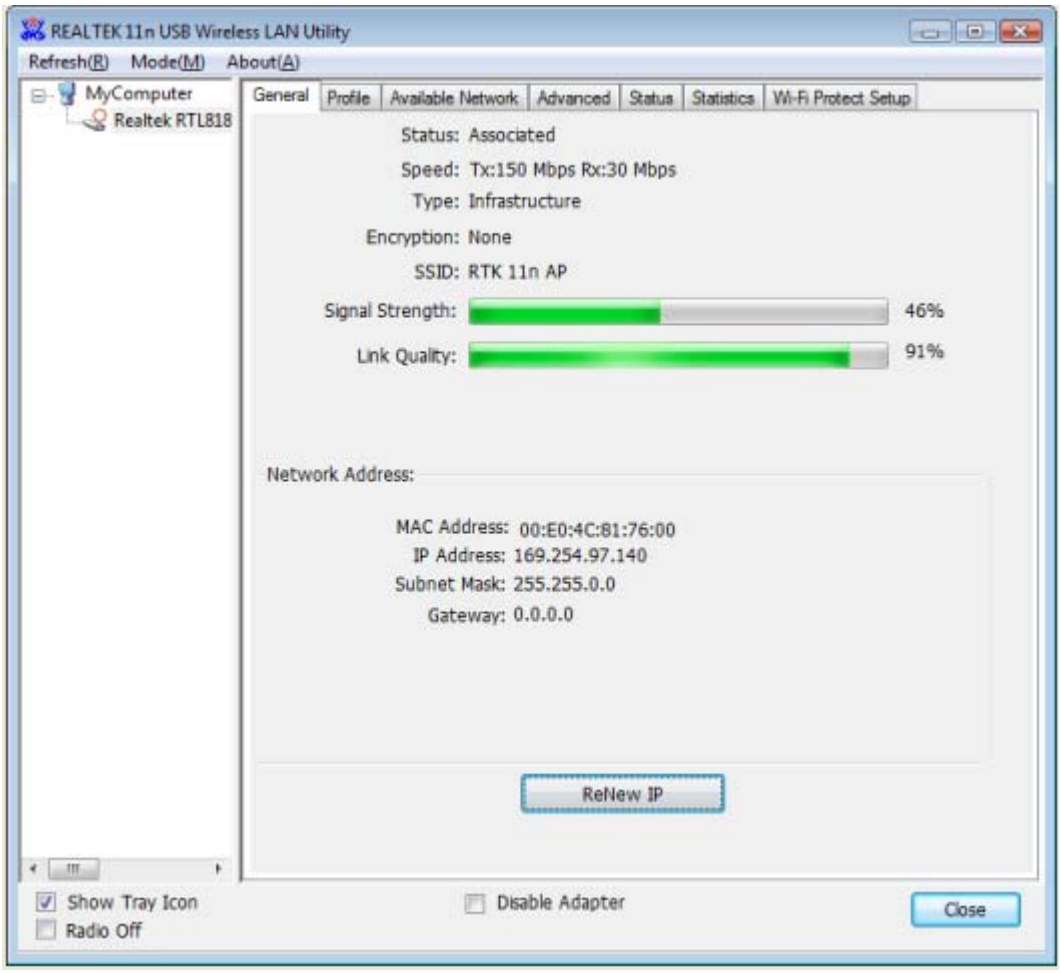
(5) Finish the configuration, and then click “OK”, that network has been added to the profile.



Profile List: The list shows all the profiles you have added before.

Buttons: You can click on these buttons to **Add** a new profile, **Remove**, **Edit**, **Duplicate** or **Set Default** an old profile.

4.3.4 General



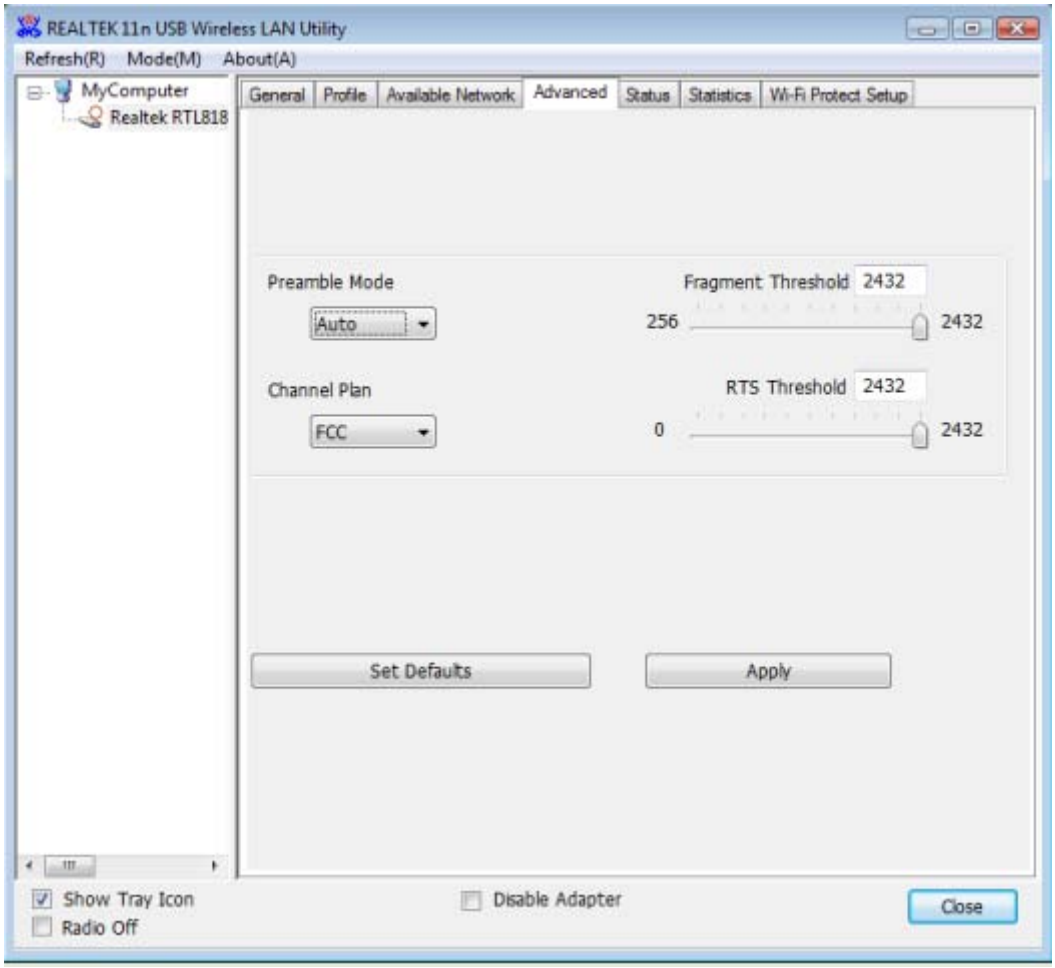
In this window, there are some items as following:

Items	Information
Status	Currently connection status.
Speed	Show current transmit rate and receive rate.
Type	Network type in use.
Encryption	Encryption type in use.
SSID	The name of the IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
Signal Strength	Receive signal strength.
Link Quality	Display connection quality based on signal strength.
Network	A. **MAC Address**: The MAC address of the wireless network adapter.

Address	B. **IP Address:** IP address of current connection. C. **Subnet Mask**: Subnet mask of current connection. D. **Gateway**: Gateway of current connection.

4.3.5 Advanced

This screen below allows you to make advanced configuration for the profile. Please refer to the following chart for definitions of each item.



1. Preamble Mode

The length of CRC blocks in the frames during the wireless communication. Select the options from the drop list : (1) Long (2)Short (3)Auto.

2. Channel Plan

The selected country: FCC, IC, ETSI, Spain, France, MKK, MKK1, Israel, TELEC, Default.

(Note: The choose between channels function is not allowed in USA.)

3. Threshold

(1) Fragment Threshold

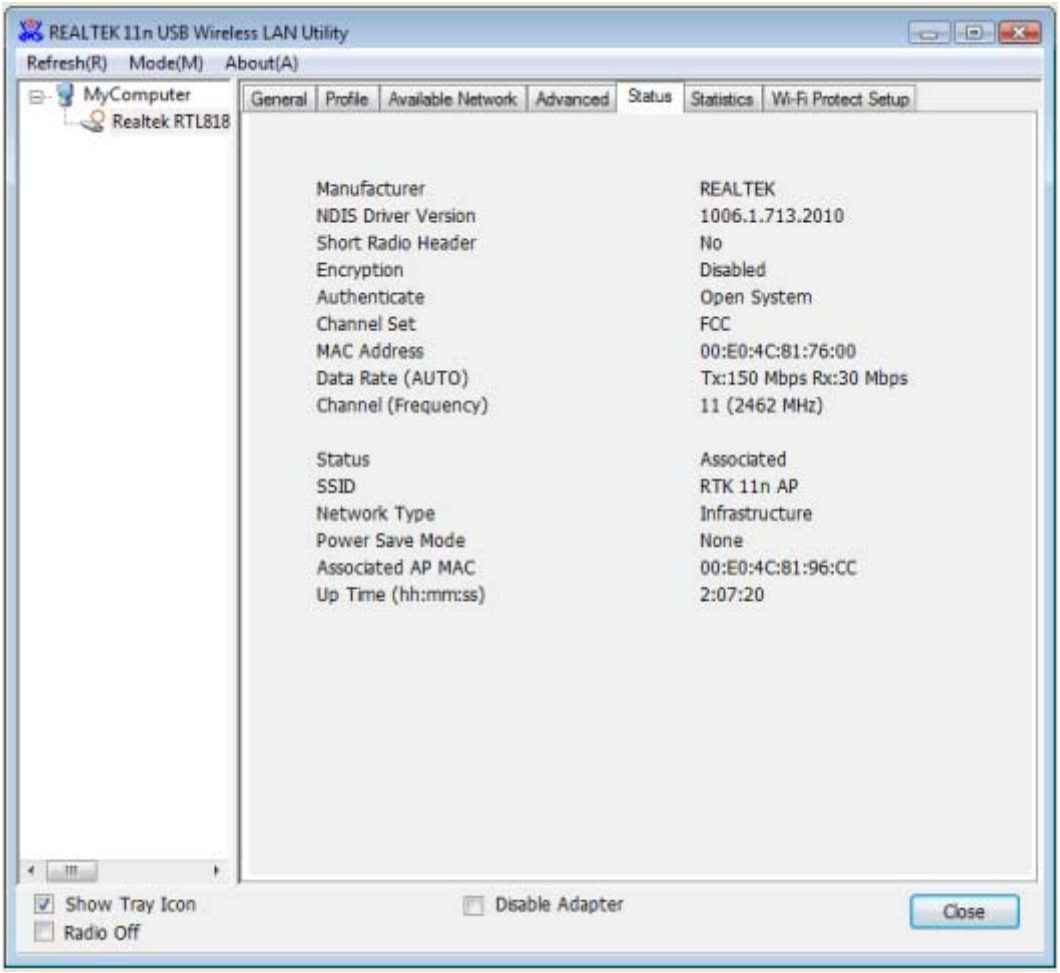
This value should remain at its default setting of 2347. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 256 to 2432. Setting the fragmentation threshold too low may result in poor performance.

(2) RTS Threshold

Request To Send threshold. This value should remain at its default setting of 2346. If you encounter inconsistent data flow, only minor modifications to the value range between 0 and 2432 are recommended.

4.3.6 Status

The Status tab contains general information about the program and its operations. The current Status tab needn't any configurations.



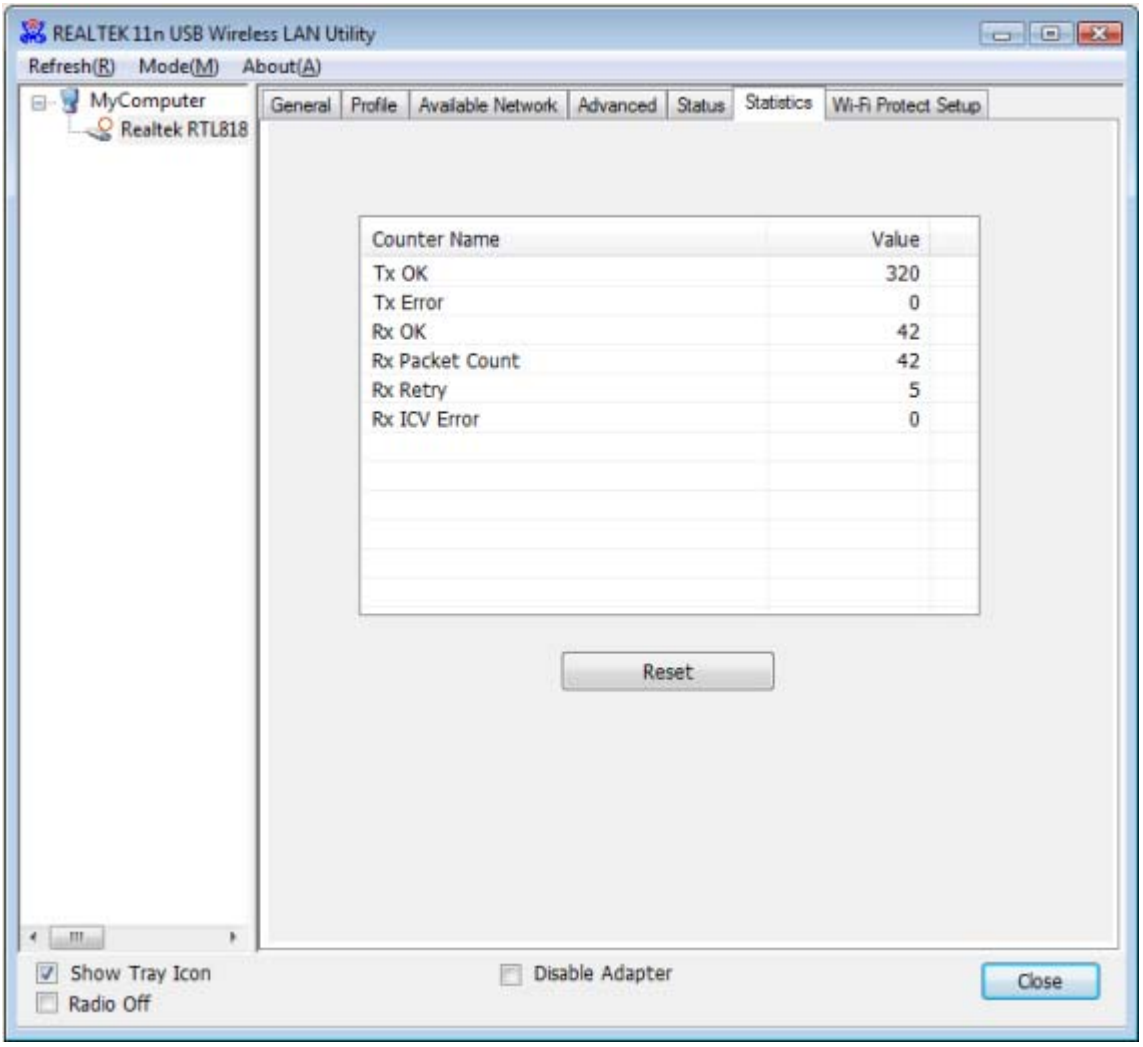
The following table describes the items found on the Status screen.

Items	Information
Manufacturer	The name of manufacturing this product.
NDIS Driver Version	The version of Network Driver Interface Specification.
Encryption	Here displays the encryption type the device is using.

Authenticate	This shows whether the server based authentication is used.
Channel Set	Appears the country of you use.
MAC Address	The MAC address of the wireless network adapter.
Data Rate(Auto)	Show current transmit rate and receive rate.
Channel Frequency	Shows the channel in use (1~14).
Status	Current connection status.
SSID	The SSID of the wireless system.
Network Type	The type of network and the station currently connected are shown here. The options include : Infrastructure, Ad Hoc
Power Save Mode	The power save mode have three mode: Max, Min, None
Associated AP MAC	The MAC Address of associated AP.
Up Time	Record life time.

4.3.7 Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates the MIB counters into a format easier for user to understand. It show receiving and transmitting statistical information about the following receiving and transmitting diagnostics for frames received by or transmitted to the wireless network adapter.



Items	Information
TX OK	Successfully transmitted frames numbers.
TX Error	Frames numbers transmitting with error.
RX OK	Successfully received frames numbers.
Rx Packet Count	The packets of receiving frames.
RX Retry	Frames numbers re-receiving.
RX ICV Error	Integrity Check Value receiving with error.
Reset Counter	Reset counters to zero.

4.3.8 Wi-Fi Protect Setup

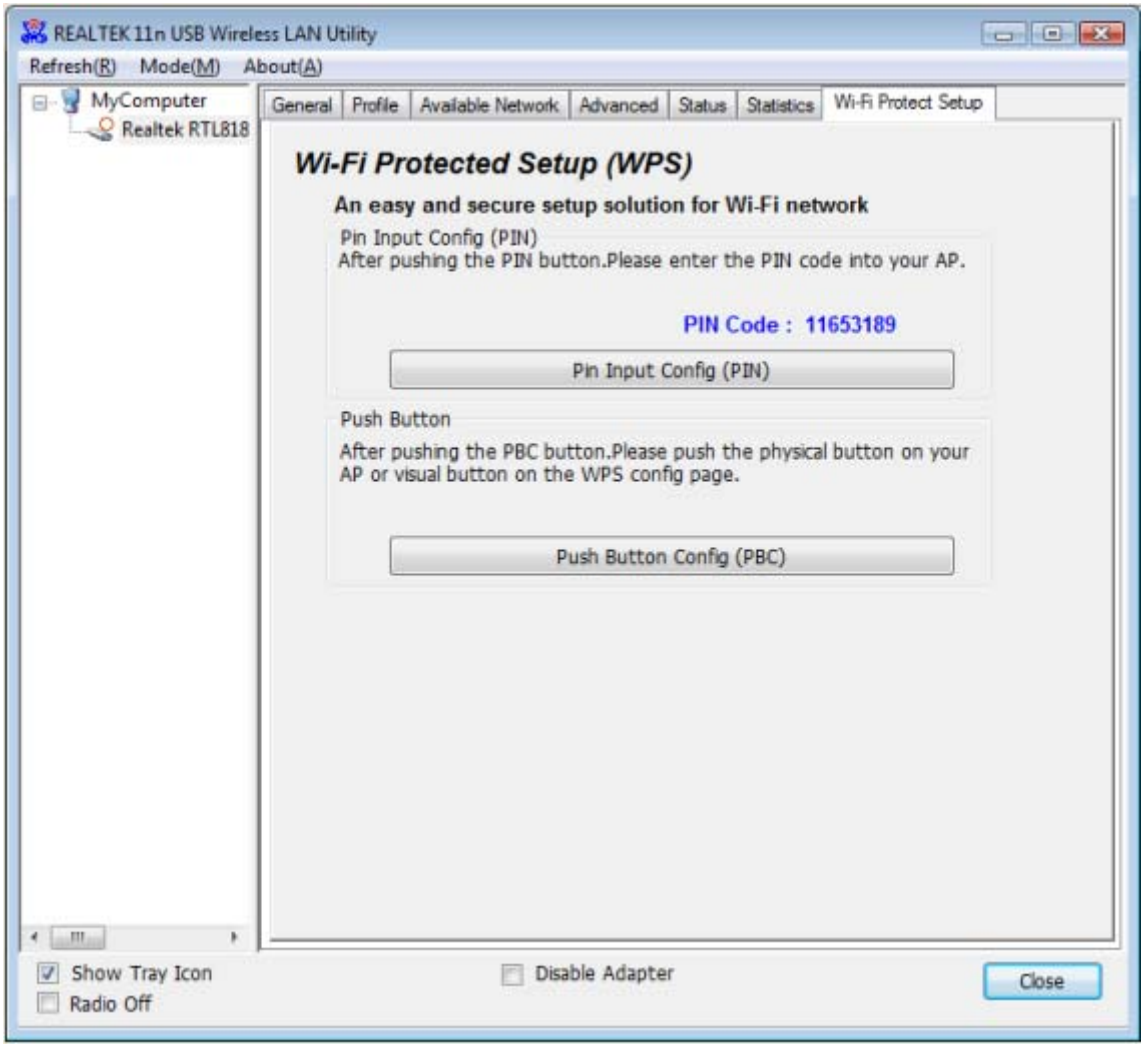
The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This adapter supports the configuration setup using PIN

configuration method or PBC configuration method. If the wireless card supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless card and router using either Push Button Configuration (PBC) method or PIN method.

Here we will introduce two ways to configure the QSS

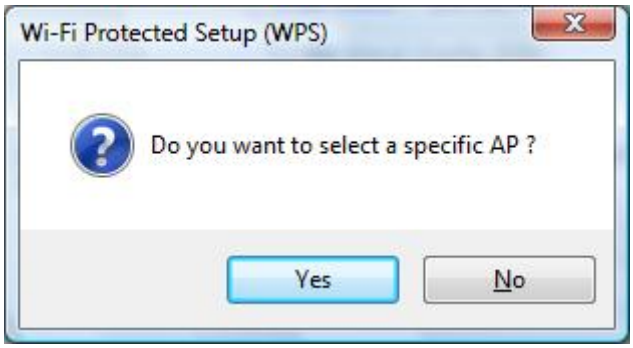
(QSS is known as rapid security settings, by pressing the wireless router and wireless card on the QSS button to automatically set up WPA2 secure connection level without the router or network adapter management software to conduct the cumbersome interface settings, greatly simplifying the operation of the wireless security settings.)

Pin Code: 8-digit numbers. It is randomly generated from system

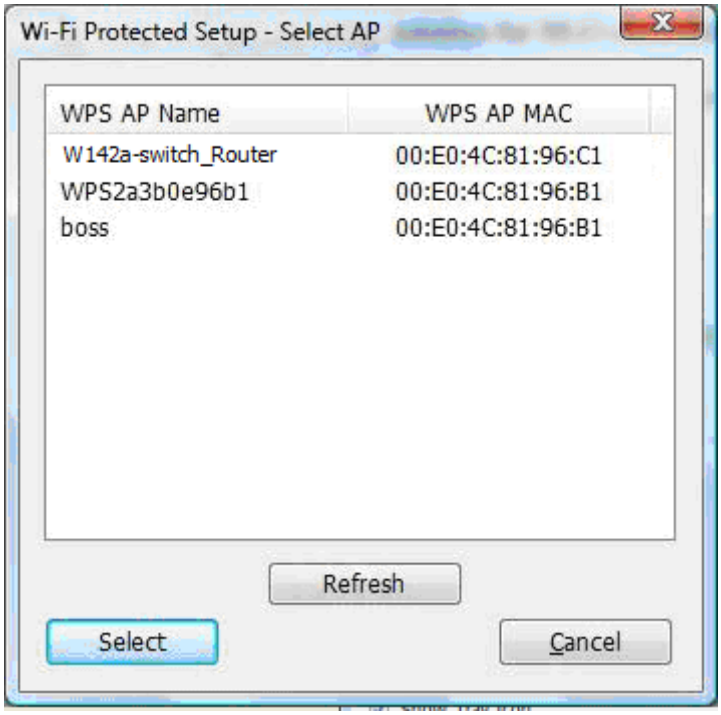


1. PIN method

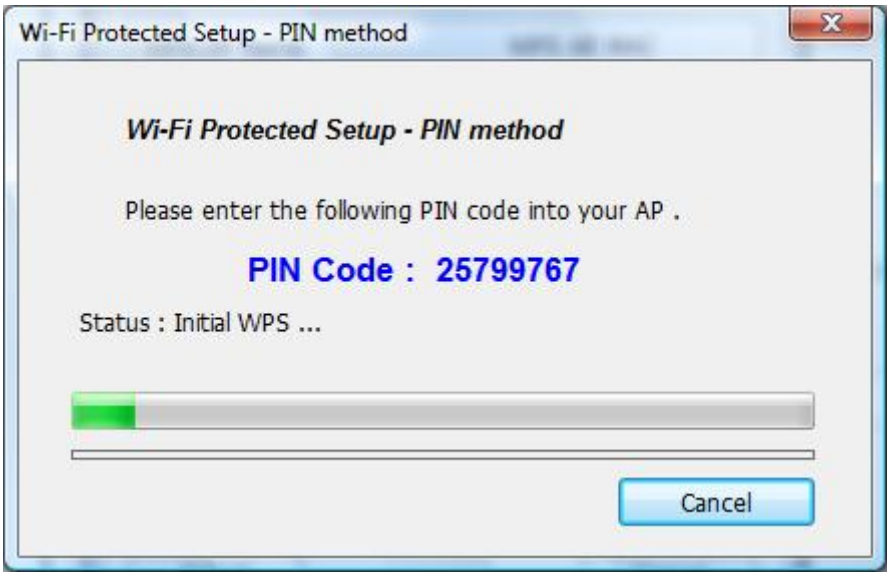
Click the button “Pin Input Config (PIN)”, and then come to the following figure.



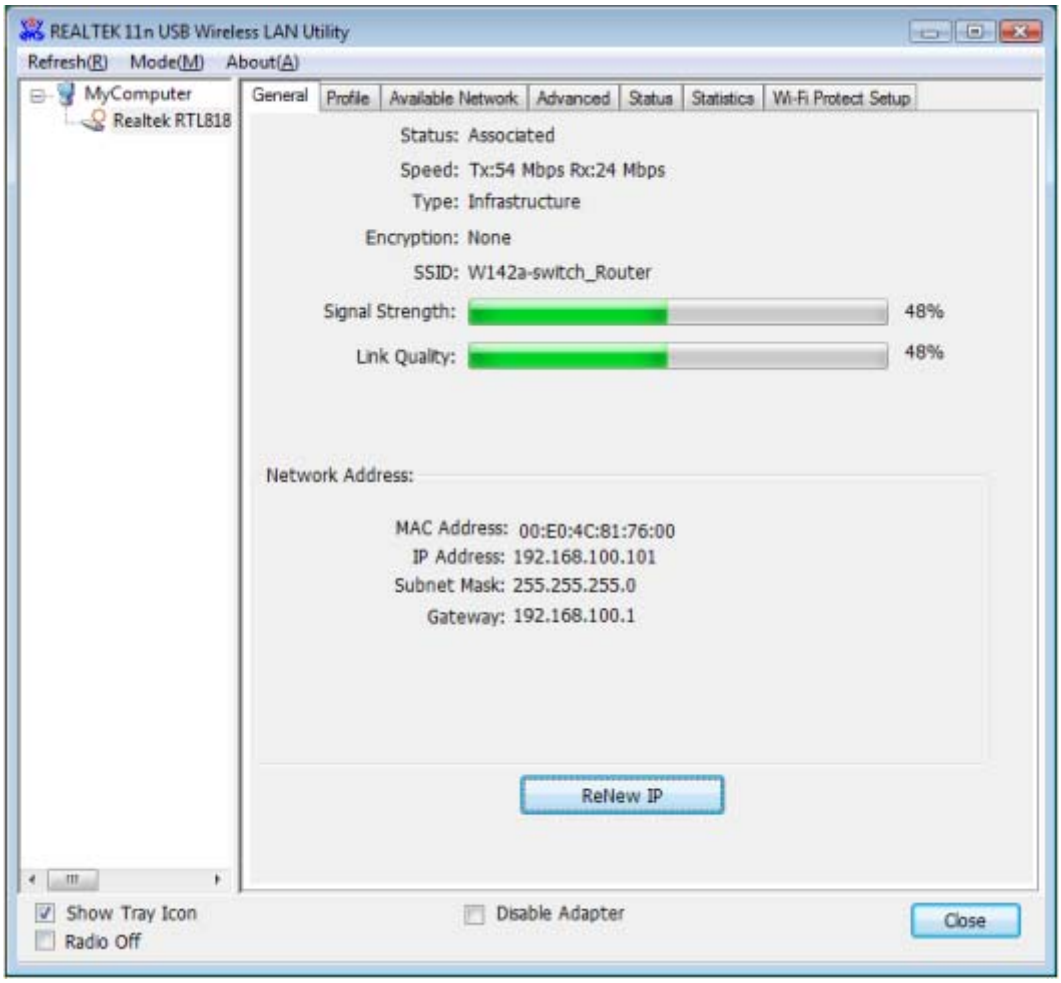
Click the button “Yes”, you can select one of the AP. Also, you can click these buttons by “Refresh / Select / Cancel” for any change.



When the following interface pops up, double click the Internet WEB browser icon on your desktop screen. Type the IP address of you selected Router/AP into the URL and press “Enter”, and then you can enter the configuration.
Please enter the WPS (Wi-Fi) configuration page, type the PIN code of adapter and click confirm button to build WPS connection.

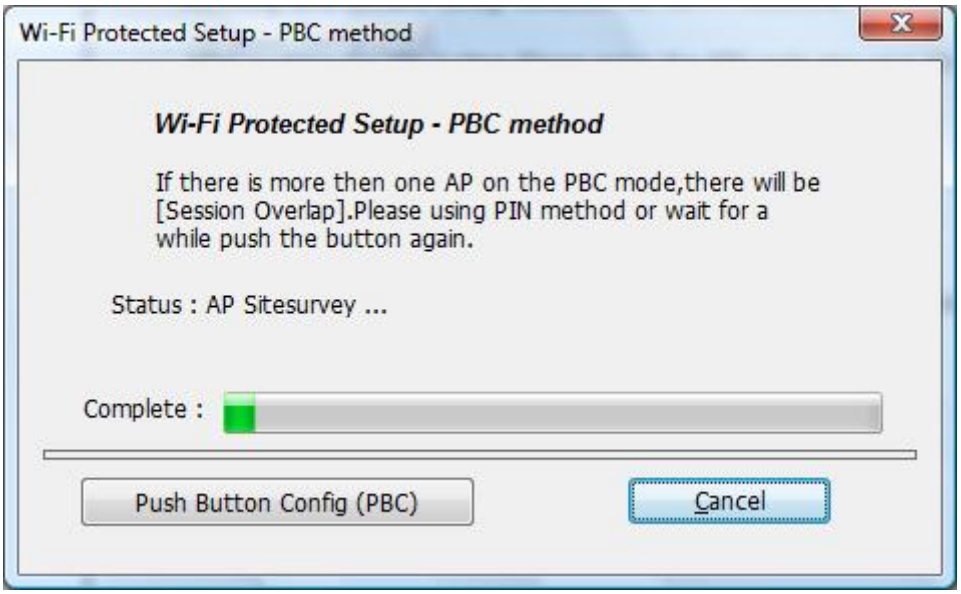


When the “General” window appears, WPS is configured successfully.



2. **PBC (Push Button Configuration) method**

After pushing the PBC button, Please push the physical button on your AP or visual button on the WPS config page, then come to the following figure.



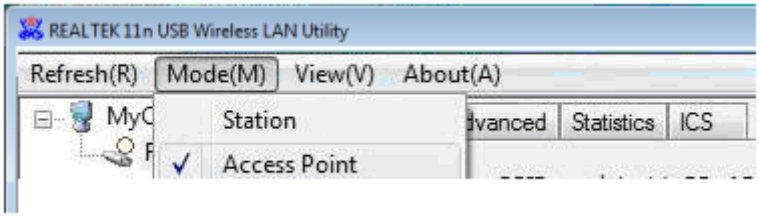
Please enter the WPS (Wi-Fi) configuration page of your desired router/AP, and then start PCB connection.

4.4 AP mode management guide for Vista

If you wish to share the Internet access with the wireless stations in your environment, you can configure this wireless adapter as a software access point (Soft AP). In this mode, this wireless adapter becomes the wireless access point that provides local area network and Internet access for your wireless stations.

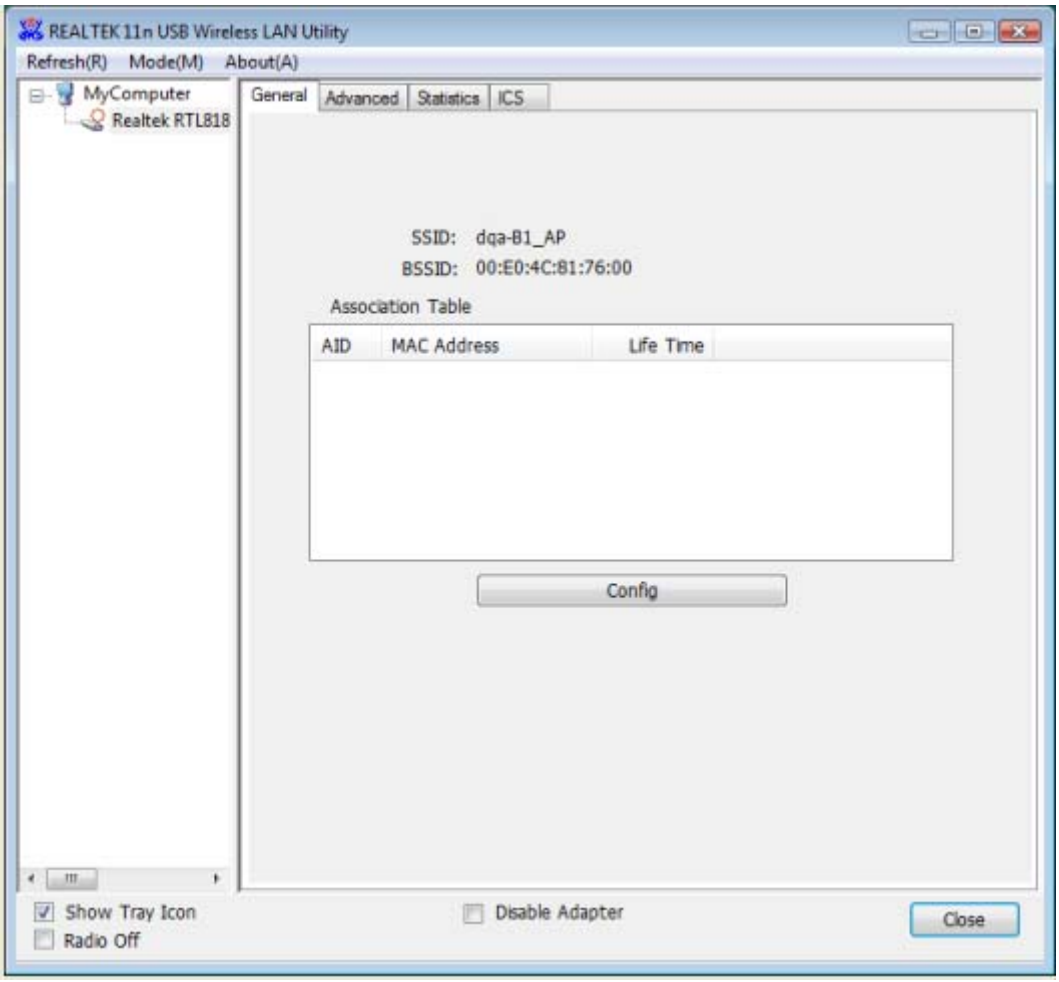
4.4.1 General

To use this adapter as an access point, please click the “Mode” on **Functional Menu** and select **“Access Point”**.



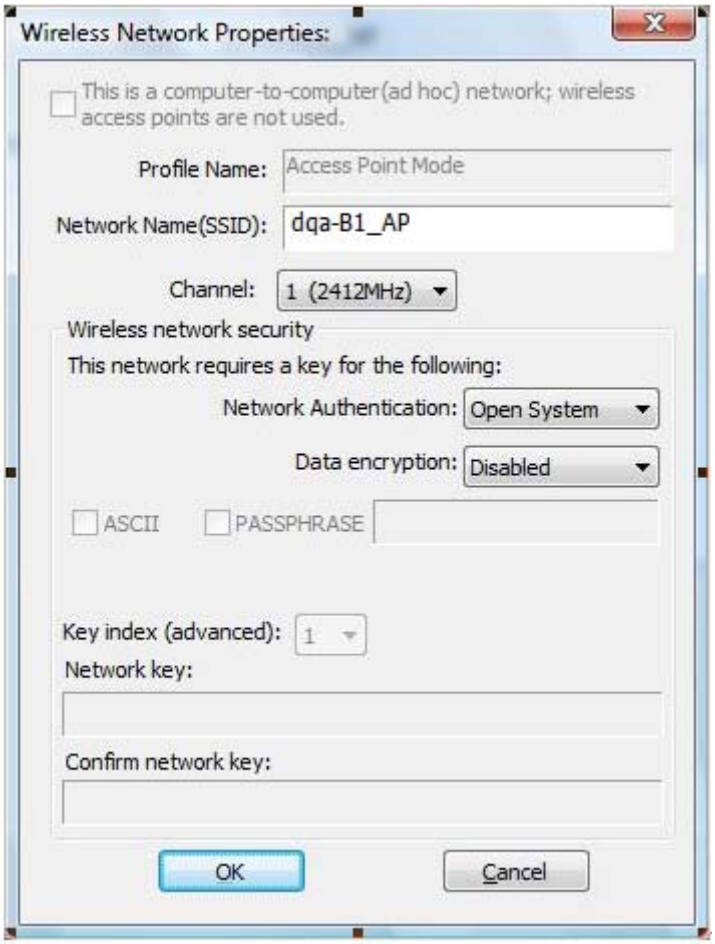
Then switching from station mode to AP: At the same time, you will find that the icon on the system tray is changed.

Please refer to the following information about this AP-mode utility.



Items	Information
SSID	AP name of user type.
BSSID	The IEEE MAC address of locally-managed, generating from a 46 random code.
AID	Raise value by current connection.
MAC Address	The station MAC address of current connection.
Life Time (mm:ss)	Record life time.

Click the “Config” button, then you can configure the wireless network properties. This page provides overall configuration to this adapter.



SSID: AP name of user type.

Channel: Manually force the AP using the channel. System default is channel 1.

Security Setting: Authentication mode and encryption algorithm used within the AP. System default is no authentication and encryption.

Cancel: Cancel the above changes.

OK: Apply the above changes.

A. Network Authentication

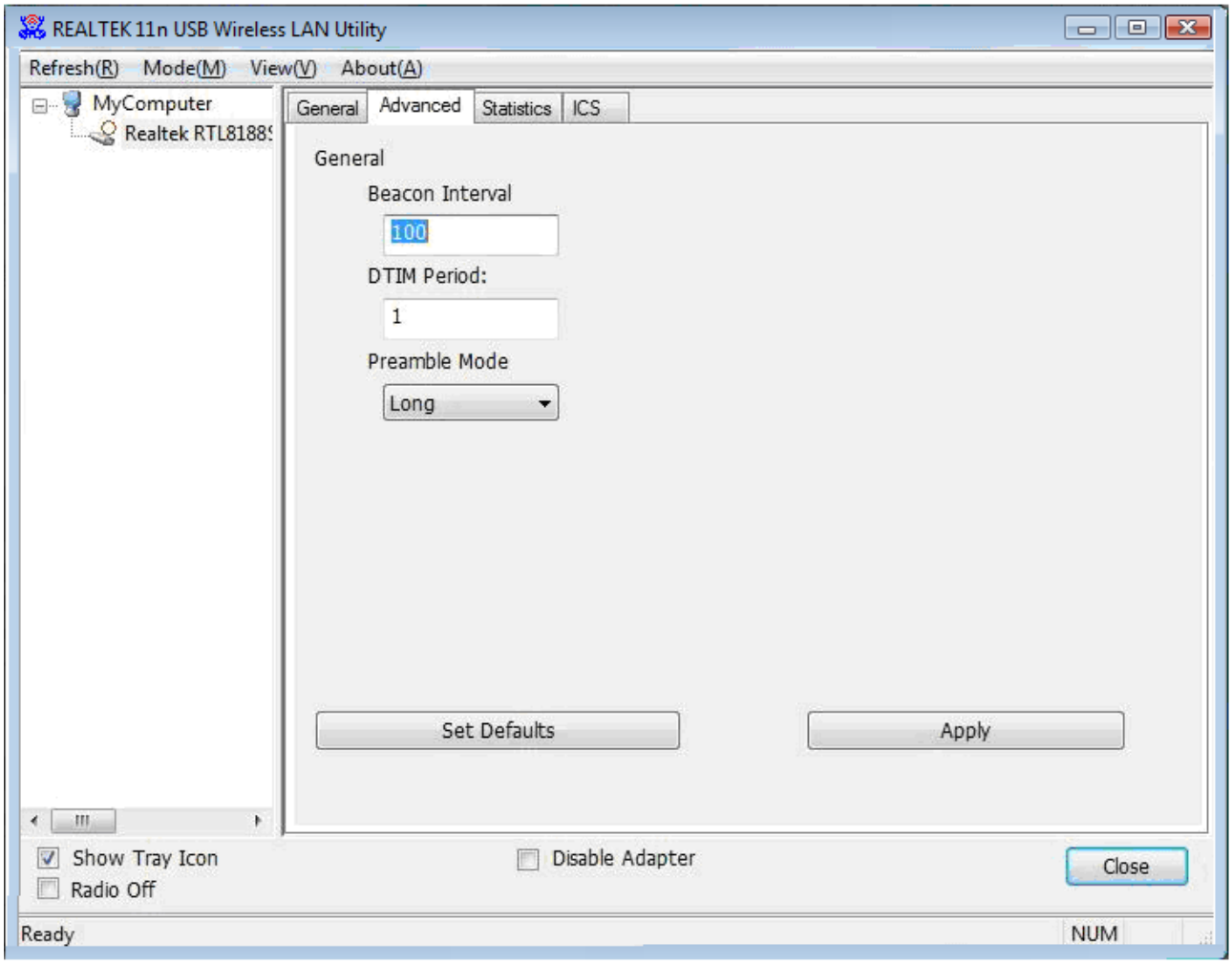
Select the Security tab in the screen above. To define the security mode, select the desired security mode as follows. There are 4 types supported: Open System, Shared Key, WPA-PSK, WPA2-PSK. Please select a type from the drop down list.

B. Data Encryption:

<table>
<tr><td>Data encryption</td><td>There are 4 types supported: Disabled, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open System</td><td>Disabled, WEP</td></tr>
<tr><td>Shared Key , WEP 802.1X</td><td>WEP</td></tr>
<tr><td>WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X</td><td>TKIP, AES</td></tr>
</table>
</td></tr>
</table>

Note: Select different Security Options, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

4.4.2 Advanced

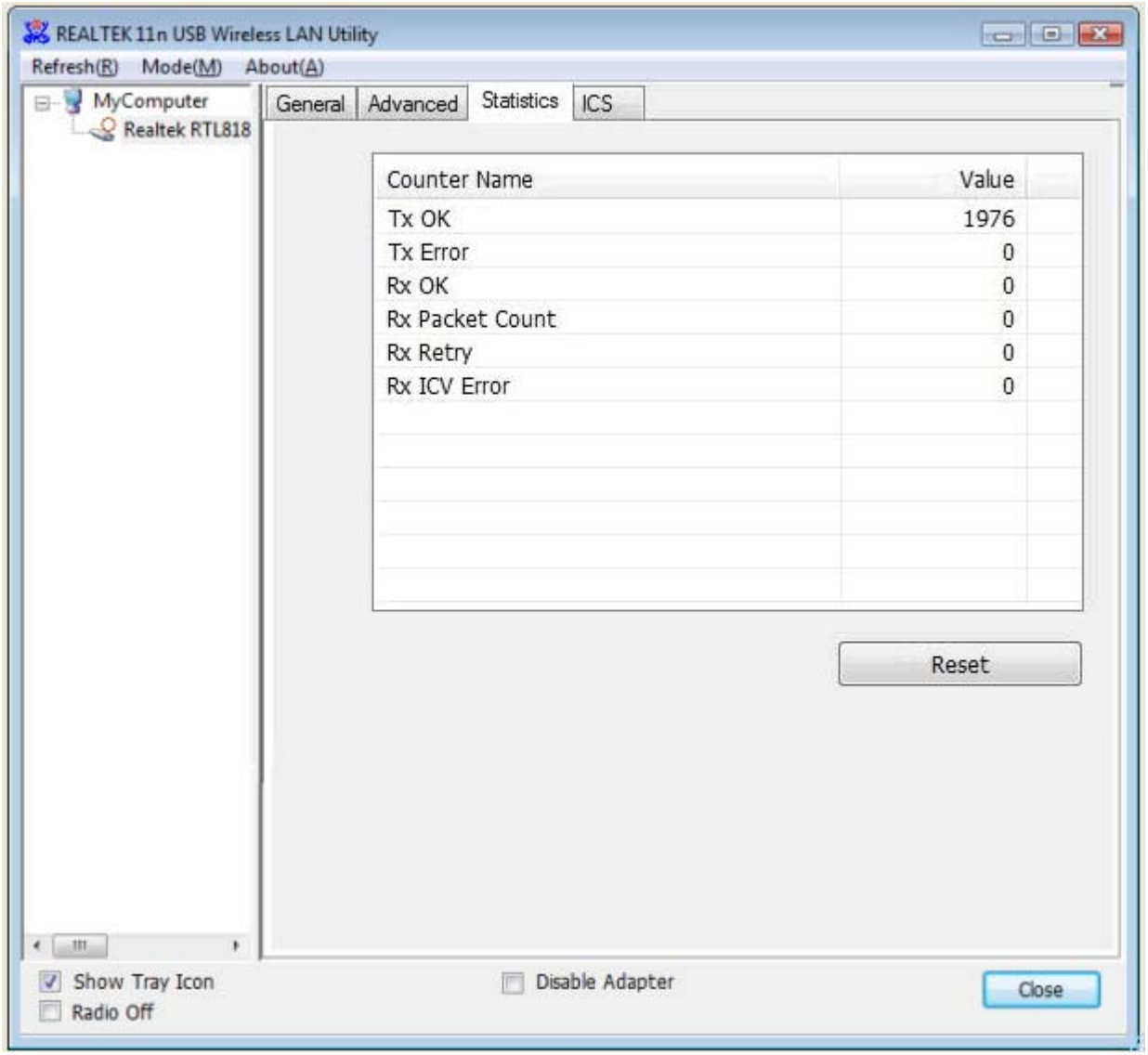


Items	Information

Beacon Interval	Beacon frequency spacing.
DTIM Period	Delay transmission indicator map (DTIM) is enabled for power management of the client. If any client power management is enabled, the DTIM should be retained for 1 (the default). Support this parameter range from 1 to 255.
Preamble Mode	Select the options from the drop list,(Long / Short).
Set Defaults	Setting the default value of General.
Apply	Apply the above changes.

4.4.3 Statistics

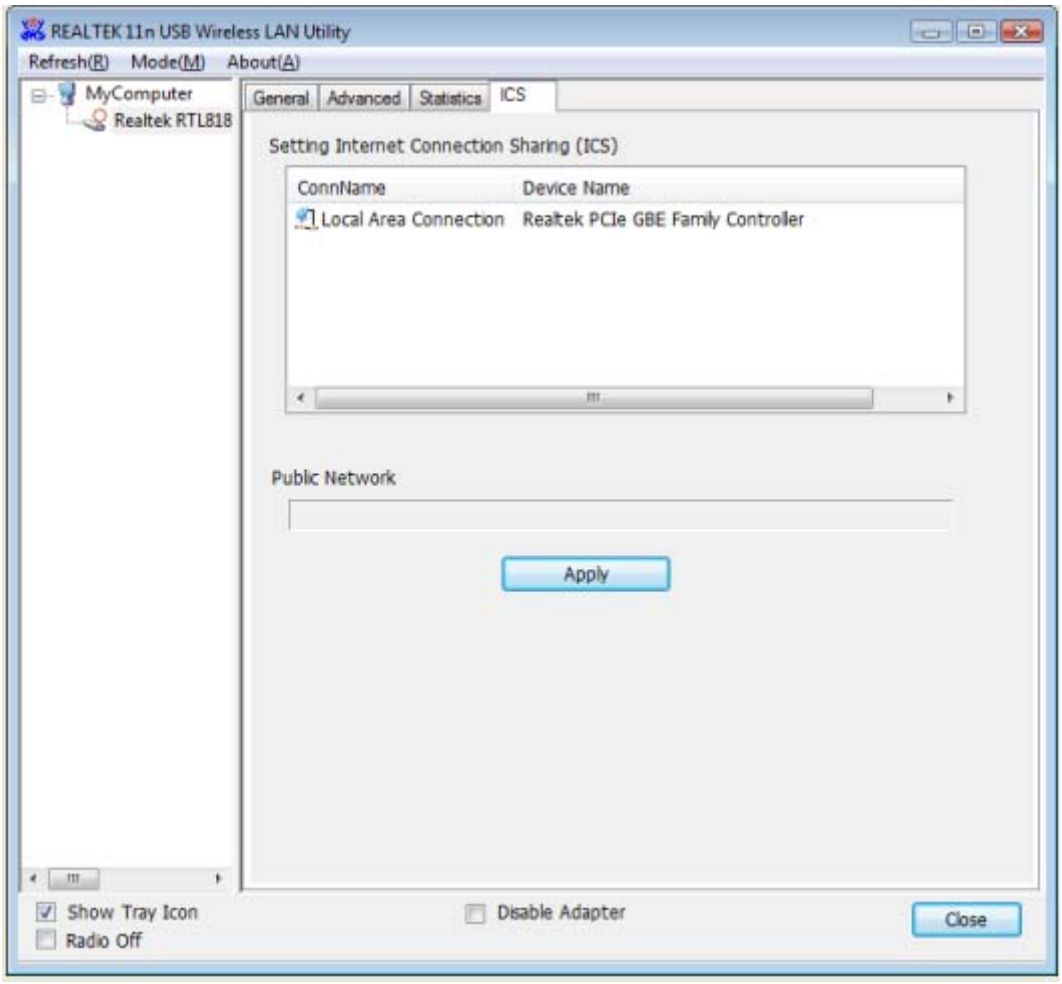
Statistics page displays the detail counter information based on 802.11 MIB counters.



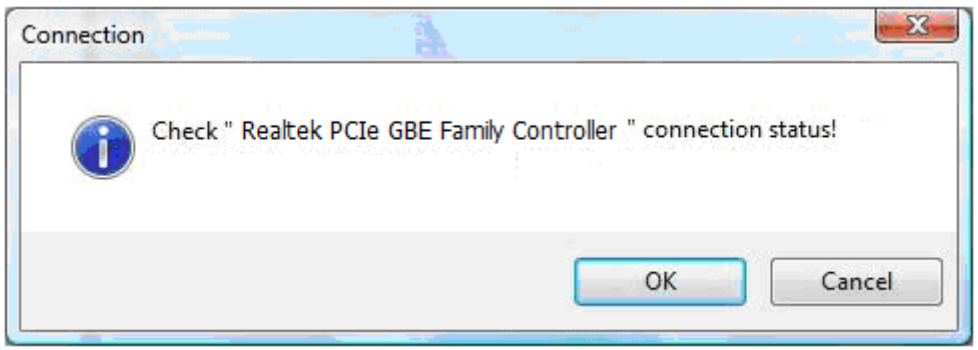
Items	Information
TX OK	Successfully transmitted frames numbers.
TX Error	Frames numbers transmitting with error.

RX OK	Successfully received frames numbers.
Rx Packet Count	The packets of receiving frames.
RX Retry	Frames numbers re-receiving.
RX ICV Error	Integrity Check Value receiving with error.
Reset Counter	Reset counters to zero.

4.4.4 ICS



In this function, you can set the device sharing with Internet. Click the button “Apply”, Prompt box pops up.



Select “OK”, then the Internet connection is sharing.

Chapter 5 Introduction for Windows 7 User

5.1 Hardware Installation

The installation of the Adapter is very simple. You could plug the Adapter directly to the USB port on your computer. The LED will light up when the Adapter is installed successfully and the PC is on.

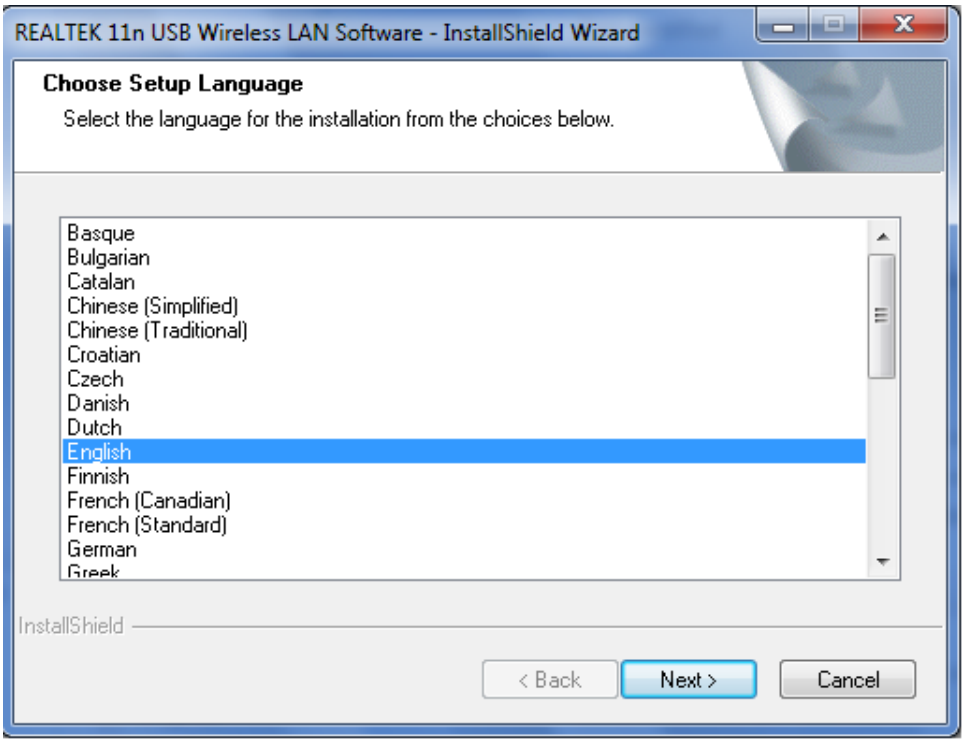
5.2 Software Installation

5.2.1 Overview

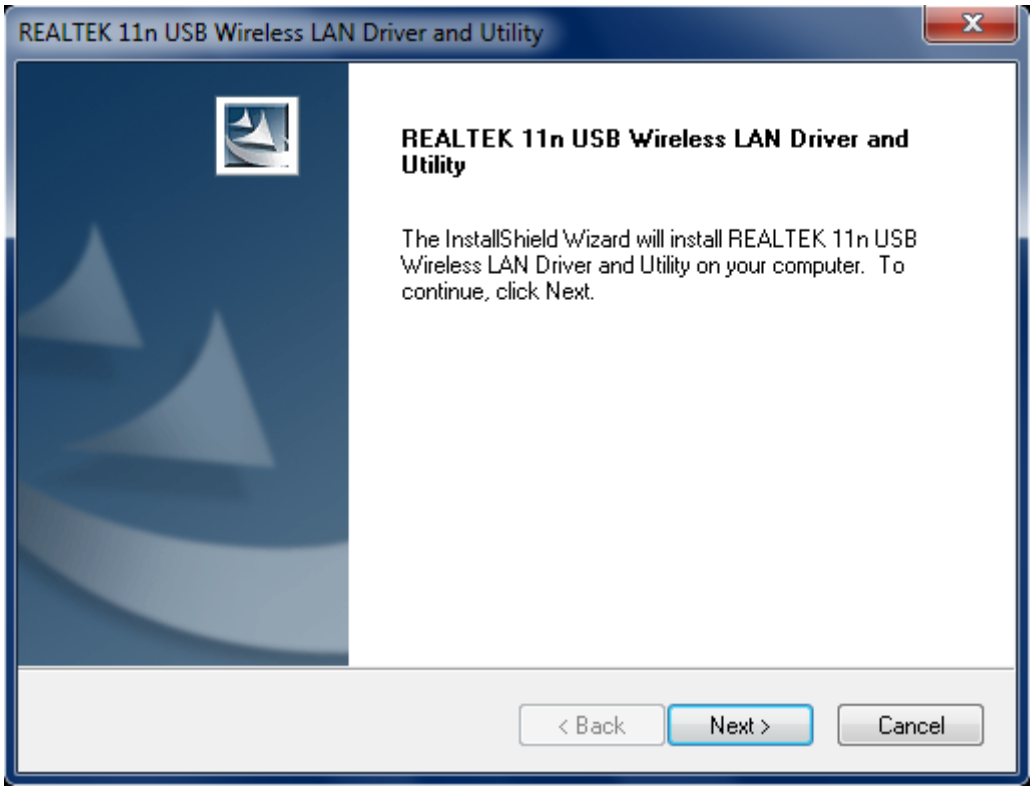
The following Setup Wizard will guide you through the Installation procedure for Windows 7. The Setup Wizard will install the REALTEK 11n USB Wireless LAN Driver and Utility. When you install the hardware before installing the software, the system will prompt “Found New Hardware Wizard” on your screen, click Cancel, and run the Setup Wizard program on the CD-ROM.

5.2.2 Installation procedures

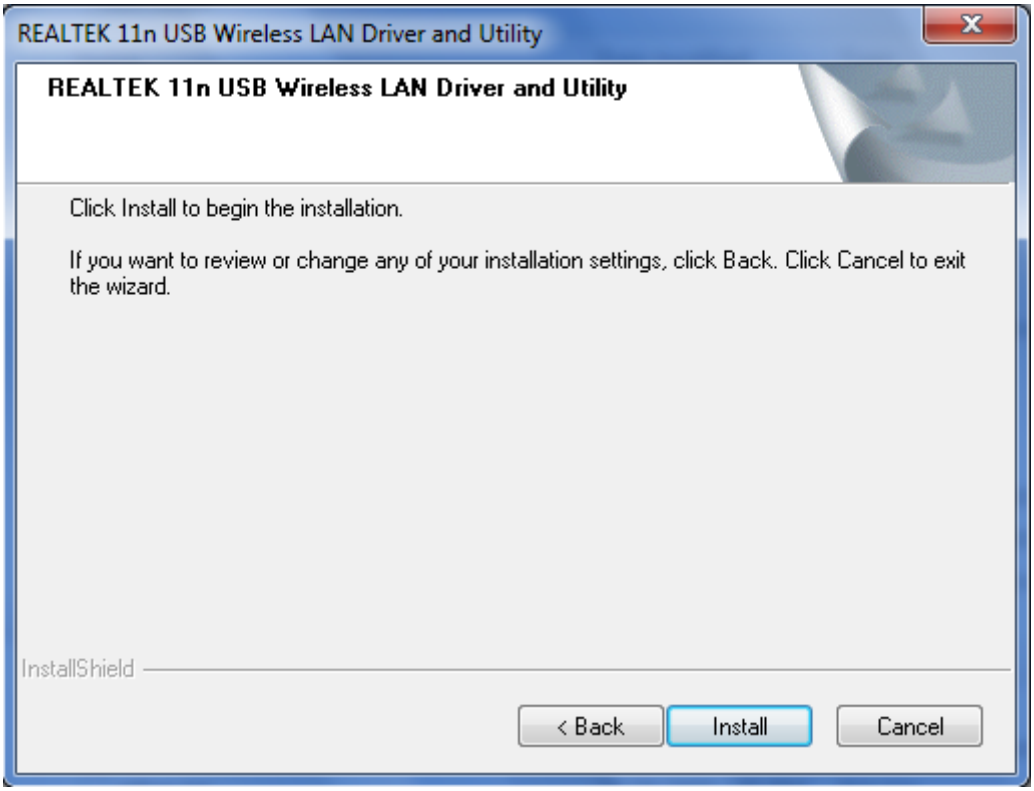
1. Insert the CD into your CD-Rom, and find the setup driver in the CD. Then click the setup icon to start the installation.
2. The language-selecting window pops up. Please select the language you use and click “Next”.



3. The welcome window pops up. Click the “Next” button to proceed.

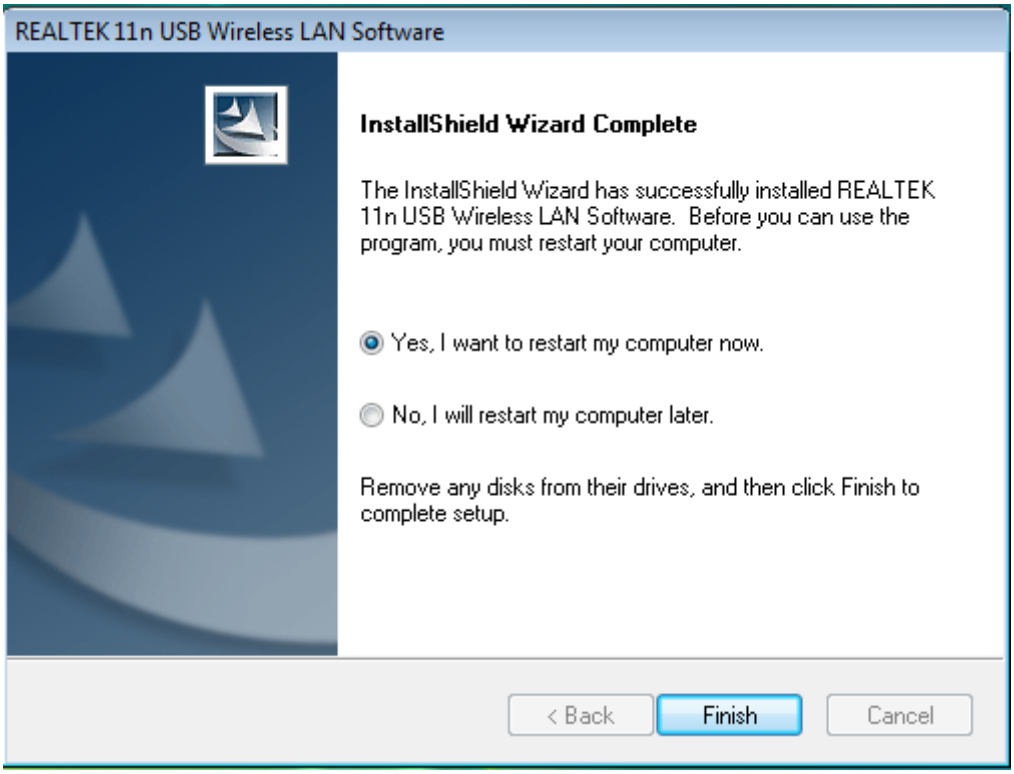


4. Click the “Install” button to start installing.



5. Please wait again while installation

6. After all the steps above, you will see the screen below, Select “Yes” or “No” and then click Finish to complete the setup..



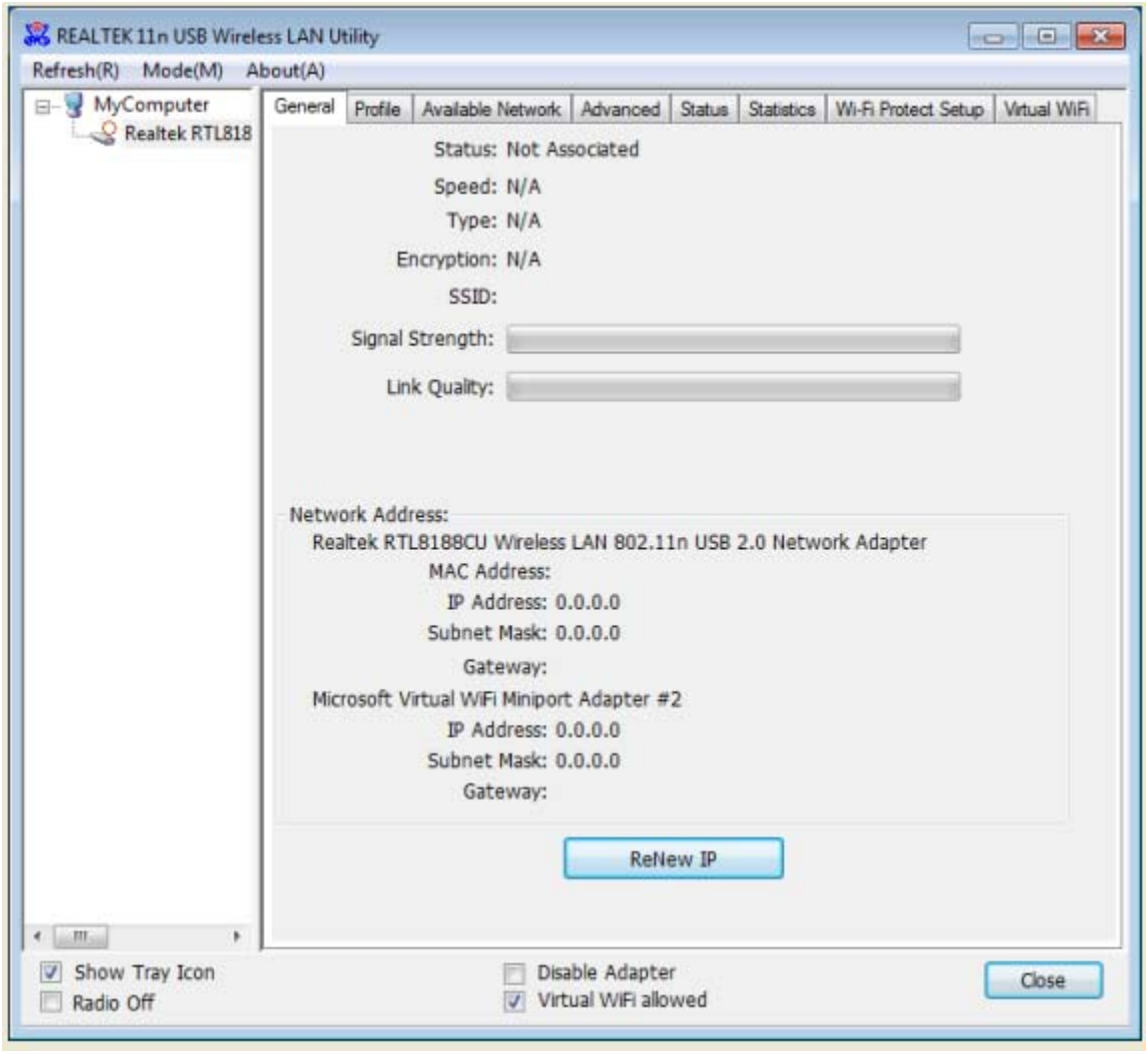
5.3 Management Guide

This chapter describes how to configure your Adapter for wireless connectivity on your Wireless Local Area Network (WLAN) and use the data security encryption features.

After Installing the Adapter, the Adapter’s tray icon will appear in your system tray. It appears at the bottom of the screen, and shows the signal strength(the icon will change its color) and the received signal strength indication (RSSI).

5.3.1 Interfaces

After the driver installation, the icon  will appear on your desktop. Double click this icon and the following interface appears:

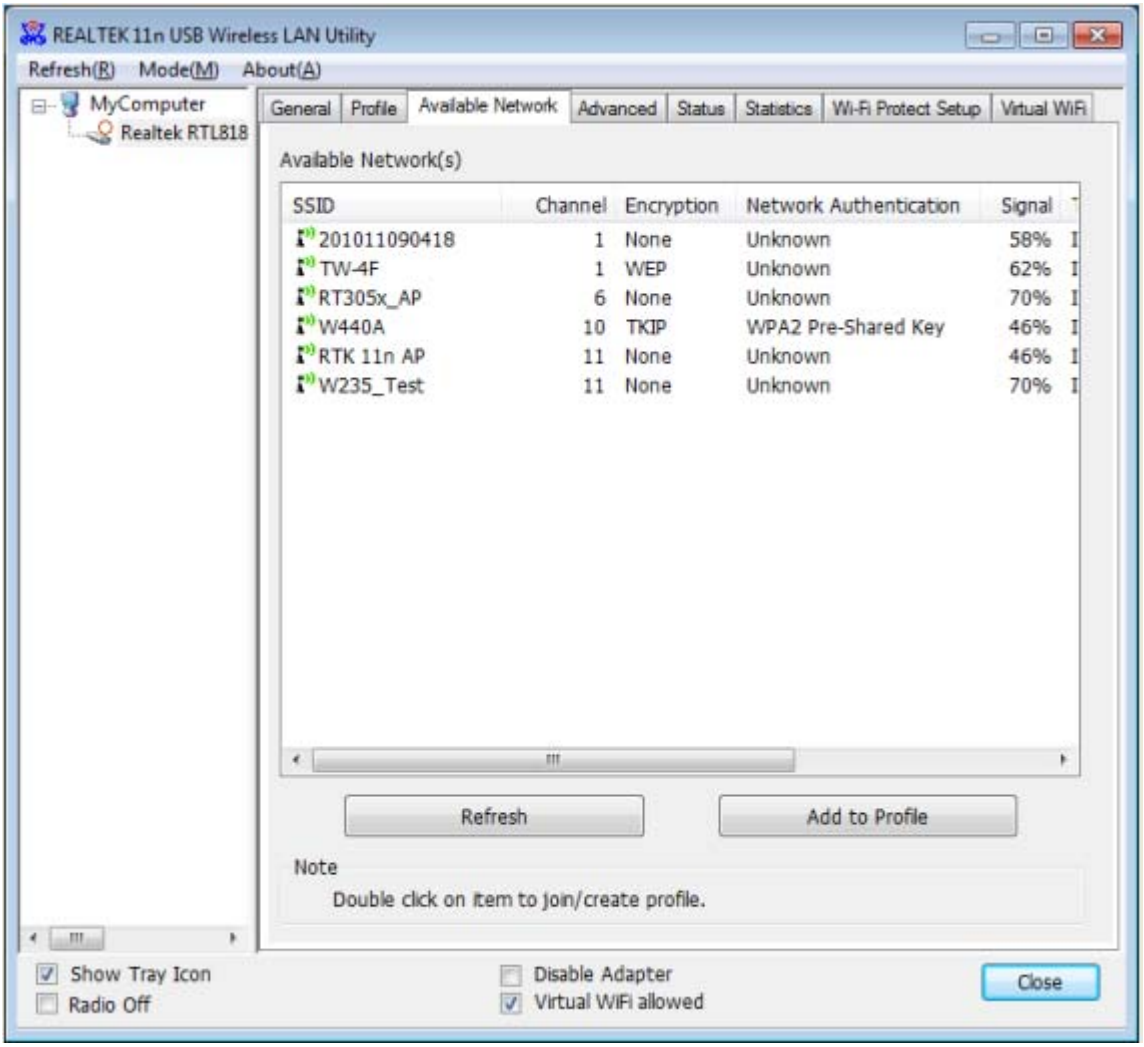


1. **Functional Buttons** : on top of the window. You can click each button to access each configuration window.
2. **Configuration Column** : Center of the Utility window. Make your changes for each function in this part.
3. **Optional Table** : “Show Tray Icon”, ”Disable Adapter”, ”Radio off” and “Virtual WiFi allowed”.

5.3.2 Available Network

The above picture shows you the available wireless network lists. The Utility will connect to a wireless network with best signal strength automatically. You can refresh the connecting network by clicking on the network name and click the **Refresh** button. In the center of the Utility windows, you

will see detail information of each network.



Available Network Information:

Items	Information
SSID	The name of the IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
Channel	Display current channel in use.
Encryption	Shows the encryption mode in use. There are total 4 modes: None, WEP, TKIP and AES.
Network Authentication	Shows the authentication mode in use.
Signal	This percentage shows the strength of the signal.
Type	The type of network and the station currently connected are shown

	here. The options include : **Infrastructure** & **Ad-Hoc**
BSSID	The IEEE MAC address of locally-managed, generating from a 46 random code.
Support Rates	Show current rate.

Note:

1) An Infrastructure network contains an Access Point or wireless router. All the wireless devices or clients will connect to the wireless router or access point.

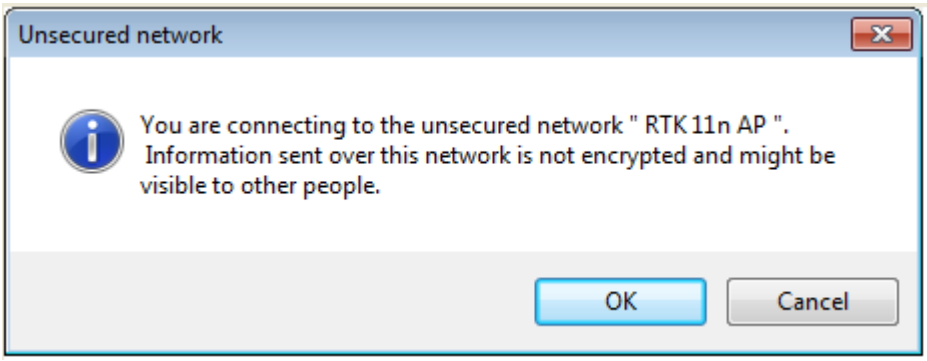
2) An Ad-Hoc network contains only clients, such as laptops with wireless desktop adapters. All the adapters must be in Ad-Hoc mode to communicate.

5.2.3 Profile

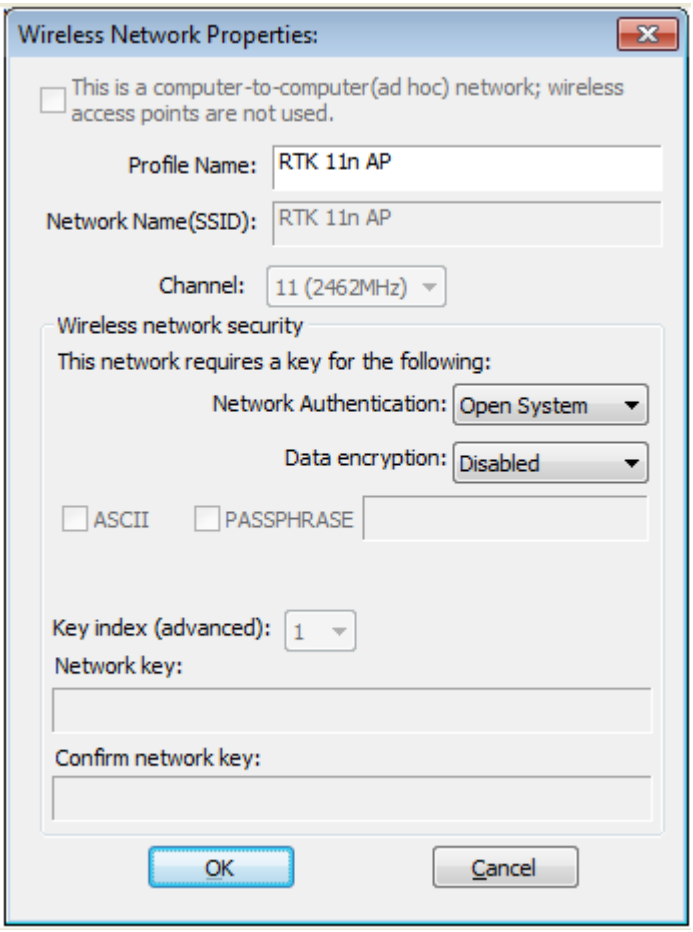
1. Add a new profile:

(1) Selecting an available network in the "**Available Network**" function then click the **Add to Profile** button, or double click the network name. You could also add a new profile quickly by clicking the **Add** button in the "**Profile**" function.

Note: If the network you add to profile is not encrypted, the following "Unsecured network" window will pop up, then Click "OK".



(2) It displays "Wireless Network Properties" dialog box. This profile page allows users to save different wireless settings, which helps users to get access to wireless networks at home, office or other wireless network environments quickly.



In the following dialog box, there are some items:

Items	Information
Profile Name	Identifies the configuration profile .This name must be unique. Note that the profile names are not case-sensitive.
Network Name(SSID)	The IEEE 802.11n wireless network name, using default name defined by system. This field has a maximum limit of 32 characters.

(3). Channel (Country Region Code): six countries to choose. Country channel list:

Country	Channel Range	Country	Channel Range
SPAIN	CH1 ~ CH11	FRANCE	CH1 ~ CH13
CANADA	CH1 ~ CH11	JAPAN	CH1 ~ CH14
ETSI	CH1 ~ CH13	ISRAEL	CH1 ~ CH13

(4) Wireless Network Security

A. Network Authentication

Select the Security tab in the screen above. To define the security mode, select the desired security

mode as follows. There are 7 types supported: Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X, WEP 802.1X, and you can select a type from the drop down list if you click the button beside ”Network Authentication”.

- **Open System:** enable an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match.
- **Shared-key:** only allows the adapter to associate with access points that have the same WEP key.
- **802.1x:** This item appears while the environment is set to an Open authentication with WEP encryption. Mark the checkbox to make the section available. The section is also available in WPA and WPA2 authentication types.
- **Preshared Key(PSK):** This is the shared secret between AP and STA. For WPA-PSK, WPA2-PSK and WPA-NONE authentication mode, this field must be filled with characters longer than 8 and less than 32 lengths. The following dialog appears if you have input invalid values.
- **WEP Key:** Only available when using WEP encryption algorithm. The key must match AP's key. Only using the same cryptographic key to access the computer, the internet can storage, and decryption the information from other computer.

B. Data Encryption:

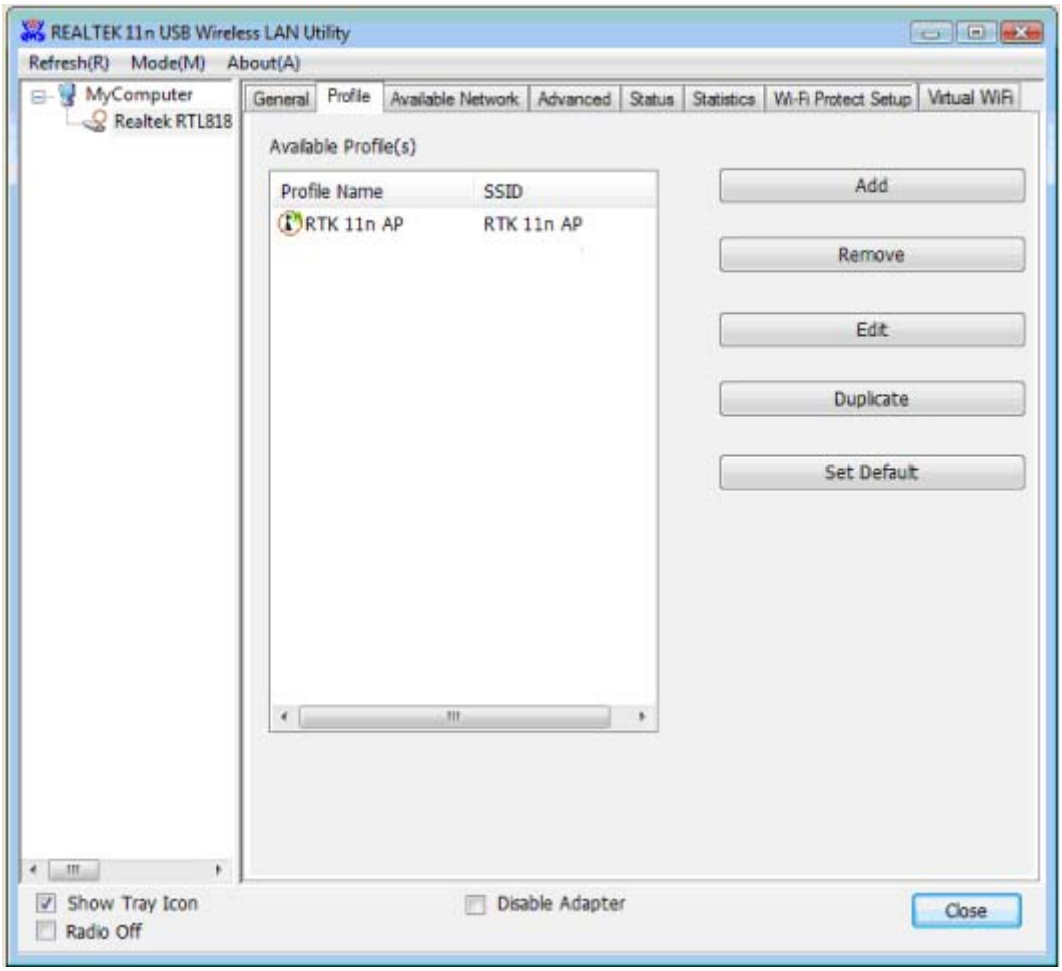
<table>
<tr><td>Data encryption</td><td>There are 4 types supported: Disabled, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open System</td><td>Disabled, WEP</td></tr>
<tr><td>Shared Key , WEP 802.1X</td><td>WEP</td></tr>
<tr><td>WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X</td><td>TKIP, AES</td></tr>
</table></td></tr>
</table>

Note: Select different Security Options, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

- **TKIP:** "Temporary Key Integration communication Protocol", it provide each packet's key mixture, message integration and key reconstruction mechanism. TKIP can use with personal or the enterprise network validation.
- **AES:** “Advanced Encryption Standard”, It is a new method that the wireless transmission of

privacy protection. AES encryption methods provides more careful than TKIP.

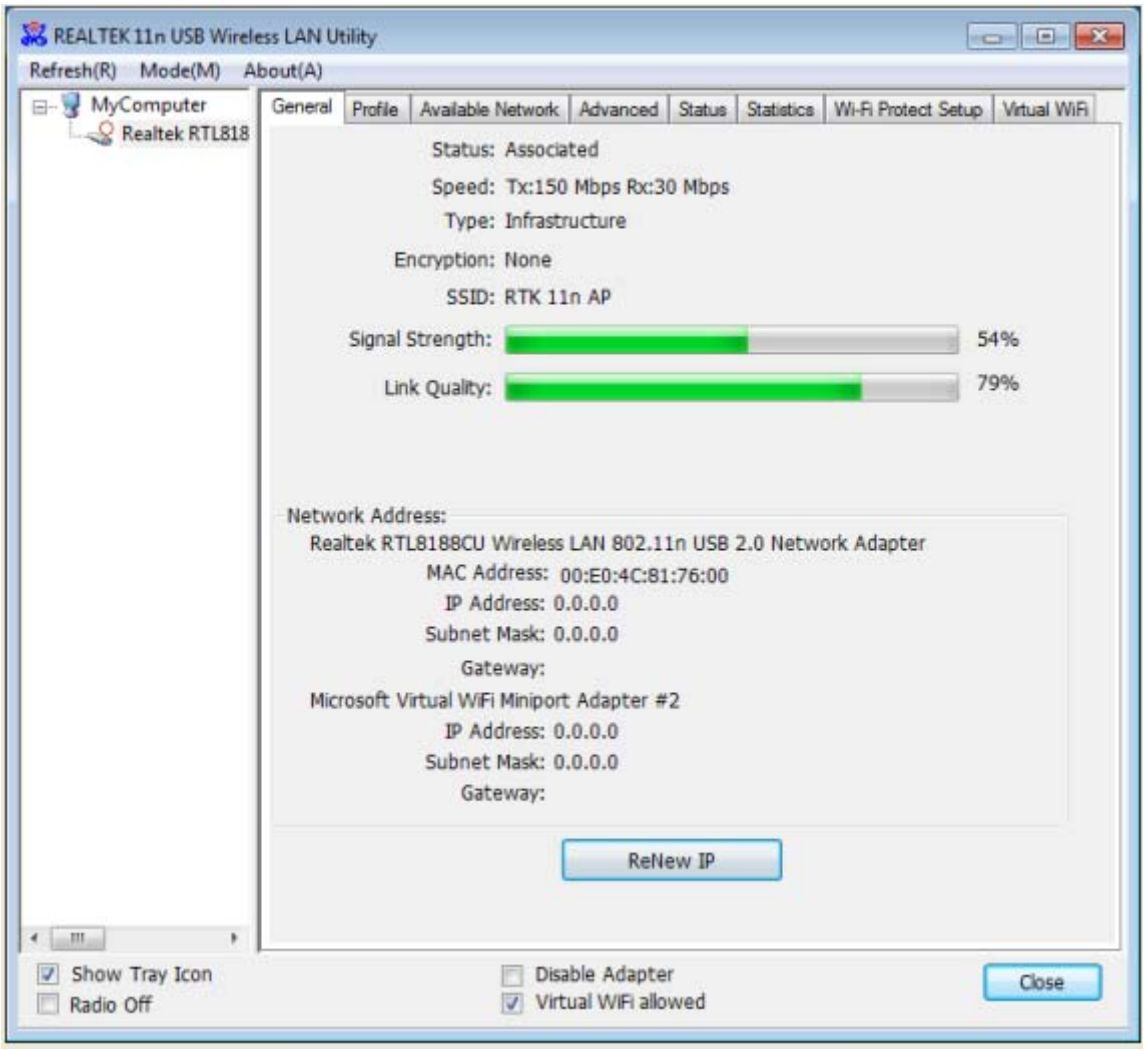
(5) Finish the configuration, and then click “OK”, that network has been added to the profile.



Profile List: The list shows all the profiles you have added before.

Buttons: You can click on these buttons to **Add** a new profile, **Remove**, **Edit**, **Duplicate** or **Set Default** an old profile.

5.3.4 General



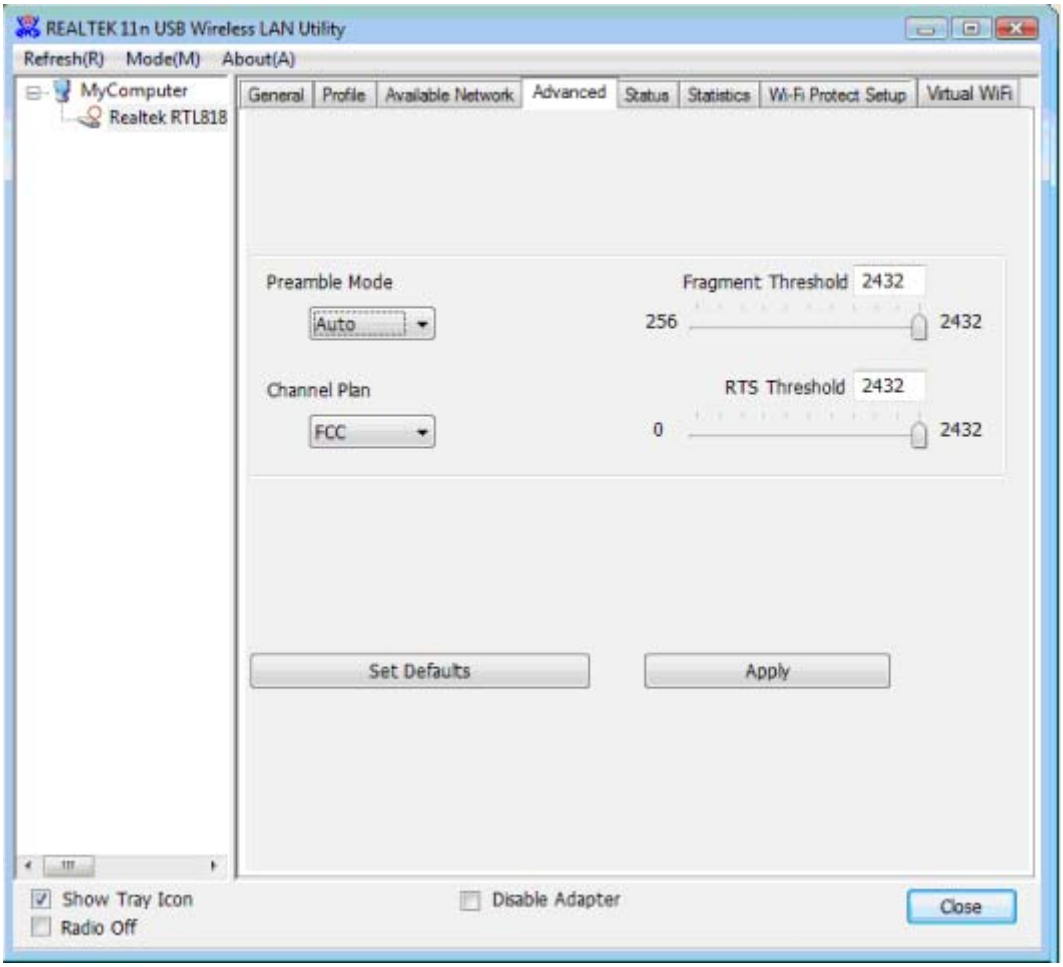
In this window, there are some items as following:

Items	Information
Status	Currently connection status.
Speed	Show current transmit rate and receive rate.
Type	Network type in use.
Encryption	Encryption type in use.
SSID	The name of the IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
Signal Strength	Receive signal strength.
Link Quality	Display connection quality based on signal strength.
Network	5. **MAC Address** : The MAC address of the wireless network adapter.

Address	6. **IP Address** : IP address of current connection. 7. **Subnet Mask** : Subnet mask of current connection. 8. **Gateway** : Gateway of current connection.

5.3.5 Advanced

This screen below allows you to make advanced configuration for the profile. Please refer to the following chart for definitions of each item.



1. Preamble Mode

The length of CRC blocks in the frames during the wireless communication. Select the options from the drop list: (1) Long (2)Short (3)Auto.

2. Channel Plan

The selected Channel: FCC, IC, ETSI, Spain, France, MKK, MKK1, Israel, TELEC, Default.

(Note: The choose between channels function is not allowed in USA.)

3. Threshold

(1) Fragment Threshold

This value should remain at its default setting of 2347. If you experience a high packet error rate,

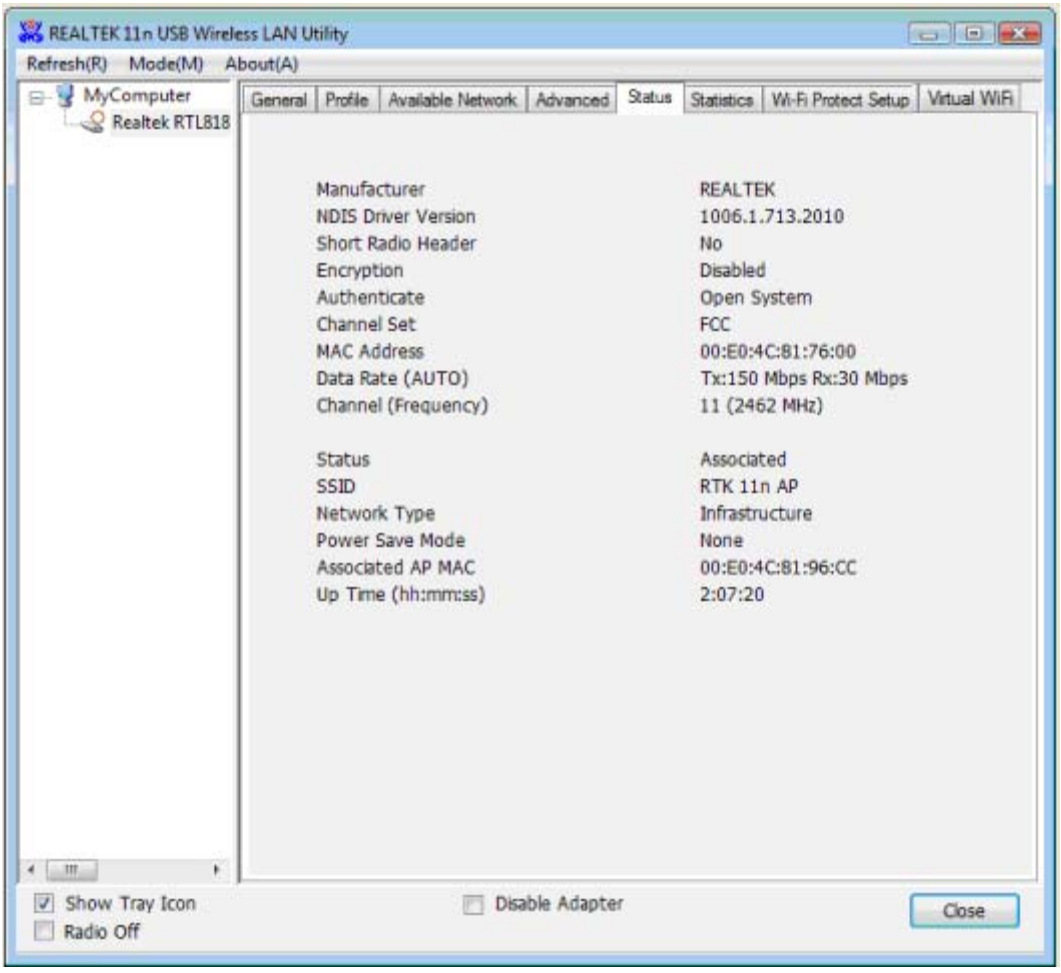
you may slightly increase your fragmentation threshold within the value range of 256 to 2432. Setting the fragmentation threshold too low may result in poor performance.

(2) RTS Threshold

Request To Send Threshold. This value should remain at its default setting of 2346. If you encounter inconsistent data flow, only minor modifications to the value range between 0 and 2432 are recommended.

5.3.6 Status

The Status tab contains general information about the program and its operations.



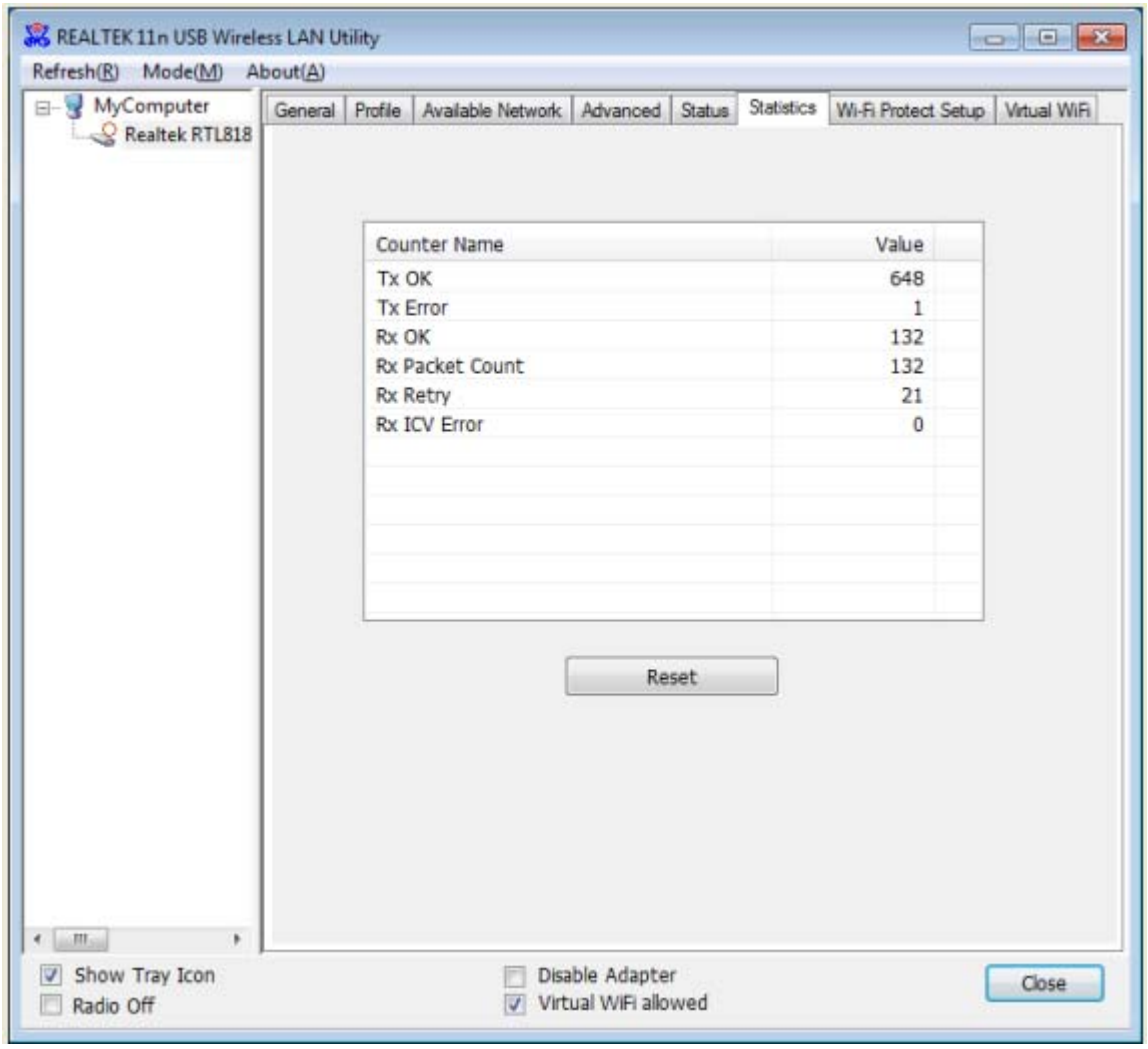
The following table describes the items found on the Status screen.

Items	Information
Manufacturer	The name of manufacturing this product.
NDIS Driver Version	The version of Network Driver Interface Specification.
Encryption	Here displays the encryption type the device is using.
Authenticate	This shows whether the server based authentication is used.

Channel Set	Appears the country you use.
MAC Address	The MAC address of the wireless network adapter.
Data Rate(Auto)	Show current transmit rate and receive rate.
Channel Frequency	Shows the channel in use (1~14).
Status	Current connection status.
SSID	The SSID of the wireless system.
Network Type	The type of network and the station currently connected are shown here. The options include : Infrastructure, Ad Hoc
Power Save Mode	The power save mode have three mode: Max, Min, None
Associated AP MAC	The MAC Address of associated AP.
Up Time	Record life time.

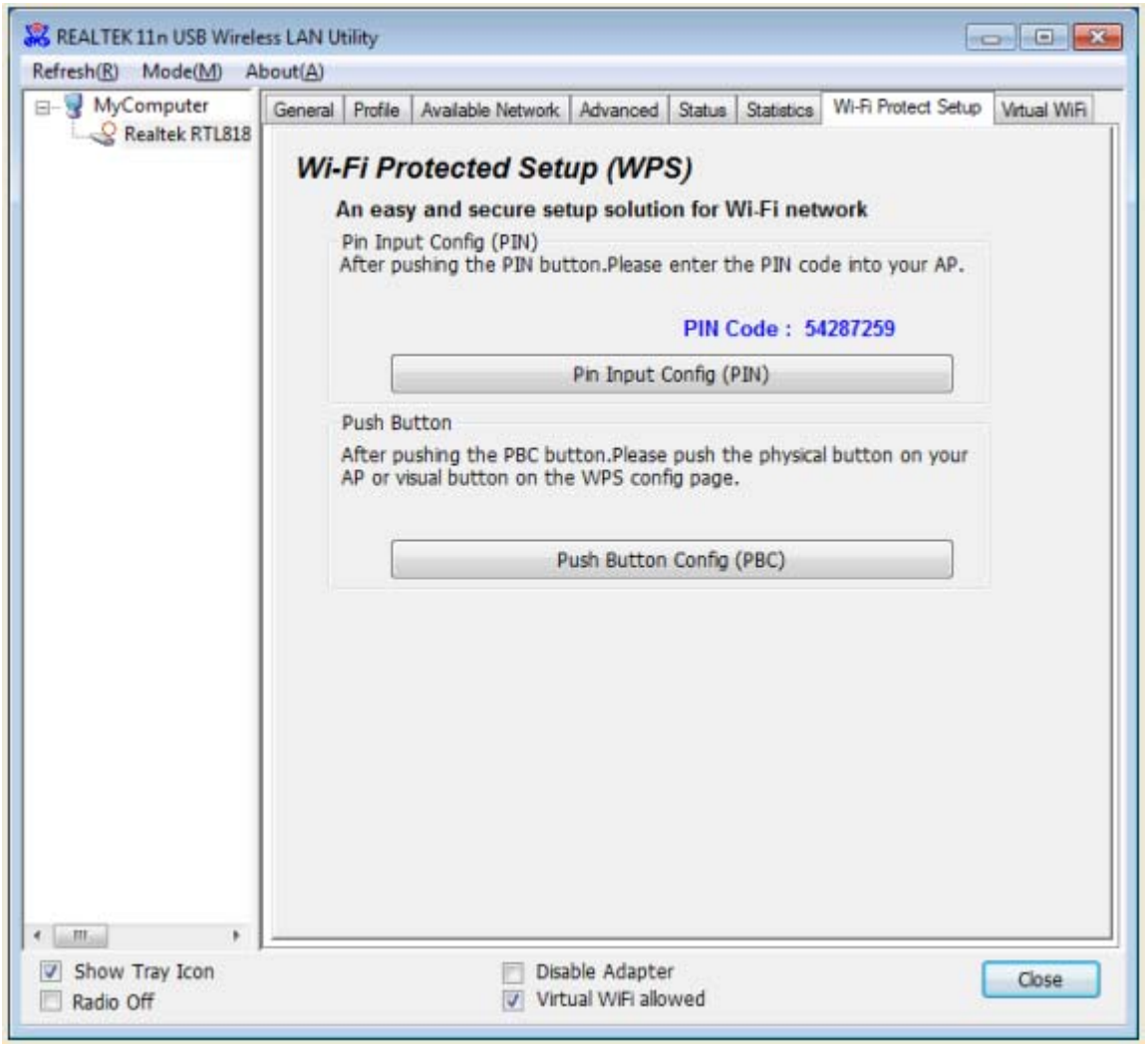
5.3.7 Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates the MIB counters into a format easier for user to understand. It show receiving and transmitting statistical information about the following receiving and transmitting diagnostics for frames received by or transmitted to the wireless network adapter.



Items	Information
TX OK	Successfully transmitted frames numbers.
TX Error	Frames numbers transmitting with error.
RX OK	Successfully received frames numbers.
Rx Packet Count	The packets of receiving frames.
RX Retry	Frames numbers re-receiving.
RX ICV Error	Integrity Check Value receiving with error.
Reset Counter	Reset counters to zero.

5.3.8 Wi-Fi Protect Setup



The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This adapter supports the configuration setup using PIN configuration method or PBC configuration method. If the wireless card supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless card and router using either Push Button Configuration (PBC) method or PIN method.

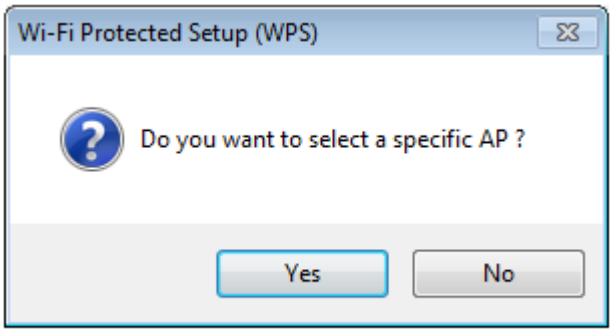
Here we will introduce two ways to configure the QSS

(QSS is known as rapid security settings, by pressing the wireless router and wireless card on the QSS button to automatically set up WPA2 secure connection level without the router or network adapter management software to conduct the cumbersome interface settings, greatly simplifying the operation of the wireless security settings.)

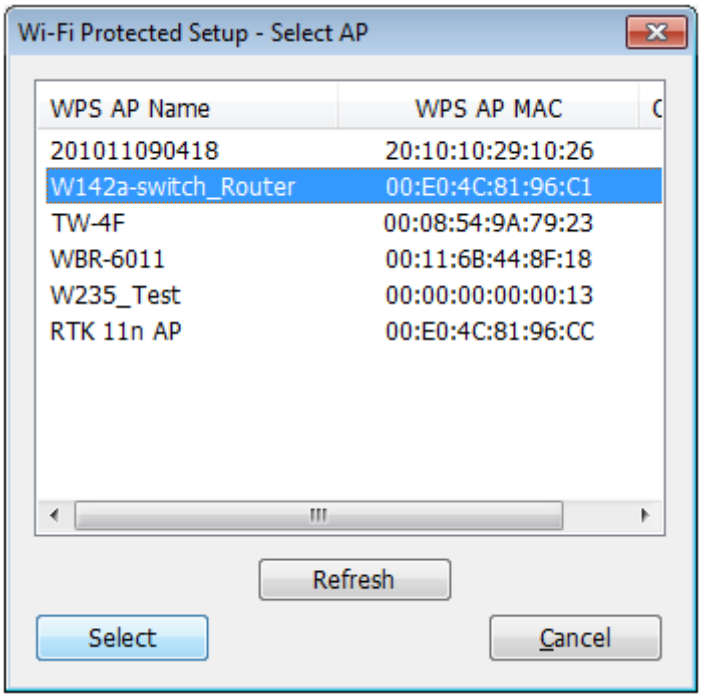
Pin Code: 8-digit numbers. It is randomly generated from system

(1) PIN method

Click the button “Pin Input Config (PIN)”, and then come to the following figure.

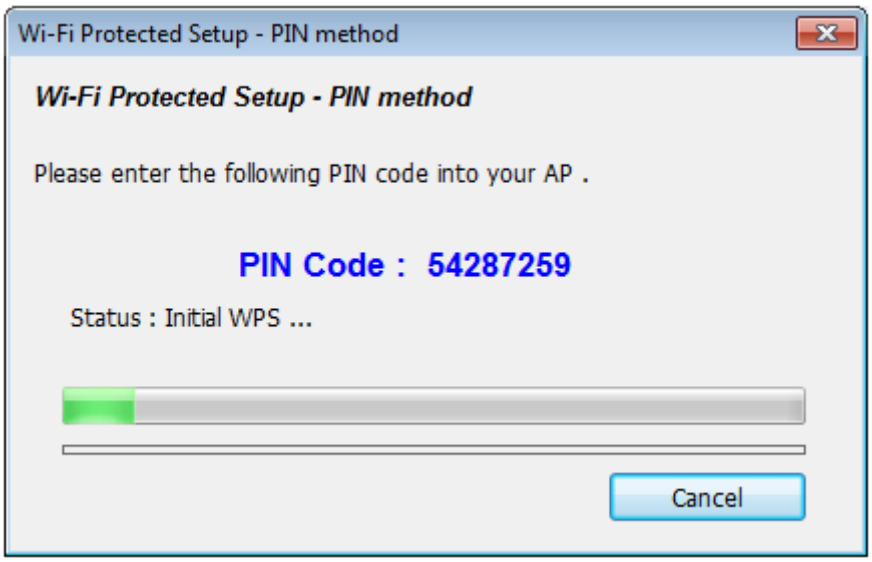


Click the button “Yes”, you can select one of the AP.

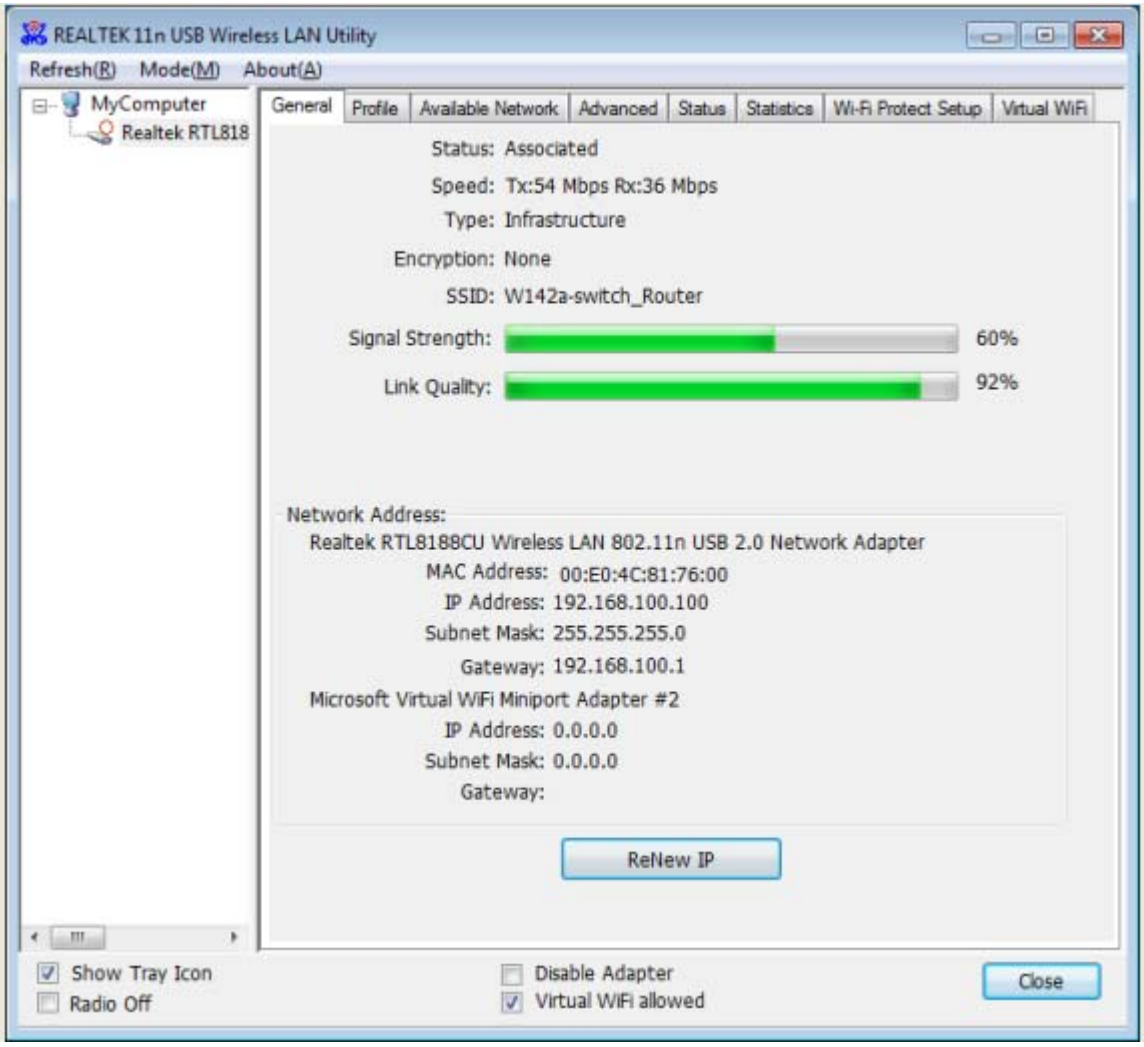


When the following interface pops up, double click the Internet WEB browser icon on your desktop screen. Type the IP address of you selected Router/AP into the URL and press “Enter”, and then you can enter the configuration.

Please enter the WPS (Wi-Fi) configuration page, type the PIN code of adapter and click confirm button to build WPS connection.

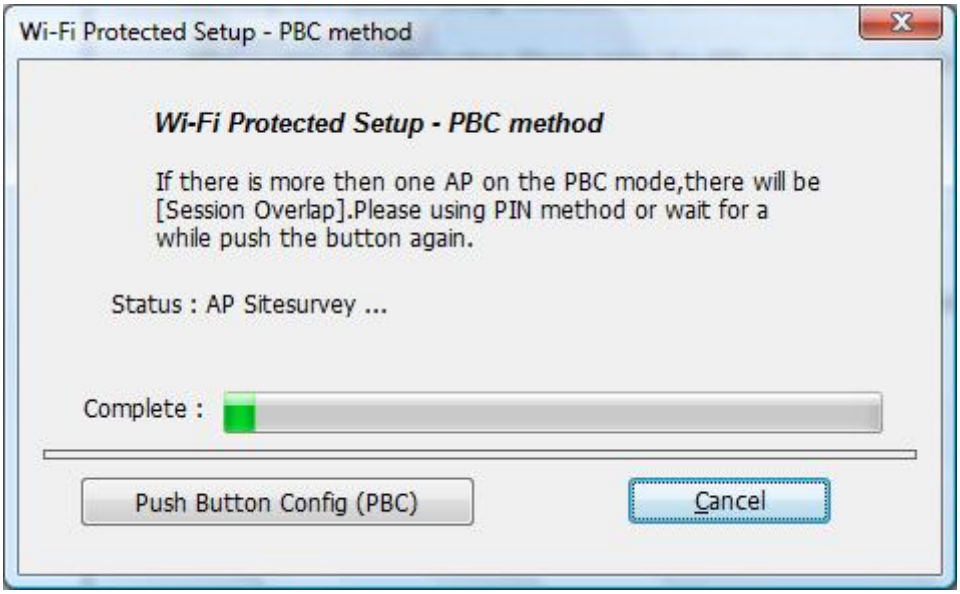


When the “General” window appears, WPS is configured successfully.



2. **PBC (Push Button Configuration) method**

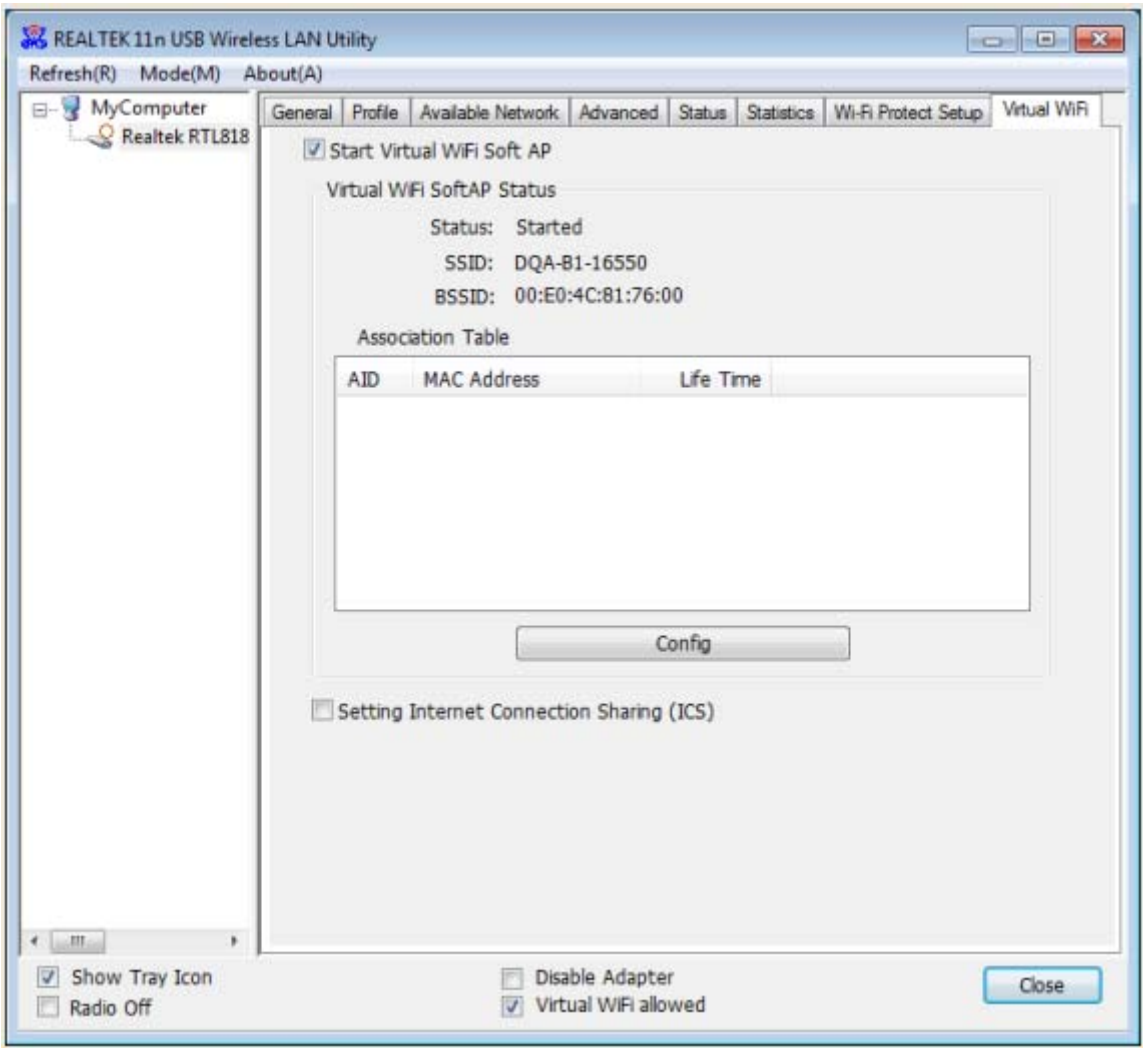
After pushing the PBC button, Please push the physical button on your AP or visual button on the WPS config page, then come to the following figure.



Please enter the WPS (Wi-Fi) configuration page of your desired router/AP, and then start PCB connection.

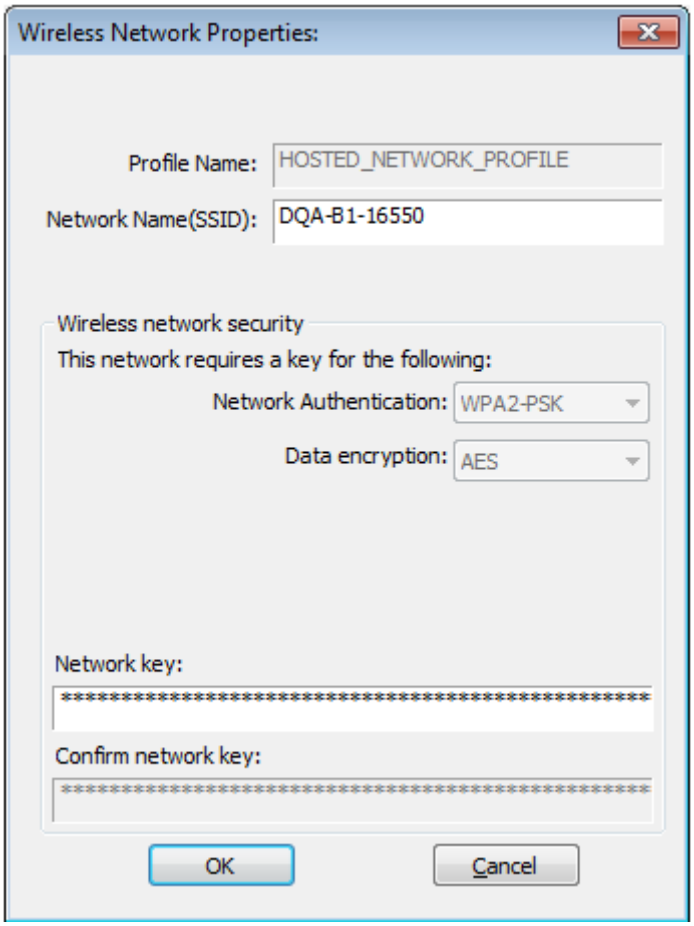
5.3.9 Virtual WiFi

Click the check box of “Virtual WiFi disallowed” at the bottom of the window to activate Virtual WiFi. Virtual WiFi , abbreviated to VWiFi, is a software layer that abstracts the wireless LAN card hardware into multiple virtual adapters. The software handles the connections of each adapter to ensure every adapter has an opportunity to connect to their respective networks limited by time. And you act as if you have multiple WLAN hardware adapters working independently.

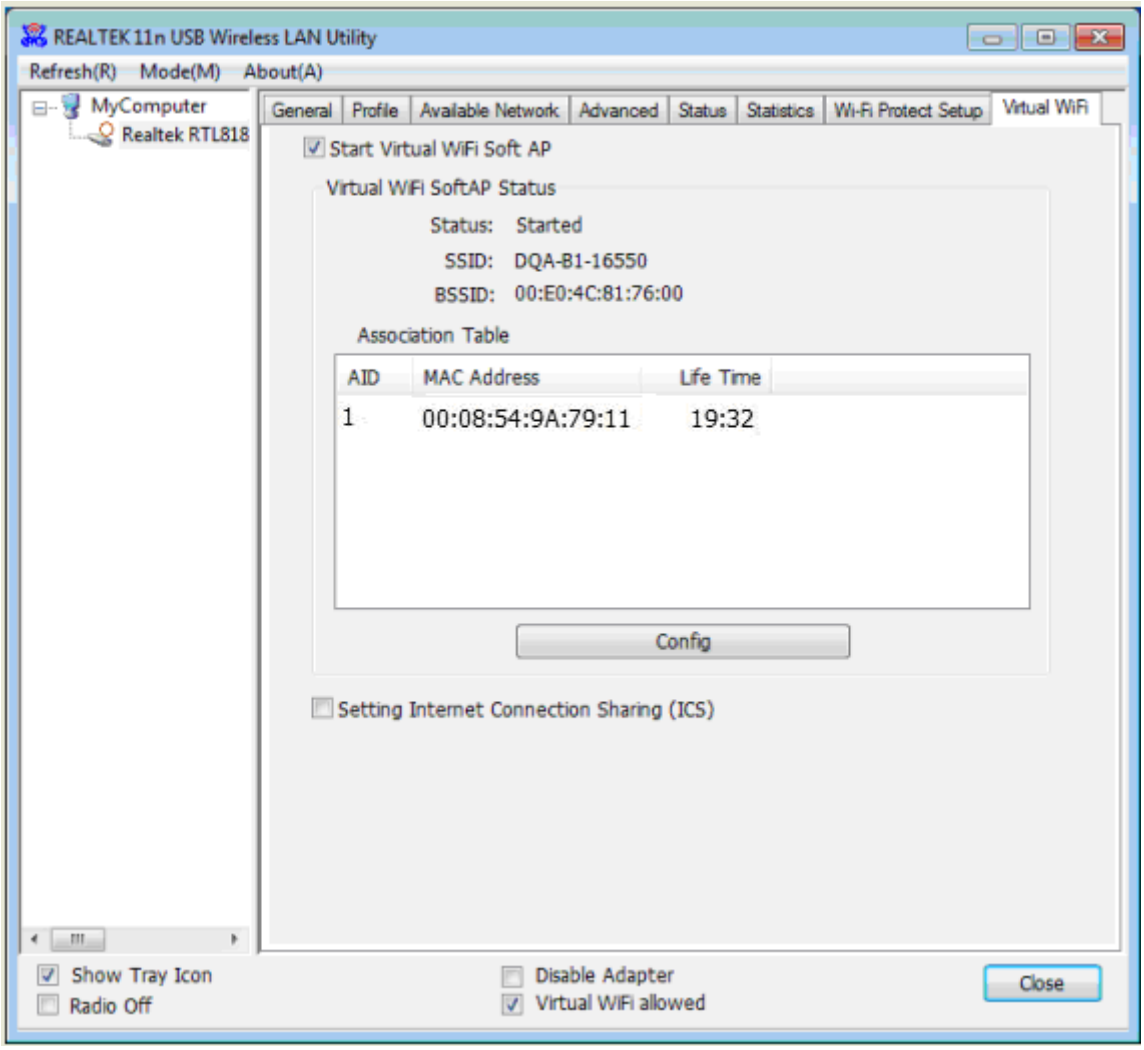


Items	Information
SSID	The name of connected IEEE 802.11 wireless network. This field has a maximum limit of 32 characters.
BSSID	a locally administered MAC address of the wireless network generated from a 64-bit random number
Association Table	It is the list of joined stations to this adapter
AID	Association ID
Mac Address	It is the six two-digit numbers that assemble the MAC address of respected joined station
Life time	It is the timer that counts down from 10 minutes whenever the adapter connects the station successfully. If an STA associated to SW adapter does not have any interaction with the adapter in 10 minutes, it will be disassociated from the Infra-structure BSS
config	A dialog of this adapter is shown for configuration modification

Click config button and the network properties interface pops up. You can key in the network key to set up the security accessing authority and click OK to finish the configuration.

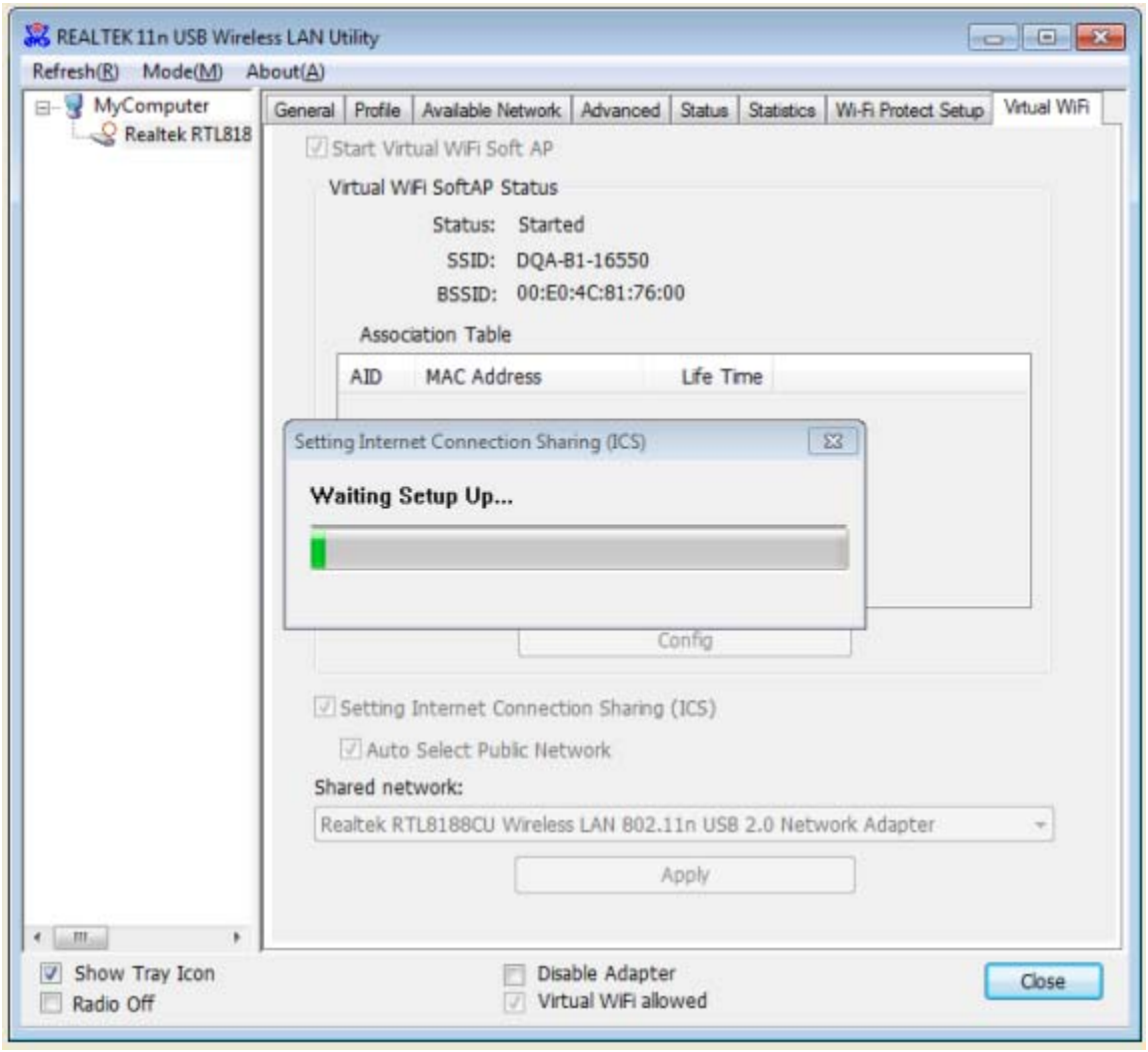


The other connecter can share the same network by typing in the network key. In this way the connecter is connected to the adapter.

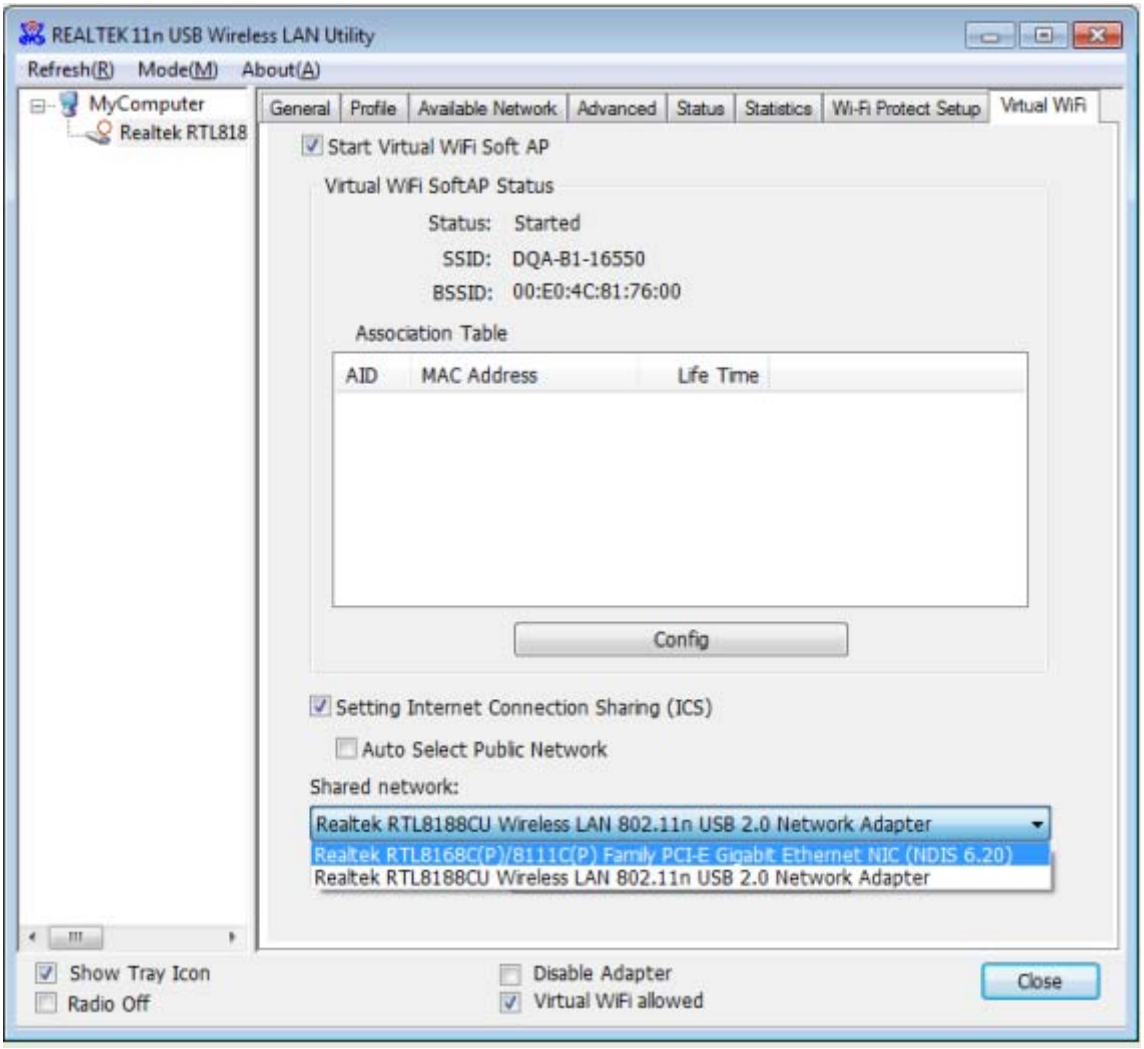


Setting Internet Connection Sharing(ICS)

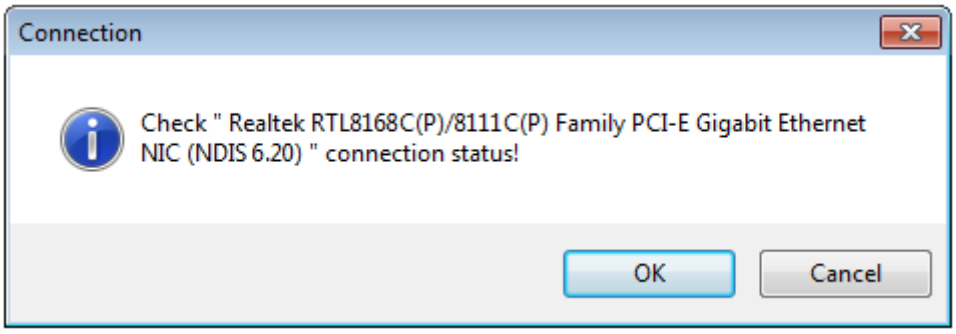
1. Click the checkbox of ICS, a box asks for waiting will pop up, and “Auto Select Public Network” is enabled automatically.



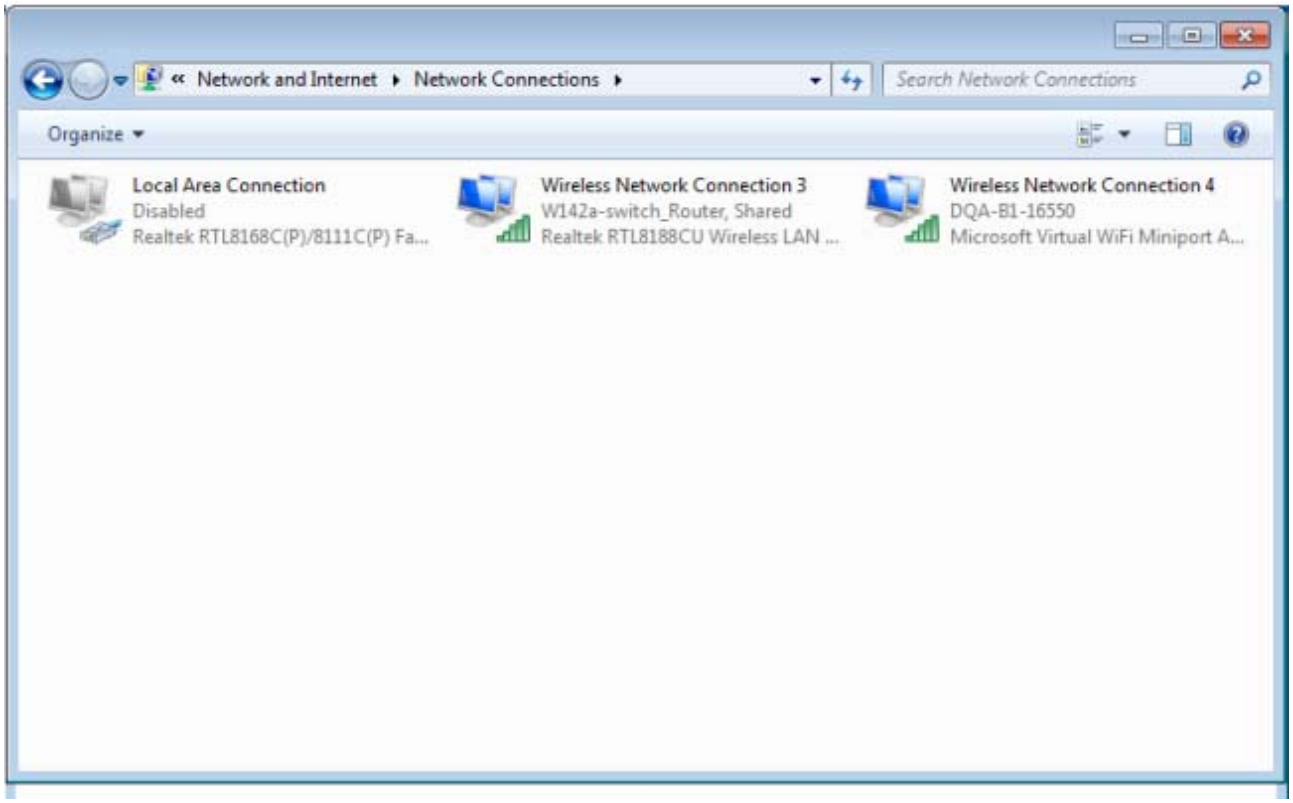
2. If you want to select the “Shared network” manually, you can enable “Auto Select Public Network” and choose the “Shared network” you want by the drop-down list as follow:



3. After selecting the shared network, click the button “Apply”, and then Prompt box pops up.



4. Select “OK”. When the connection is successful, you will find that the tray “Local Area Connection” has been changed.

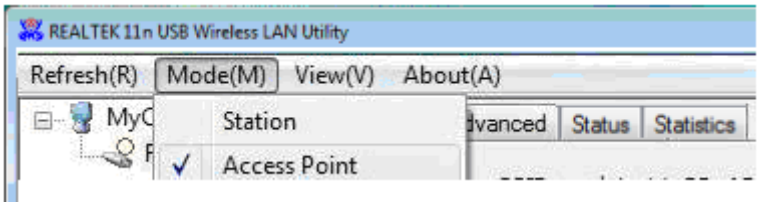


5.4 AP mode management guide for Windows 7

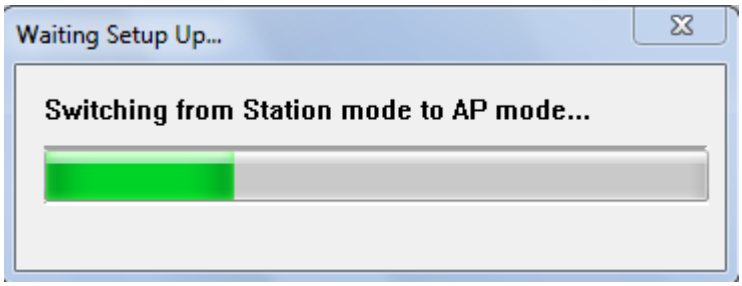
If you wish to share the Internet access with the wireless stations in your environment, you can configure this wireless adapter as a software access point (Soft AP). In this mode, this wireless adapter becomes the wireless access point that provides local area network and Internet access for your wireless stations.

5.4.1 General

To use this adapter as an access point, please click the “Mode” on **Functional Menu** and select **“Access Point”**.



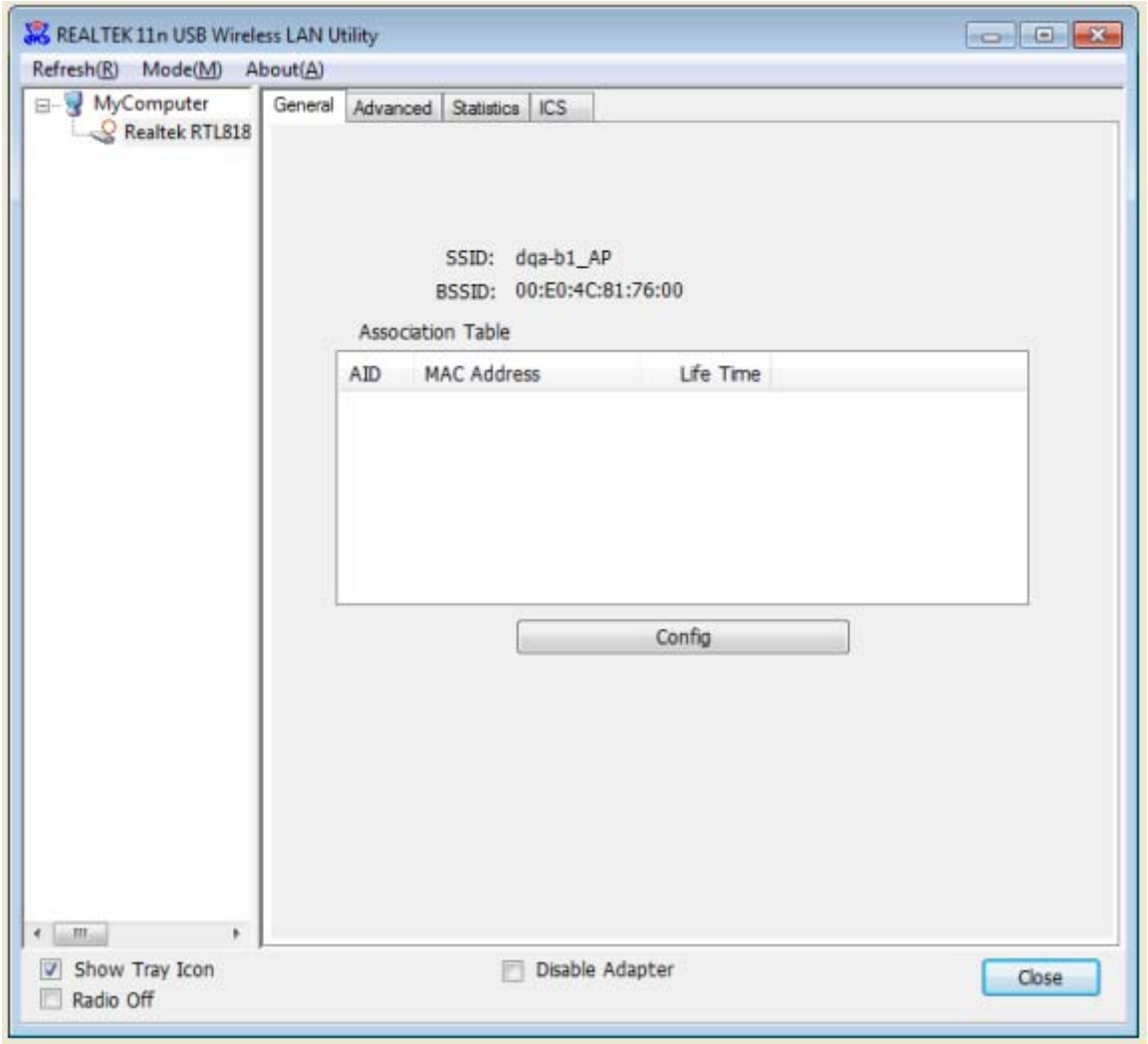
At this time a box pops up:



Then switching from station mode to AP: At the same time, you will find that the icon on the system tray is changed form 

to 

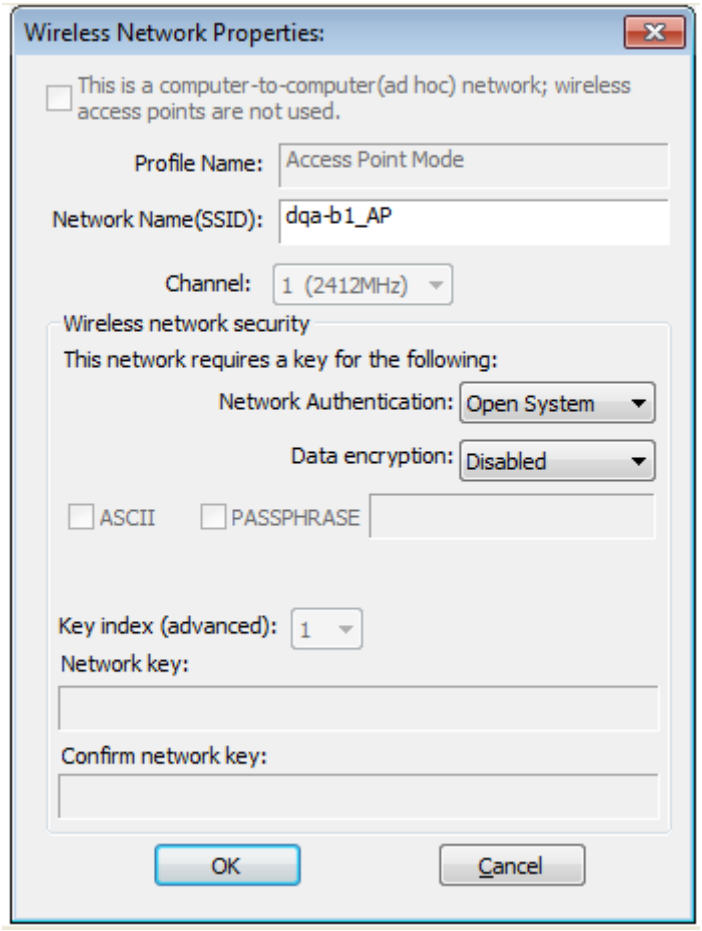
Please refer to the following information about this AP-mode utility.



Items	Information
SSID	AP name of user type.
BSSID	The IEEE MAC address of locally-managed, generating from a 46 random code.

AID	Raise value by current connection.
MAC Address	The station MAC address of current connection.
Life Time (mm:ss)	Record life time.

Click the “Config” button, then you can configure the wireless network properties. This page provides overall configuration to this adapter.



SSID: AP name of user type.

Channel: Manually force the AP using the channel. System default is channel 1.

Security Setting: Authentication mode and encryption algorithm used within the AP. System default is no authentication and encryption.

Cancel: Cancel the above changes.

OK: Apply the above changes.

A. Network Authentication

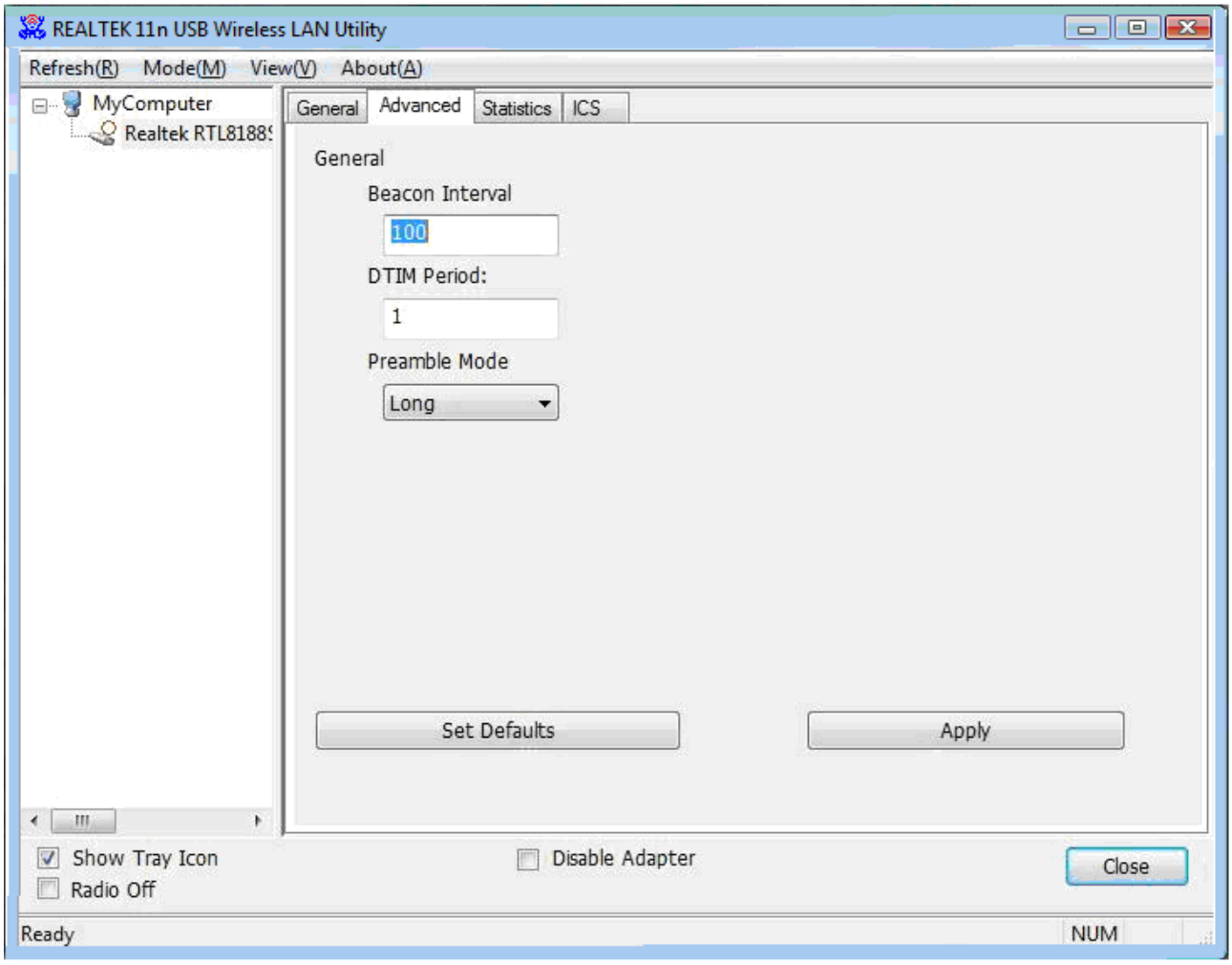
Select the Security tab in the screen above. To define the security mode, select the desired security mode as follows. There are 4 types supported: Open System, Shared Key, WPA-PSK, WPA2-PSK. Please select a type from the drop down list.

B. Data Encryption:

<table>
<tr><td>Data encryption</td><td>There are 4 types supported: Disabled, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open System</td><td>Disabled, WEP</td></tr>
<tr><td>Shared Key , WEP 802.1X</td><td>WEP</td></tr>
<tr><td>WPA-PSK, WPA2-PSK, and WPA 802.1X, WPA2 802.1X</td><td>TKIP, AES</td></tr>
</table>
</td></tr>
</table>

Note: Select different Security Options, the configurations are different; you can select the appropriate security option and configure the exact key as your need.

5.4.2 Advanced

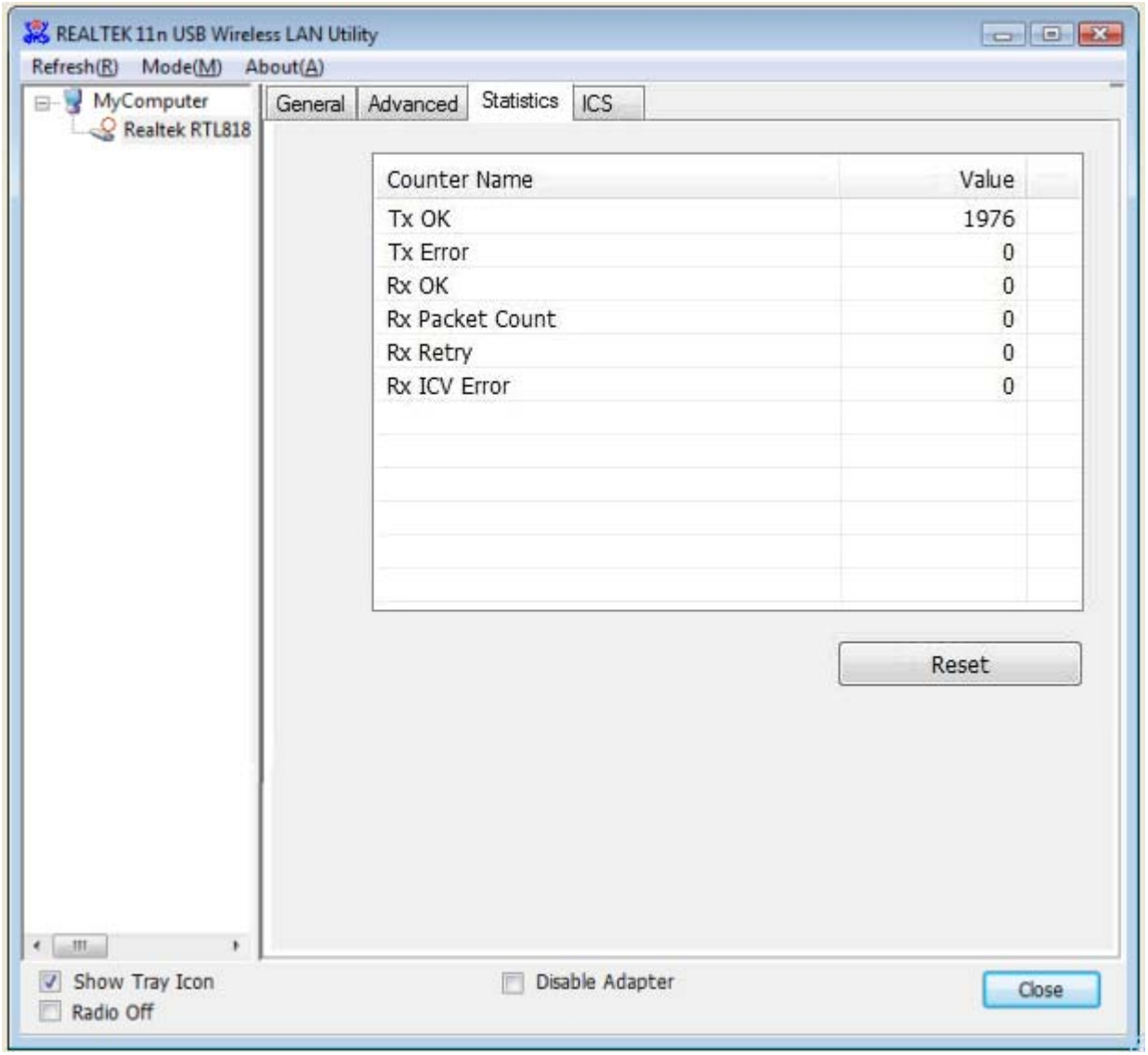


Items	Information

Beacon Interval	Beacon frequency spacing.
DTIM Period	Delay transmission indicator map (DTIM) is enabled for power management of the client. If any client power management is enabled, the DTIM should be retained for 1 (the default). Support this parameter range from 1 to 255.
Preamble Mode	Select the options from the drop list,(Long / Short).
Set Defaults	Setting the default value of General.
Apply	Apply the above changes.

5.4.3 Statistics

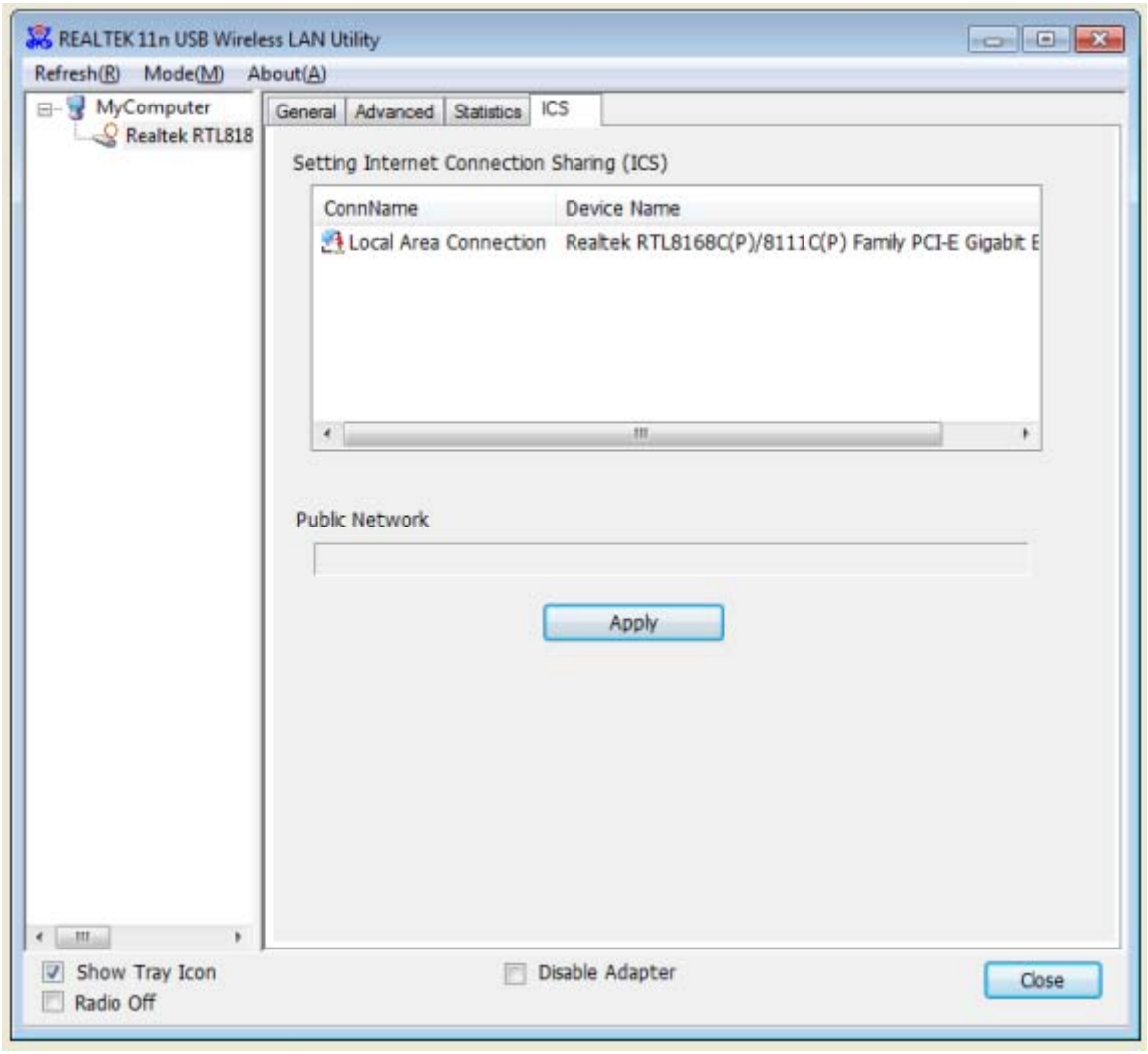
Statistics page displays the detail counter information based on 802.11 MIB counters.



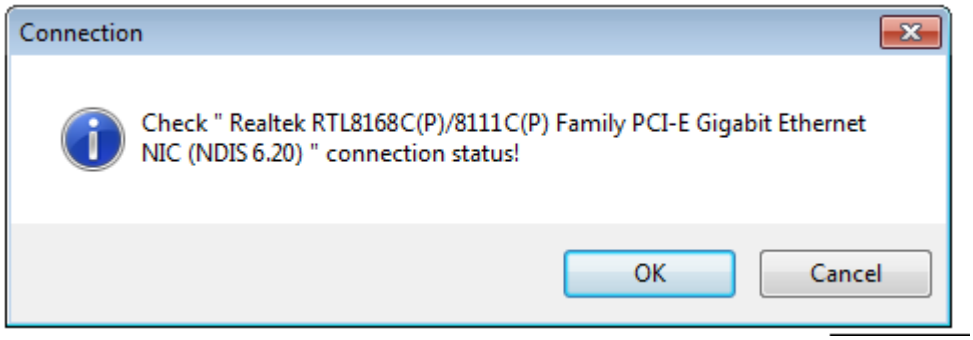
Items	Information
TX OK	Successfully transmitted frames numbers.
TX Error	Frames numbers transmitting with error.

RX OK	Successfully received frames numbers.
Rx Packet Count	The packets of receiving frames.
RX Retry	Frames numbers re-receiving.
RX ICV Error	Integrity Check Value receiving with error.
Reset Counter	Reset counters to zero.

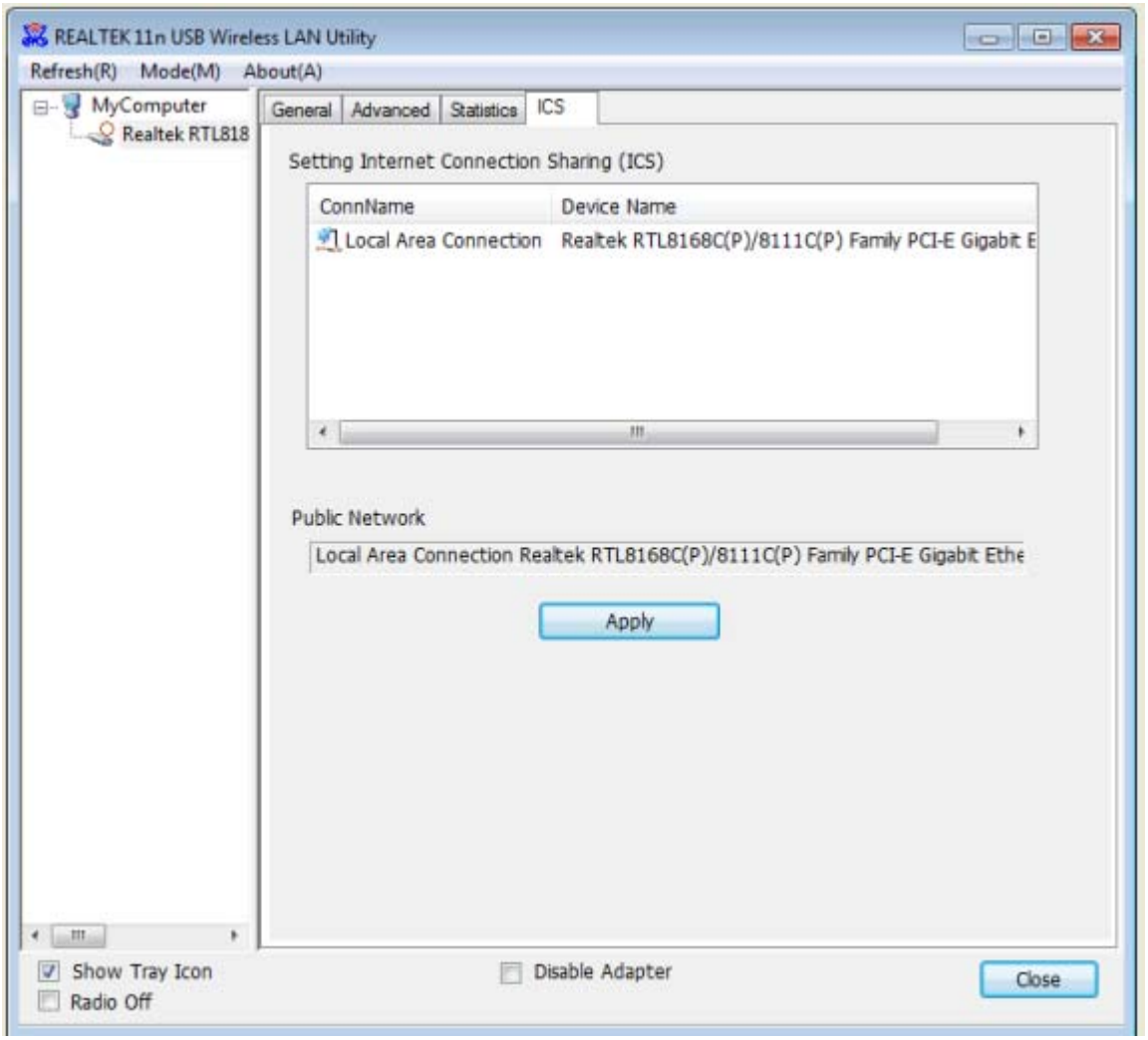
5.4.4 ICS



Click the button “Apply”, then a dialogue box appears and asks for checking the connection status appears.



Select “OK”, then the Internet connection is sharing.



Appendix A: Specifications

Standard
IEEE 802.11n draft 2.0, IEEE 802.11g, IEEE 802.11b
Interface
Complies with USB 2.0
Security
64/128-bit WPA , WPA2
Receiver Sensitivity
802.11n Typical -68 dBm
802.11g Typical -73 dBm
802.11b Typical -84 dBm
Channel
USA 11, Europe 13
Transmit Power
16 dBm typically @ 802.11b
14 dBm typically @ 802.11g
13 dBm typically @ 802.11n
Network Data Rate
802.11b: 1,2,5.5 and 11 Mbps
802.11g: 6,9,12,18,24,36,48 and 54 Mbps
802.11n: up to 150 Mbps
Range Coverage
Indoor 35~100 meters
Outdoor 100~300 meters
Temperature
Operating: 0°C ~ 40°C (32°~104°F)
Storage: -20°C ~ 70°C (-4°~158°F)
Humidity
Operating: 10% ~ 90% RH, non-condensing
Storage: 5%~90% RH, non-condensing
Emission
FCC, CE, VCCI Class B

Appendix B: Glossary

- **802.11b -** The 802.11b standard specifies a wireless product networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **Ad-hoc Network -** An ad-hoc network is a group of computers, each with a Wireless Adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.
- **DSSS -** (Direct-Sequence Spread Spectrum) **-** DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need of retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).
- **Infrastructure Network -** An infrastructure network is a group of computers or other devices, each with a Wireless Adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.
- **SSID -** A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate

with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

- **WEP -** (Wired Equivalent Privacy) - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.
- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN -** (Wireless Local Area Network) - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
- **WPA -** (Wi-Fi Protected Access) **-** A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server