NETSCOUT 802.11ac Network USB Adapter D1080-Z1 User Guide

Version: 1.0
(May, 2017)

Federal Communication Commission Interference Statement

FCC Part 15

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 or more 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.
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 user's authority to operate the equipment.

Note: The manufacturer is not responsible for any Radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment has been SAR-evaluated for use in hand. SAR measurements are based on a 50mm spacing from the body and that compliance is achieved at that distance.

RED Compliance Statement

Safety

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

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

‣ RF Exposure Information (SAR)

This device meets the government's requirements for exposure to radio waves. This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

The exposure standard for wireless device employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6W/kg. *Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the poser required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output.

SAR compliance has been established in the host product(s) (laptop computers), tested at 50mm separation distance to the human body, and tested with USB slot configurations including Horizontal-UP, Horizontal-Down, Vertical-Front, Vertical-Back, Tip. This device can be used in host product(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics.

The highest SAR value, tested per FCC RF exposure guidelines for USB dongle, as described in this user guide, is 1.19 W/kg. The FCC has granted an Equipment Authorization for this device with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this device is on file with the FCC and can be found under the Display Grant section of www.fcc.gov/oet/ea/fccid after searching on FCC ID: NDD9578221212.
This USB dongle transmitter is approved for use in typical laptop computers. To comply with FCC RF exposure requirements, this USB dongle should not be used in other devices or certain laptop and tablet computer configurations where the USB connectors on the host computer are unable to provide or ensure the necessary operating configurations intended for the device and its users or bystanders to satisfy RF exposure compliance requirements. This USB dongle should be installed and operated with minimum distance 50mm between the radiator & your body.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage;

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:

(i) The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;

(iii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and

The high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

DFS (Dynamic Frequency Selection) products that operate in the bands 5250- 5350 MHz, 5470-5600MHz, and 5650-5725MHz.

Avertissement:

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est reserve uniquement pour une utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux;

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer a la

imitation P.I.R.E.;

(iii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer a la limitation P.I.R.E specifiee pour l'exploitation point a point et non point a point, selon le cas.

This EUT is compliance with SAR for general population/uncontrolled exposure limits in IC RSS-102 and had been tested in accordance with the measurement methods and procedures specified in IEEE 1528 and IEC 62209.
This equipment should be installed and operated with minimum distance 5cm between the radiator and your body. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet appareil est conforme aux limites d'exposition DAS incontrolee pour la population generale de la norme CNR-102 d'Industrie Canada et a ete teste en conformite avec les methodes de mesure et procedures specifiees dans IEEE 1528 et IEC 62209.
Cet appareil doit etre installe et utilise avec une distance minimale de 5cm entre l'emetteuret votre corps. Cet appareil et sa ou ses antennes ne doivent pas etre co-localises ou fonctionner en conjonction avec tout autre antenne ou transmetteur.
Body SAR: 1.19 W/kg

Table of Contents

Chapter I: Product Information

1-1 Introduction and Safety Information

Thank you for purchasing the NETSCOUT 802.11ac Network USB Adapter, an extreme high-speed 802.11a/b/g/n/ac dual band wireless network adapter! Excepting common wireless standards 802.11a/b/g/n, this wireless network adapter is also 802.11ac compatible - data transfer rate is 867Mbps, and that's sixteen times faster than 802.11g wireless network! 802.11ac also provides wider wireless coverage, so you don't have to worry if your computer is far from your wireless access point.

With easy-to-install Super Speed USB 3.0 interface - a very common expansion port of computers - plug this wireless network adapter into any empty USB 3.0 port of your computer, just that simple!

Other features of this router include:

- IEEE 802.11a/b/g/n/ac compatible.
- Extreme High transfer data rate – 11ac up to 867Mbps, 11n up to 300Mbps
- Support WMM wireless QoS feature.
- Support 64/128-bit WEP, WPA, WPA2 with IEEE 802.1x functions for high level of security.
- Support the most popular operating system: Windows XP/Vista/7/8, Linux, MAC OS
- Support WPS (Wi-Fi Protected Setup) hardware button for easy connection.
- Support USB 3.0/2.0 interface. (11ac mode use USB 3.0 is required)
- Portable dongle type design.

1-2 Safety Information

In order to keep the safety of users and your properties, use   the following safety instructions:

1. This USB wireless network adapter is designed for indoor use only. DO NOT expose this network adapter to direct sun light, rain, or snow.

2. DO NOT put this network adapter at or near hot or humid places, like kitchen or bathroom. Also, do not left this wireless network adapter in the car in summer.

3. This network adapter is small enough to put in a child's mouth, and it could cause serious injury or could be fatal. If they throw the network adapter, the adapter will be damaged. PLEASE KEEP THIS NETWORK ADAPTER OUT THE REACH OF CHILDREN!

4. This network adapter will become hot when being used for long time (***This is normal and is not a malfunction***). DO NOT put the network adapter on a paper, cloth, or other flammable objects after the network adapter has been used for a long time.

5. There's no user-serviceable part inside the network adapter. If you found that the network adapter is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the network adapter by yourself, warranty will be void.

6. If the network adapter falls into water, DO NOT USE IT AGAIN BEFORE YOU SEND THE ADAPTER TO THE DEALER OF PURCHASE FOR INSPECTION.

7. If you smell something strange or even see some smoke coming out from the network adapter, switch the computer off immediately, and call dealer of purchase for help.

1-3 System Requirements

- An empty USB 3.0/2.0 port (11ac mode use Super Speed USB 3.0 is required) (May not be able work with USB 1.1 port, and performance will be greatly reduced)
- Windows XP, Vista, Windows 7, Windows 8 operating system
- CD-ROM drive
- At least 100MB of available disk space

1-4 Package Contents

Before you starting to use this wireless network adapter, please check if there is any of the items missing in the package, and contact your dealer of purchase to claim for missing items:

- USB Wireless Network Adapter (1 pcs) ……...………………… 1
- Quick Installation Guide (1 pcs)………………..……………….. 2
- Driver/Utility/Quick Guide/User Manual CD-ROM (1 pcs) …… 3
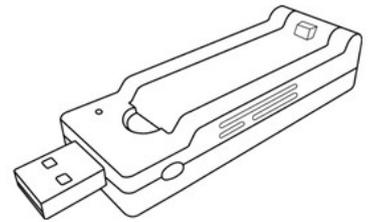
3　　　　　　　**2**　　　　　　　**1**

1-5 Familiar with your new wireless network adapter

1. USB Connector
2. External Wireless Antenna
3. Power/Activity/WPS LED
4. WPS Button (Press 2 seconds to activate WPS pairing mode)
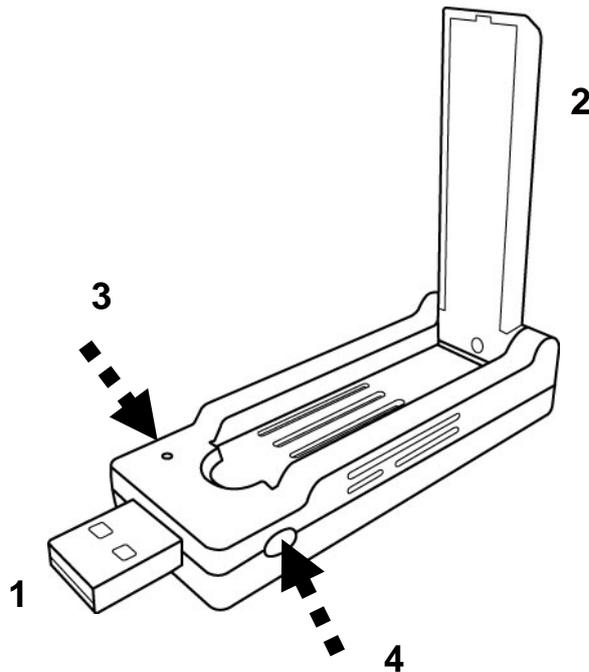
LED Name	Light Status	Description
Power/ Activity/ WPS	Off	1.No wireless network adapter is installed 2.Radio off mode.
	On	1.Wireless network adapter is normally installed 2.Radio on mode.
	Blinking	1.Transferring or receiving data. 2.Slow Blinking one time per seconds means WPS is activated. The network adapter will wait for 2 minutes to establish WPS connection. 3. Fast Blinking 30 seconds, then Solid light 15 seconds, means WPS connection is established successfully.

CHAPTER II: Driver Installation and Configuration

2-1 Network Adapter Installation

Follow the following instructions to install your new wireless network adapter:

1. Insert the USB wireless network adapter into an empty **Super Speed USB 3.0** port of your computer when computer is switched on. Never use force to insert the adapter, if you feel it's stuck, flip the adapter over and try again.

Super Speed USB 3.0
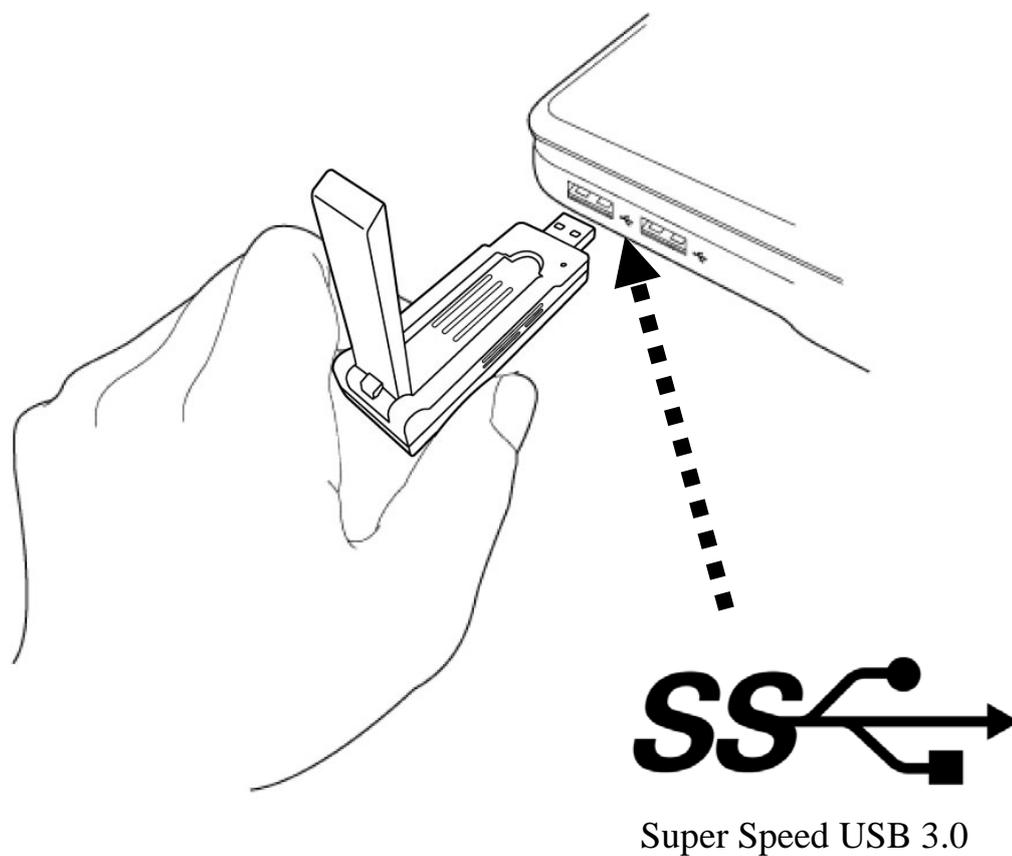
2. Insert device driver CDROM into the CD/DVD ROM drive of your computer, and execute 'Setup.exe' program in 'Driver' folder.
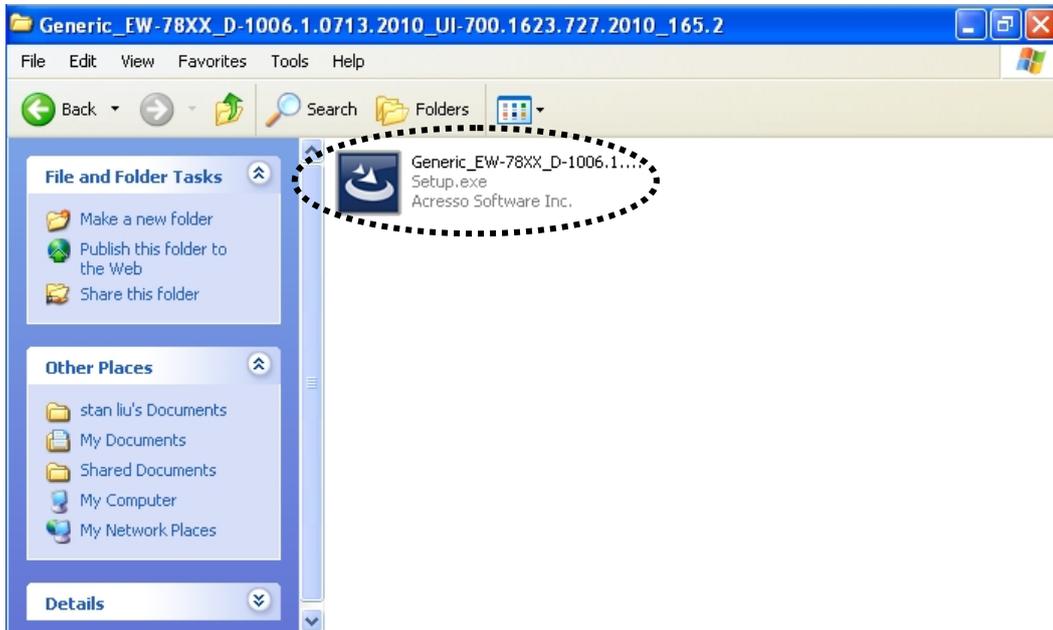
For Windows Vista / Windows 7 OS, you'll be prompted to confirm installation. Click 'Yes' to continue.
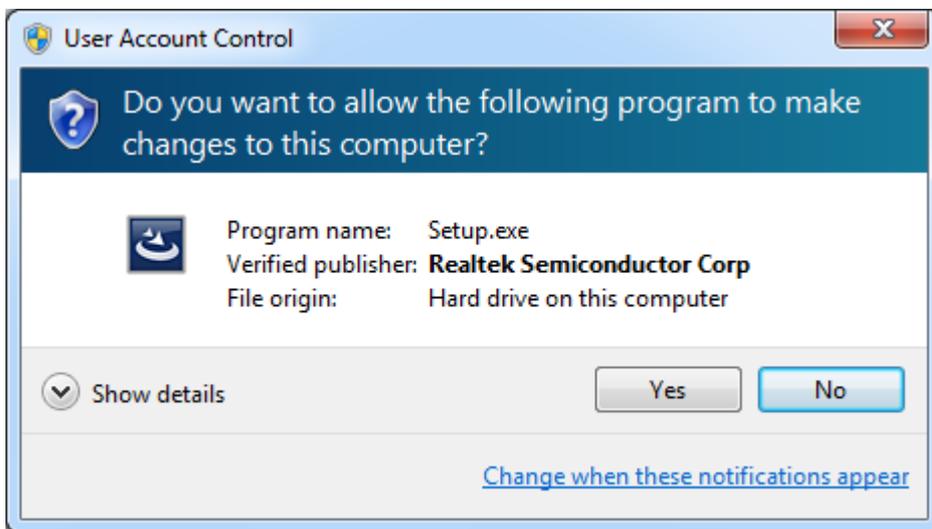
3. Click 'Next' to continue.

Click 'Next' to start installation. Installation procedure needs few minutes to complete, please be patient.

4. Click 'Finish' to restart your computer to complete installation procedure. If you don't want to restart computer now, select 'No, I will restart my computer later' option and click 'Finish'. Please note you have to restart your computer before you can use your new USB wireless network adapter.
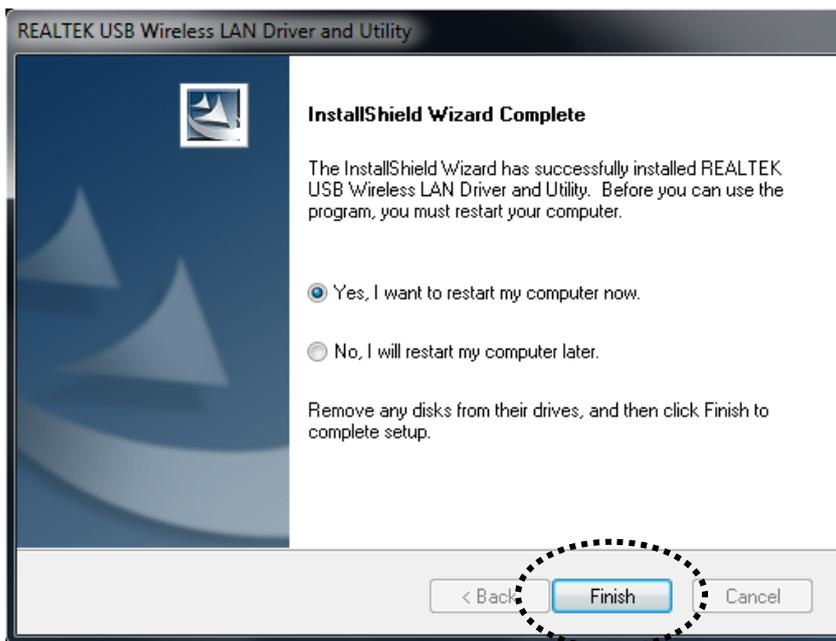
5. A new icon will appear near the clock of system tray:

HERE!
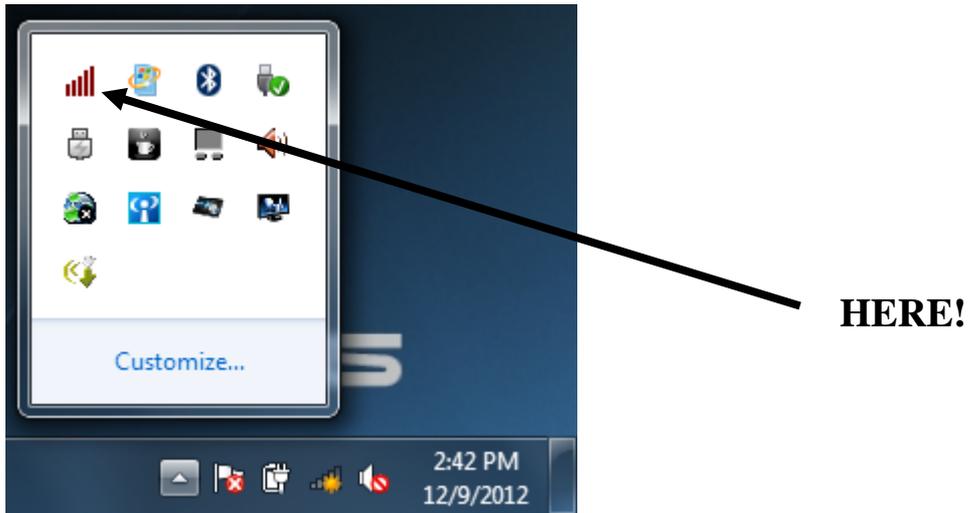
Left-click the icon will launch wireless network configuration utility, and you can right-click the icon to show the quick menu of configuration utility. This icon also uses different color to show the status of wireless connection:

Wireless network adapter not detected

No connection with access point is established (black).

Connection with access point has been established (green)

For detailed instructions of wireless network configuration utility, please see next chapter.

2-2 Connect to Wireless Access Point

To use wireless network, you have to connect to a wireless access point first. You can either use Realtek utility (comes with network adapter driver), or Windows Zero Config utility (comes with Windows operating system).

2-2-1 Using Realtek Utility

Please follow the following instructions to use Realtek configuration utility to connect to wireless access point.

1. Left-click the Realtek configuration utility icon located at lower-right corner of computer desktop, and configuration menu will appear:
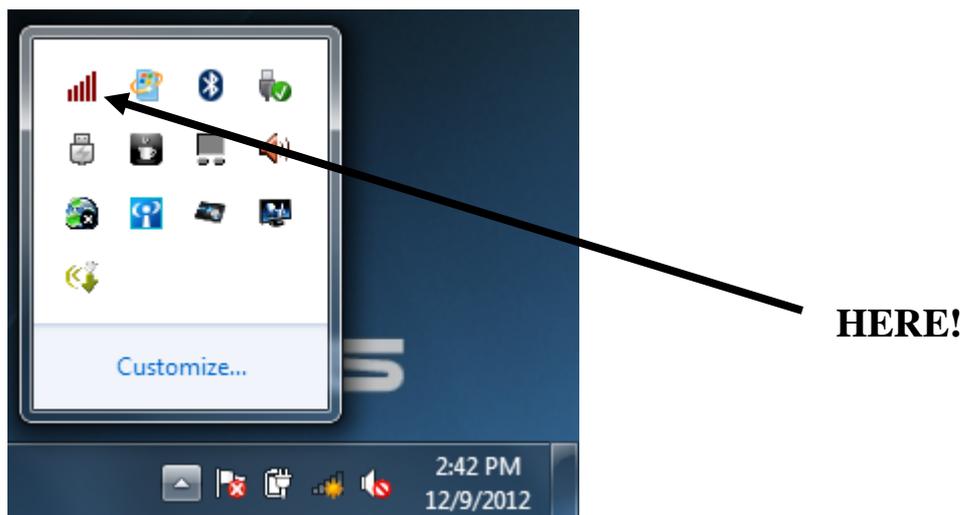
HERE!

2. Wireless utility will appear. Click 'Available Network' menu to search for wireless access points nearby.
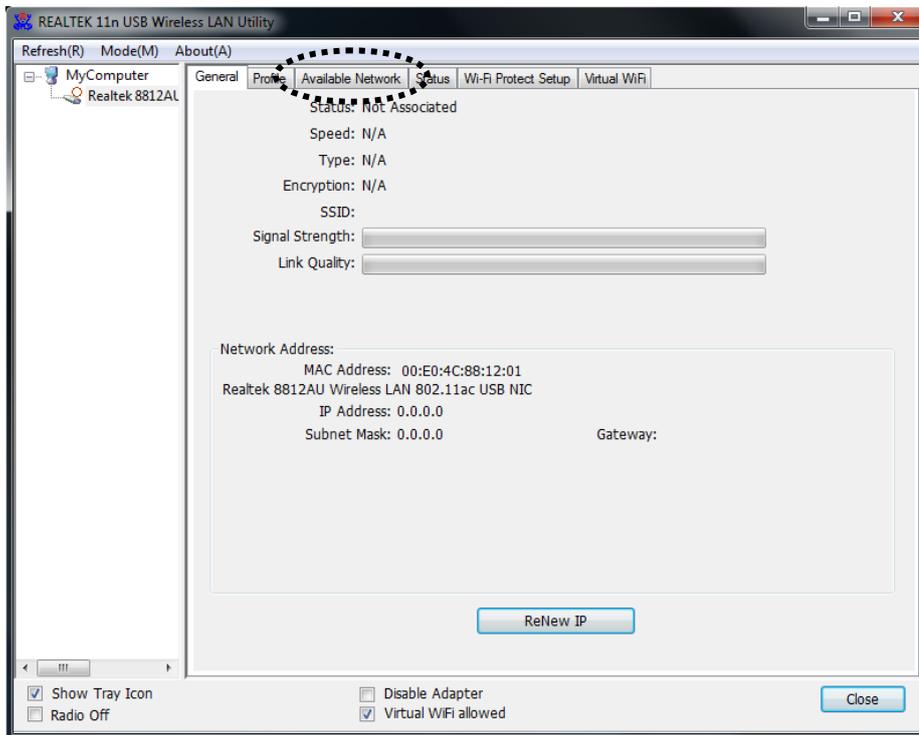
3. Please wait for a while, and all wireless access points which can be reached by this wireless network adapter will be displayed here.
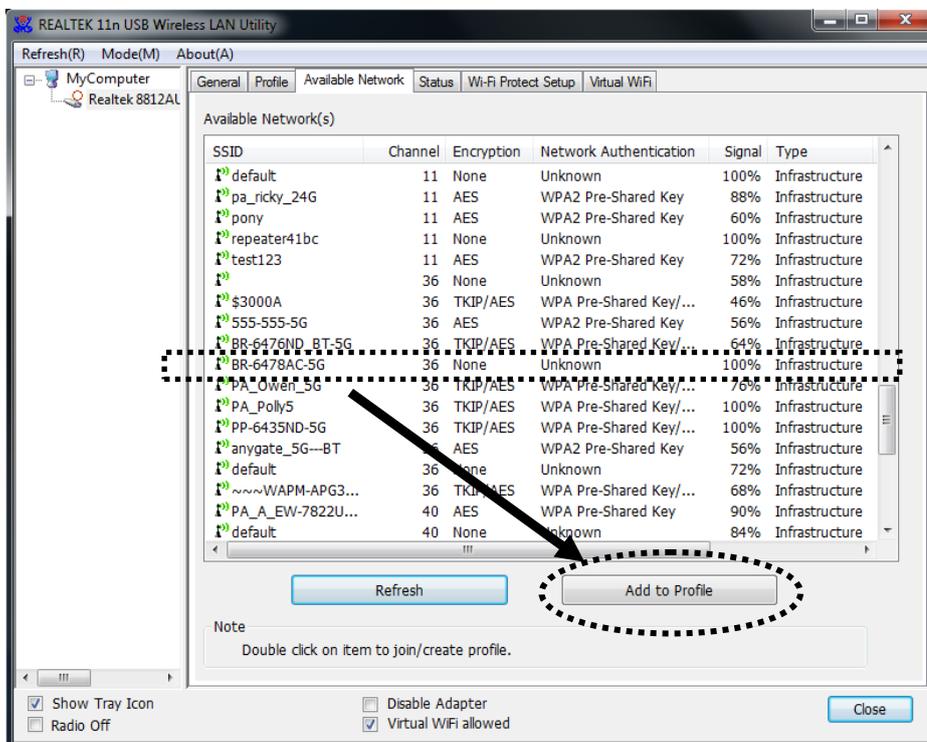
If the wireless access point you wish to connect does not appear here, you can click 'Refresh' button to scan for wireless access points again; if the wireless access point you're looking for still not appear, try to move the computer closer.

When the access point you're looking for is on the list, left-click it and then double click it or click 'Add to Profile'.

4. If a password (Network Key) is required to access the wireless access point, please input it in 'Network key' (and input it again in 'Confirm network key' for confirmation). Click 'OK' when password is properly inputted.

NOTE: Network security type ('Network Authentication' and 'Data encryption') will be selected automatically based on wireless access point's security setting. It's not required to change these settings by yourself.
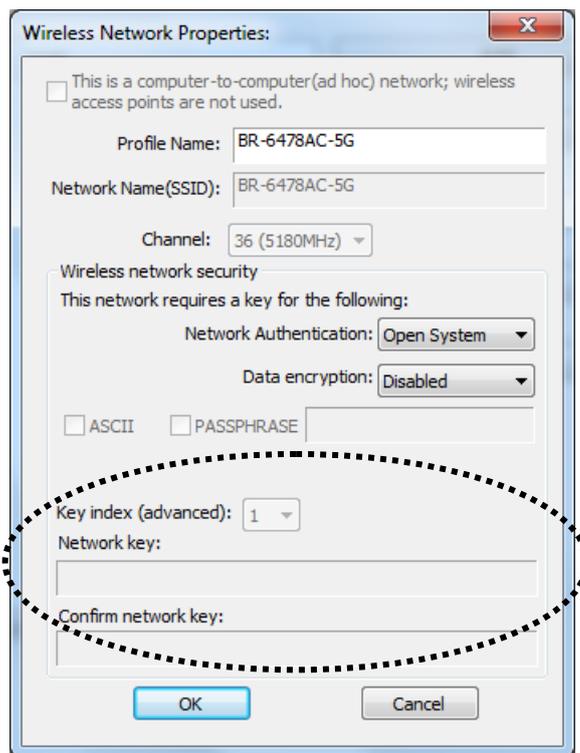
All options in this page will be filled automatically according to the access point you wish to add to profile. However, you can still modify any of them to meet your requirement.

Profile name	You can give a name to this profile, so you can remember its purpose easily. It can be any phrase to help you remember.
Network Name (SSID)	The SSID (Service Set ID entities, i.e. access point's name). This field will be filled as the access point you selected when SSID is not hidden and grayed out. If SSID is hidden, you have to input correct SSID you yourself.
This is a computer-to-computer (ad hoc) network	Check this box if you wish to connect to another computer / network device by ad hoc method. When not accessing to wireless access point, you have to check this box.
Channel	Select wireless channel for ad hoc connection. This option only appears when you're using ad hoc connection.
Network Authentication	Select the network authentication type from drop-down menu. This setting must be identical with the setting of wireless access point you with to connect.
Data encryption	Select the data encryption type from drop-down menu. This setting must be identical with the setting of wireless access point you with to connect.
ASCII / PASSPHRASE	When the encryption type is 'WEP', it's required to input a set of 'passphrase' to connect to wireless access point. Check 'ASCII' or 'PASSPHRASE' depends on the security setting of access point, and input it in the box; if you select 'PASSPHRASE' you also need to select the length of the key.

The passphrase must be identical with the setting of wireless access point you with to connect. |
| Key index (advanced) | Select WEP key index. For most of access points you can select '1', but please refer to the setting of the access point. |

13

Network key / Confirm network key	When the encryption type is 'WPA' or 'WPA2-PSK', it's required to input a set of 'passphrase' to connect to wireless access point. Please input the same passphrase in two boxes for confirmation.
EAP TYPE / Tunnel / Provision Mode	When authentication type is any of 802.1X, you have to select EAP type, tunnel, and provision mode from dropdown menu. This setting must be identical with your 802.1x authentication server.
Username / Identity / Domain / Password	Please input 802.1x related authentication information here.
Certificate	If certification is required to authenticate with 802.1x authentication server, please select a local certificate from dropdown list.
PAC	Check this box and PAC (Privilege Access Certificate) will be automatically selected.

Please click 'OK' when ready.

5. Network adapter will attempt to connect to access point now, this may require few seconds to minutes, please be patient. When the 'Status' become 'Associated', your computer is connected to access point you selected. Click 'Close' to close configuration menu.
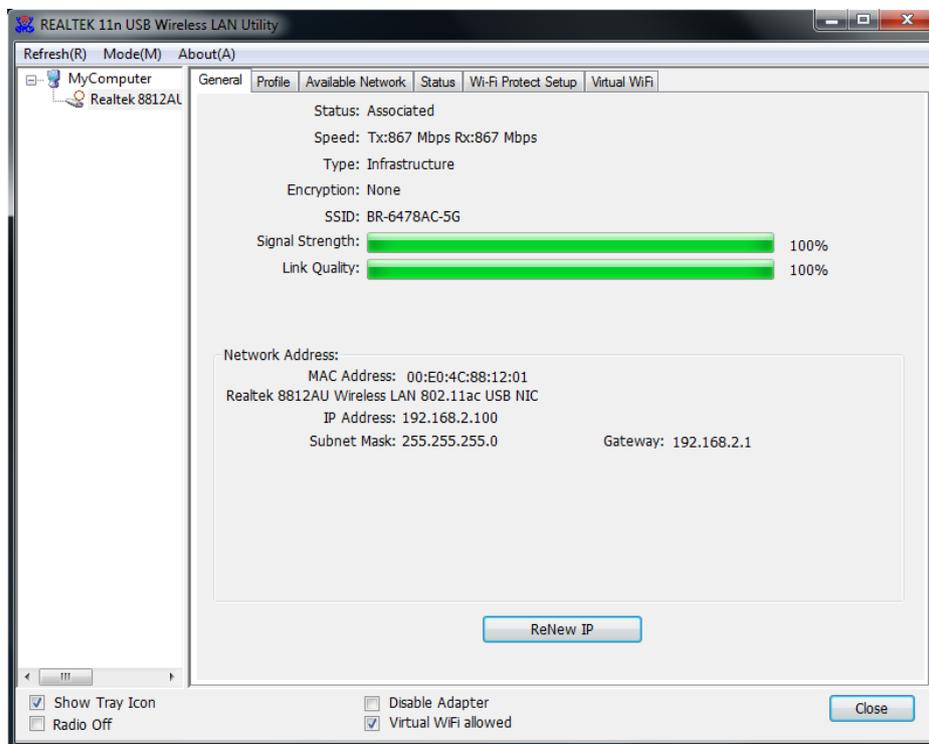
NOTE: If you connected to an access point but the connection has been dropped soon, please check security settings and re-check password spelling.

NOTE: If you insert the USB wireless network adapter into an USB 3.0 port and connect to an 11ac AP, device driver will doing auto USB mode switch and shown the message as below photo, or you will heard sounds of USB insert or unplug, this is the normal states.

2-2-2 Using Windows Zero Configuration

Windows XP and Vista has a built-in wireless network configuration utility, called as 'Windows Zero Configuration' (WZC). You can also use WZC to configure your wireless network parameter:

1. Right-click Realtek configuration utility icon, and click 'Open Config Utility'.
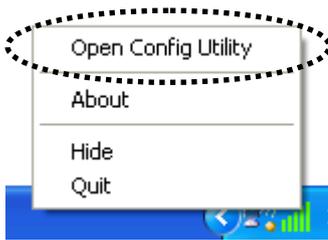

2. Check 'Windows Zero Config' box.
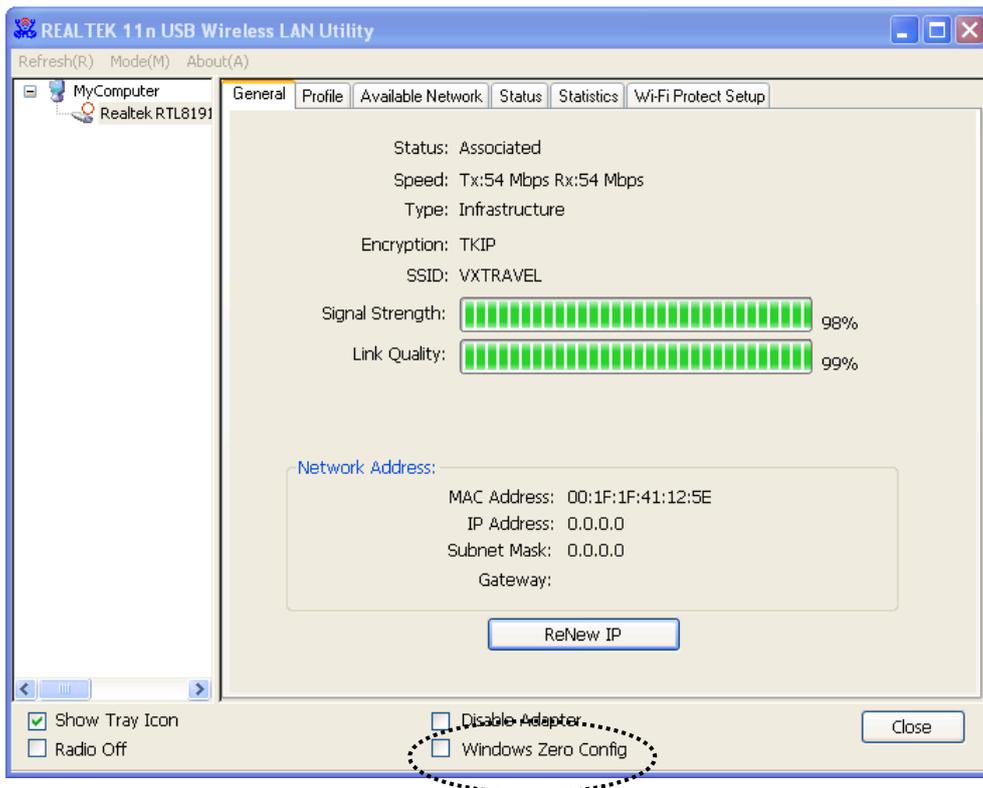
3. A message indicating that you've been switched to Windows Zero Configuration mode will appear. Click 'OK' to continue.

NOTE: To return to use Realtek utility, uncheck 'Windows Zero Config' box.

4. Click the 'Start' button (should be located at the bottom-left corner of windows desktop), click 'Control Panel', then click 'Network and Internet Connections' in Control Panel.
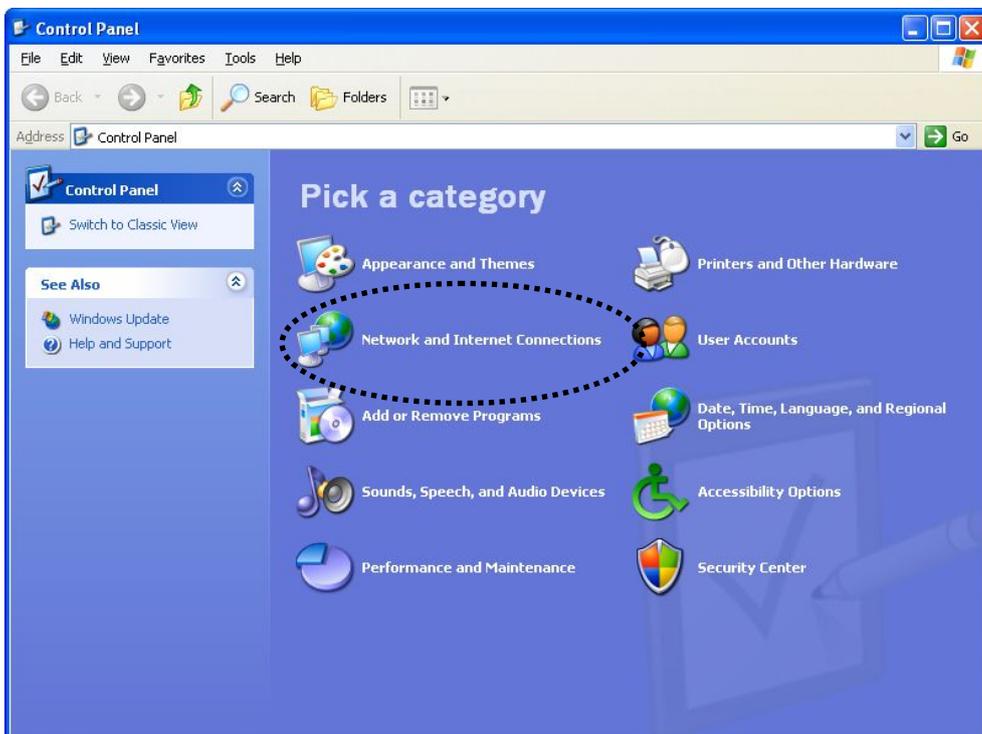
5. Double click 'Network Connections'.
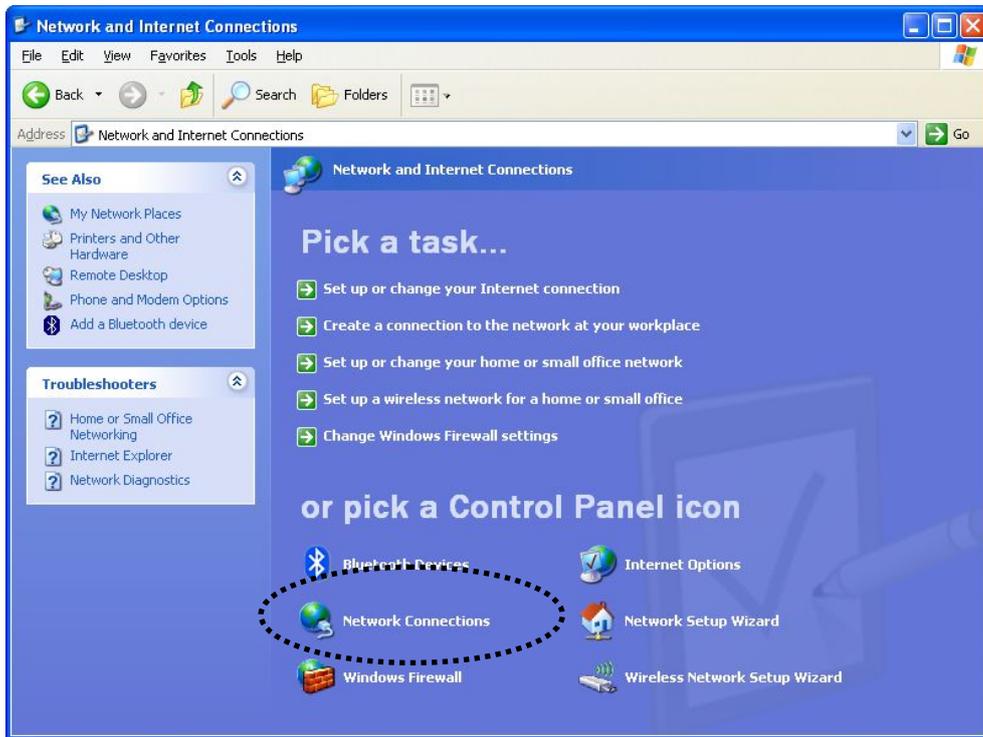
6. Right-click 'Wireless Network Connection' (it may have a number as suffix if you have more than one wireless network adapter, please make sure you right-click the 'Realtek 8812AU Wireless LAN 802.11ac USB NIC), then select 'View Available Wireless Networks'.
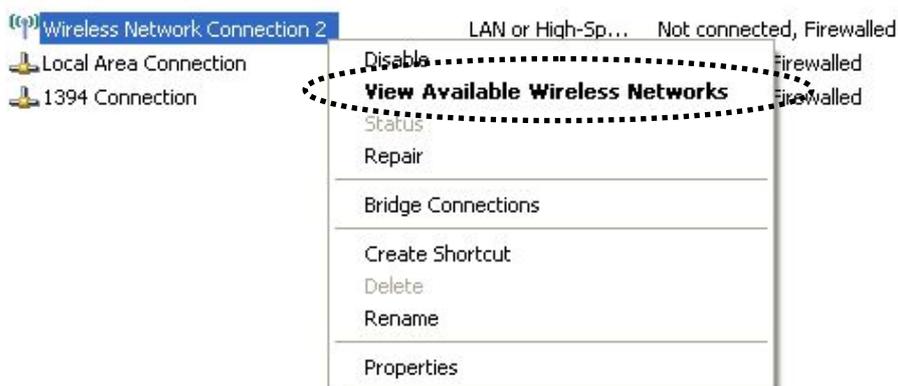
7. All wireless access points in proximity will be displayed here. If the access point you want to use is not displayed here, please try to move your computer or notebook closer to the access point, or you can click 'Refresh network list' to rescan access points. Click the access point you want to use if it's shown, then click 'Connect'.
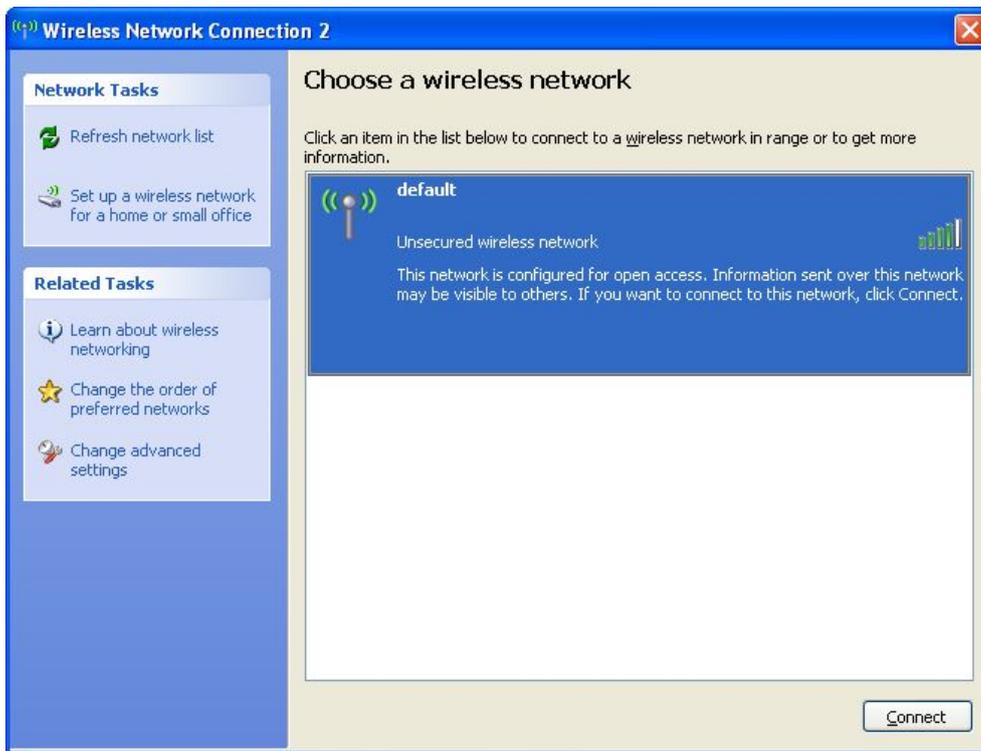

8. If the access point is protected by encryption, you have to input its security key or passphrase here. It must match the encryption setting on the access point.

   If the access point you selected does not use encryption, you'll not be prompted for security key or passphrase.

9. If you can see 'Connected' message, the connection between your computer and wireless access point is successfully established.
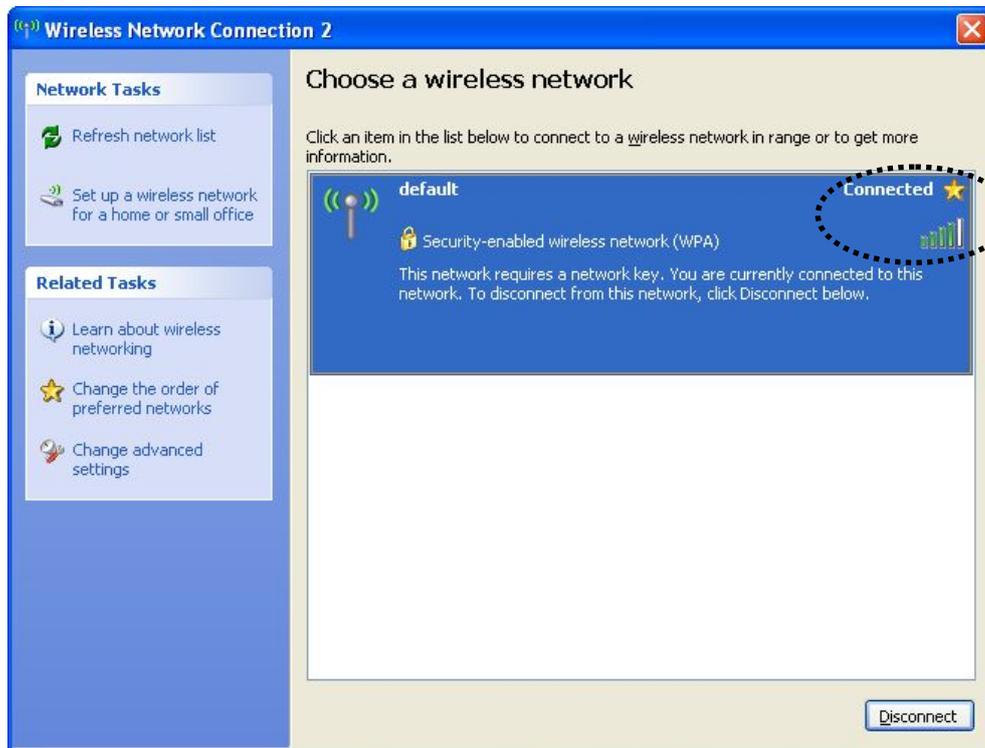
2-3 Connection Profile Management

If you need to connect to different wireless access points at different time, like of access point of your home, office, cybercafe, or public wireless service, you can store the connection parameters (encryption, passphrase, security, and so on.) as a profile for every access point, so you don't have to input these parameters every time when you want to connect to a specific wireless access point.

To manage profiles, right-click the Realtek configuration utility icon located at lower-right corner of computer desktop, then click 'Open Config Utility'.

Click the 'Profile' menu.
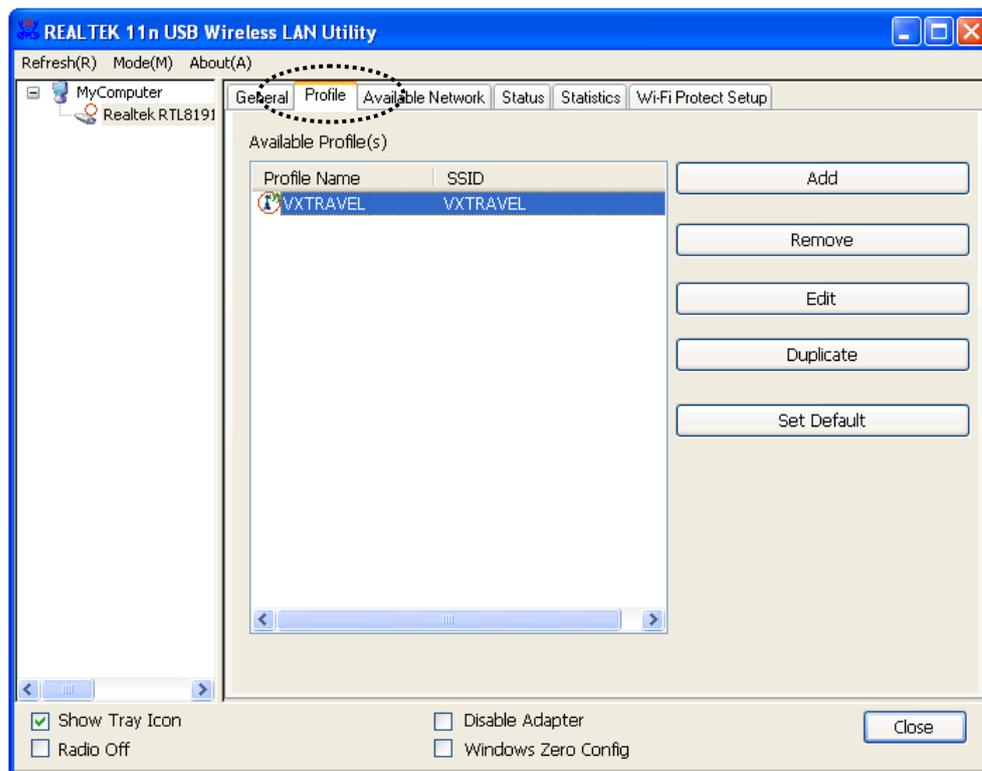
2-3-1 Add a New Profile

By this function you can setup the connection parameters for a specific wireless access point in advance, without contacting it first.

If you want to create a new profile, click 'Profile' menu, then click 'Add' button.
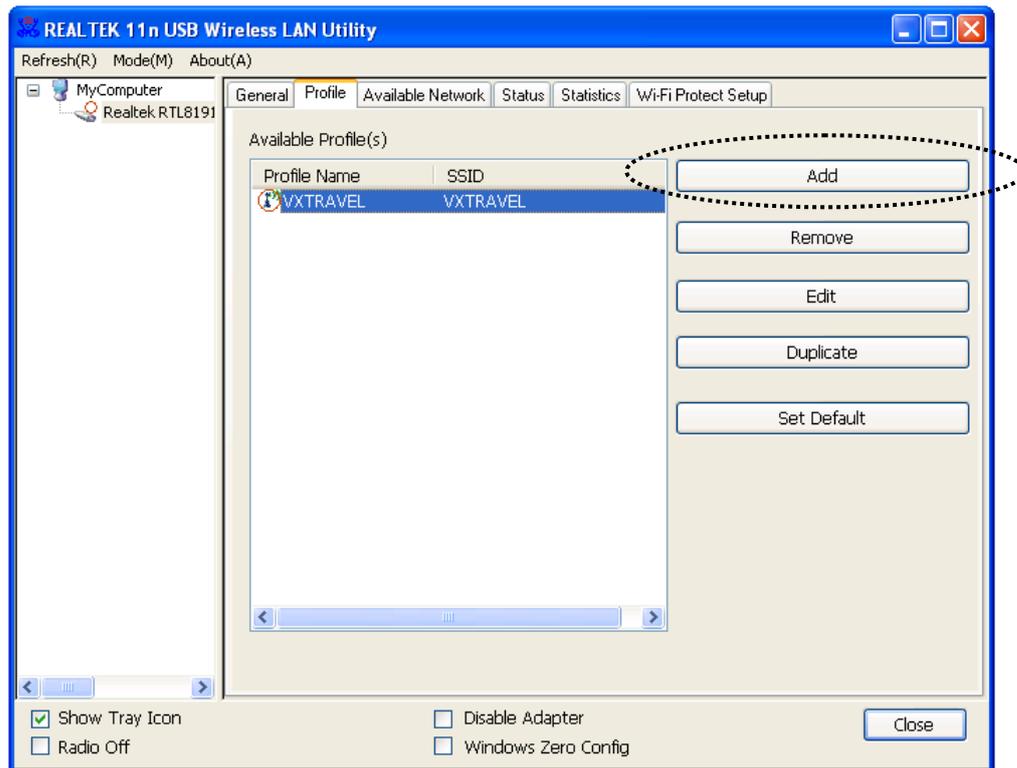
You'll be prompted to input connection parameters for the wireless access point you wish to connect:
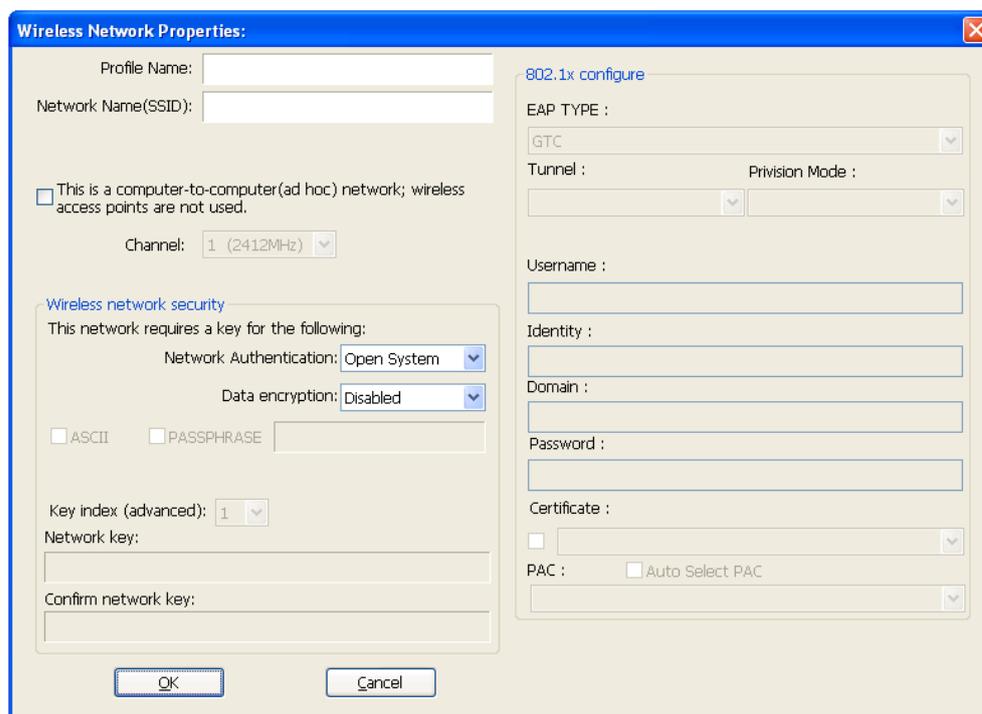
Required parameters are:

Profile name	You can give a name to this profile, so you can remember its purpose easily. It can be any phrase to help you remember.
Network Name (SSID)	The SSID (Service Set Identifier, i.e. access point's name). This must be identical with the SSID of the access point you wish to connect.
This is a computer-to-computer (ad hoc) network	Check this box if you wish to connect to another computer / network device by ad hoc method. When not accessing to wireless access point, you have to check this box.
Channel	Select wireless channel for ad hoc connection. This option only appears when you're using ad hoc connection.
Network Authentication	Select the network authentication type from drop-down menu. This setting must be identical with the setting of wireless access point you with to connect.

Data encryption	Select the data encryption type from drop-down menu. This setting must be identical with the setting of wireless access point you with to connect.
ASCII / PASSPHRASE	When the encryption type is 'WEP', it's required to input a set of 'passphrase' to connect to wireless access point. Check 'ASCII' or 'PASSPHRASE' depends on the security setting of access point, and input it in the box; if you select 'PASSPHRASE' you also need to select the length of the key. The passphrase must be identical with the setting of wireless access point you with to connect.
Key index	Select WEP key index. For most of access points you can select '1', but please refer to the setting of the access point.
Network key / Confirm network key	When the encryption type is 'WPA' or 'WPA2-PSK', it's required to input a set of 'passphrase' to connect to wireless access point. Please input the same passphrase in two boxes for confirmation.
EAP TYPE / Tunnel / Provision Mode	When authentication type is any of 802.1X, you have to select EAP type, tunnel, and provision mode from dropdown menu. This setting must be identical with your 802.1x authentication server.
Username / Identity / Domain / Password	Please input 802.1x related authentication information here.
Certificate	If certification is required to authenticate with 802.1x authentication server, please select a local certificate from dropdown list.
PAC	Check this box and PAC (Privilege Access Certificate) will be automatically selected.

When all required parameters are set, click 'OK' to create and save a new profile.

2-3-2 Remove an Existing Profile

When you no longer need an existing profile, you can remove it.

If you want to remove a profile, click 'Profile' menu, then select an existing profile which you wish to remove, and then click 'Remove' button.
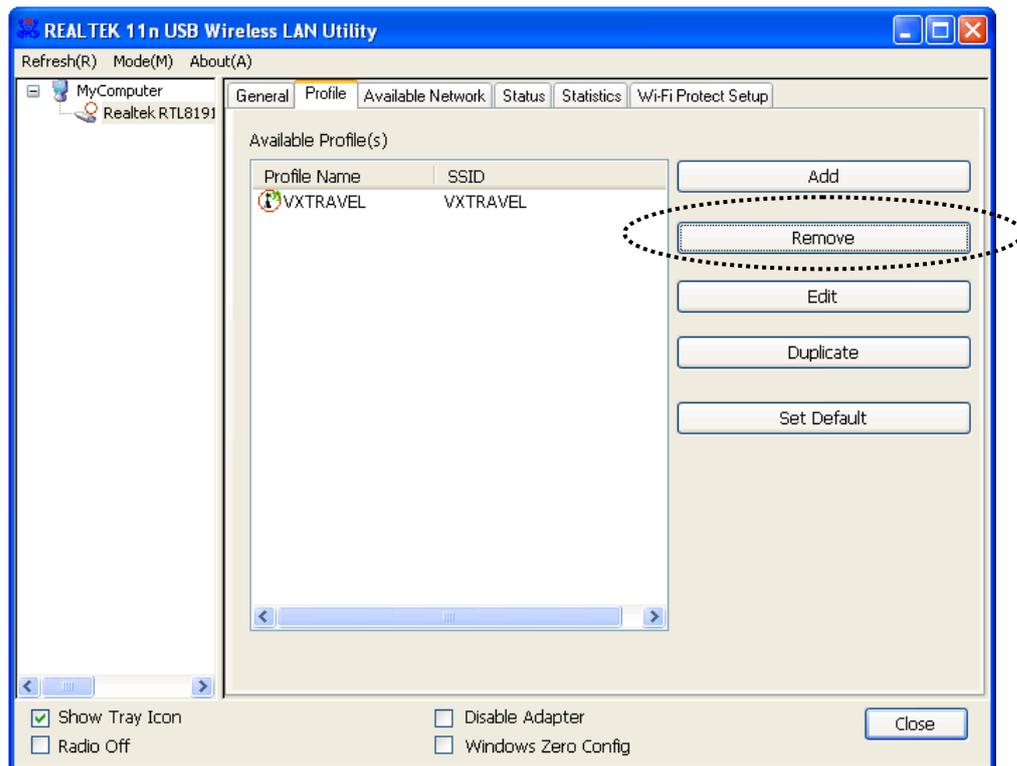
2-3-3 Edit an Existing Profile

If you have added a profile before, and you wish to change the content of the profile, you can use this function. Please select a profile from the list first, then click 'Edit' button. You'll be provided with the contents of selected profile, and you can edit them. Click 'OK' to save changes, or click 'Cancel' to disadapter changes.

2-3-4 Make a Copy of an Existing Profile

If you need to make a copy of a specific profile, you can use this function.
This function is very convenient when you need to build a new profile
which parameters are similar to any existing profile.

To do this, select an existing profile, then click 'Duplicate' button.
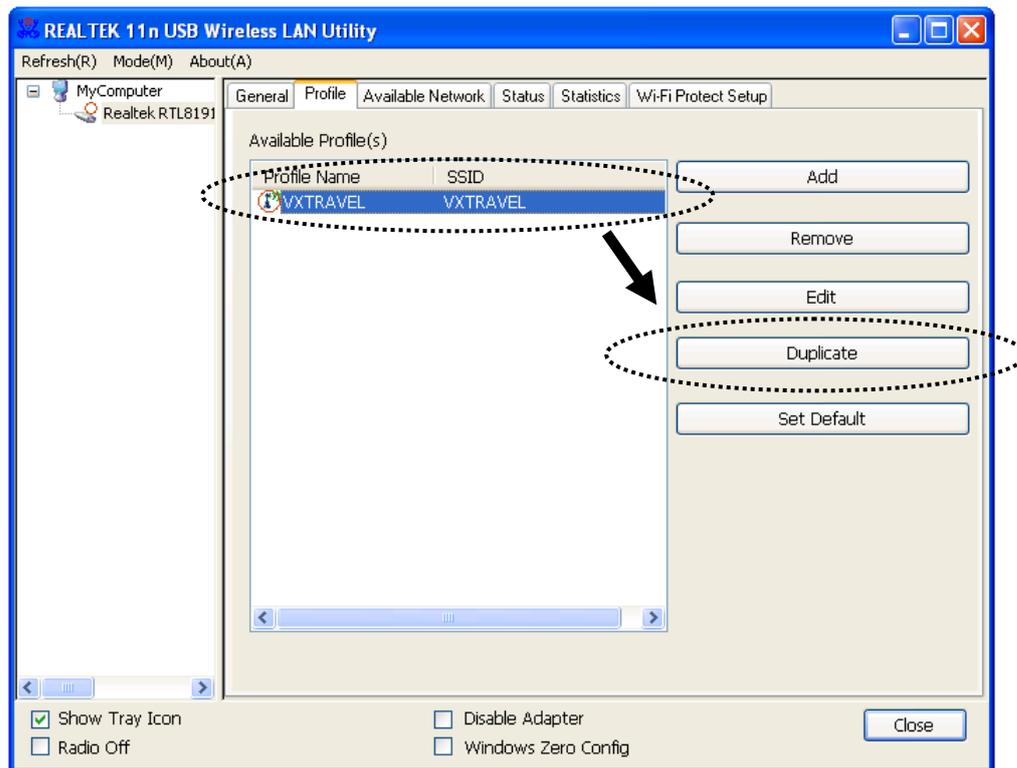
You'll be prompted to input a profile name, please use an identical name
that does not exist in profile list.

2-3-5 Set as a Default Profile

If you wish to use a specific profile as default connection, you can select a profile in the list, and click 'Set Default'. Selected profile will become default selection and Realtek configuration utility will attempt to connect to selected access point.
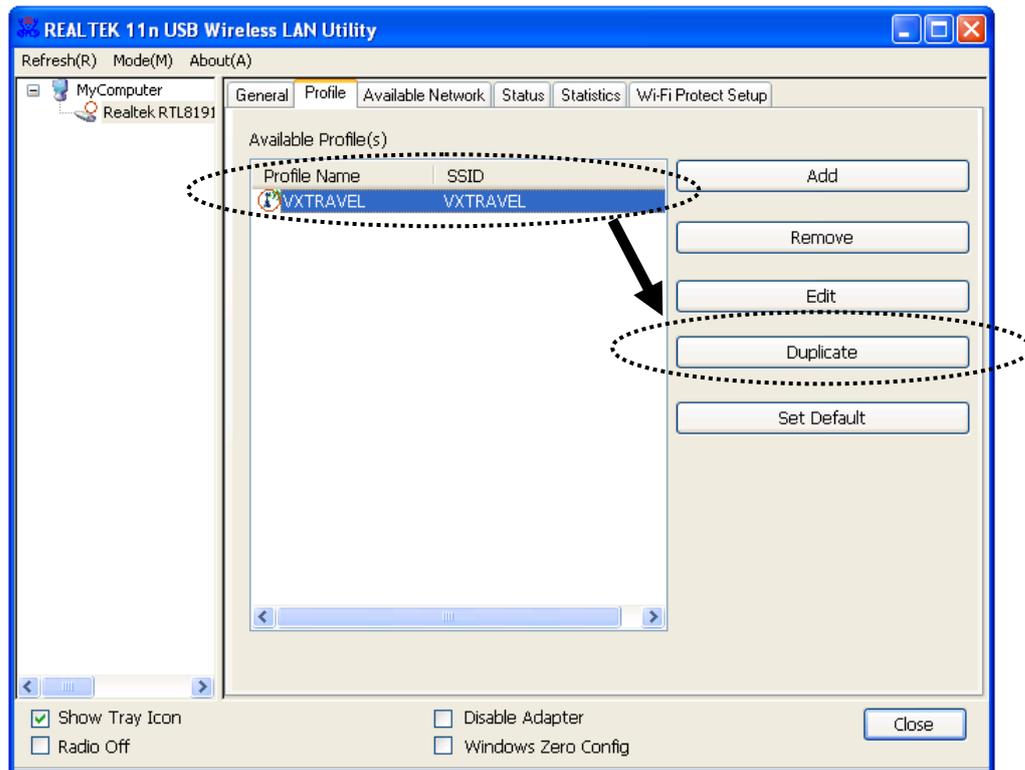
2-4 View Network Statistics, General Information, and Status

The configuration utility provides information about network statistics and link status. If you want to know how your wireless network adapter works, you can use these functions to get detailed information about the wireless connection you're using.

2-4-1 General Information

If you want to know the general information of the access point you're connecting to, click 'General' menu:
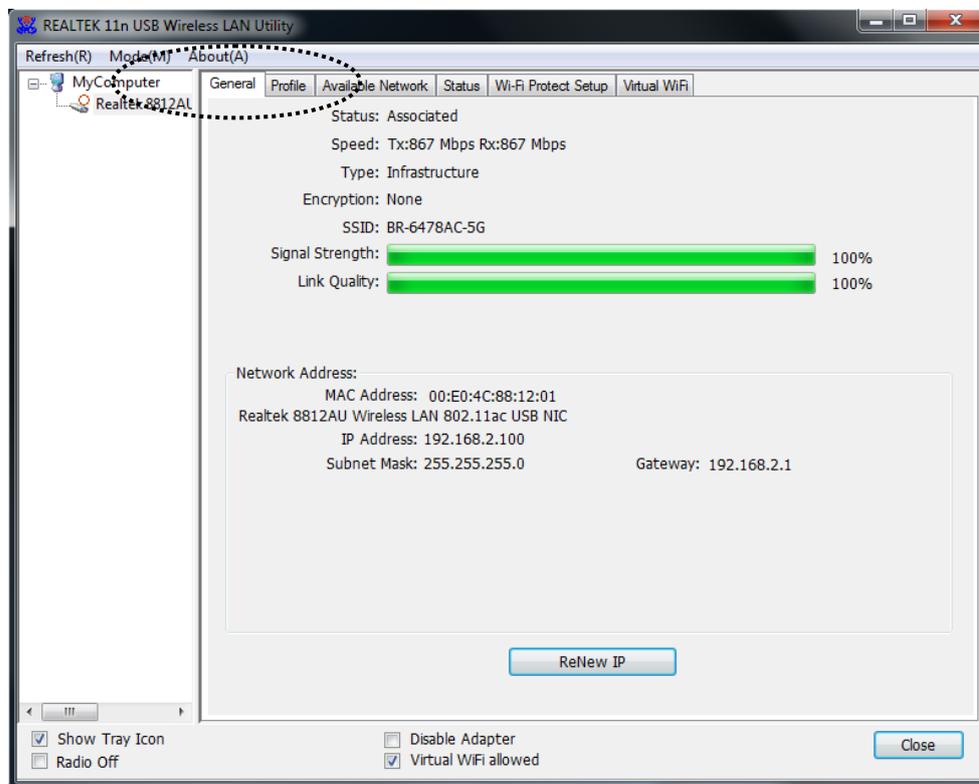

All general information like signal strength and link quality will be displayed here. These information are very useful when you encounter some problem on connecting to access point.

If you wish to get a new IP address from DHCP server, you can click 'ReNew IP' button.

2-4-2 Status

If you want to know the status of your wireless network adapter, click 'Status' menu:
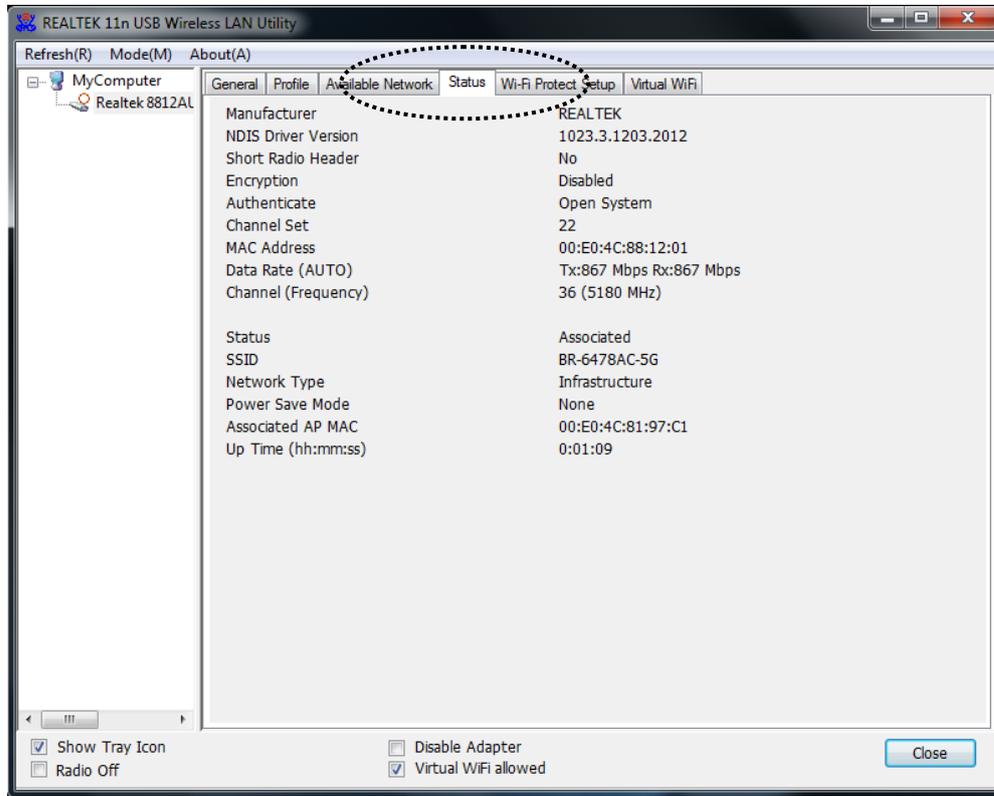
2-4-3 View Network Statistics

To view the statistical data of wireless network adapter, click 'Statistics' menu, and the statistics of wireless connection will be displayed:
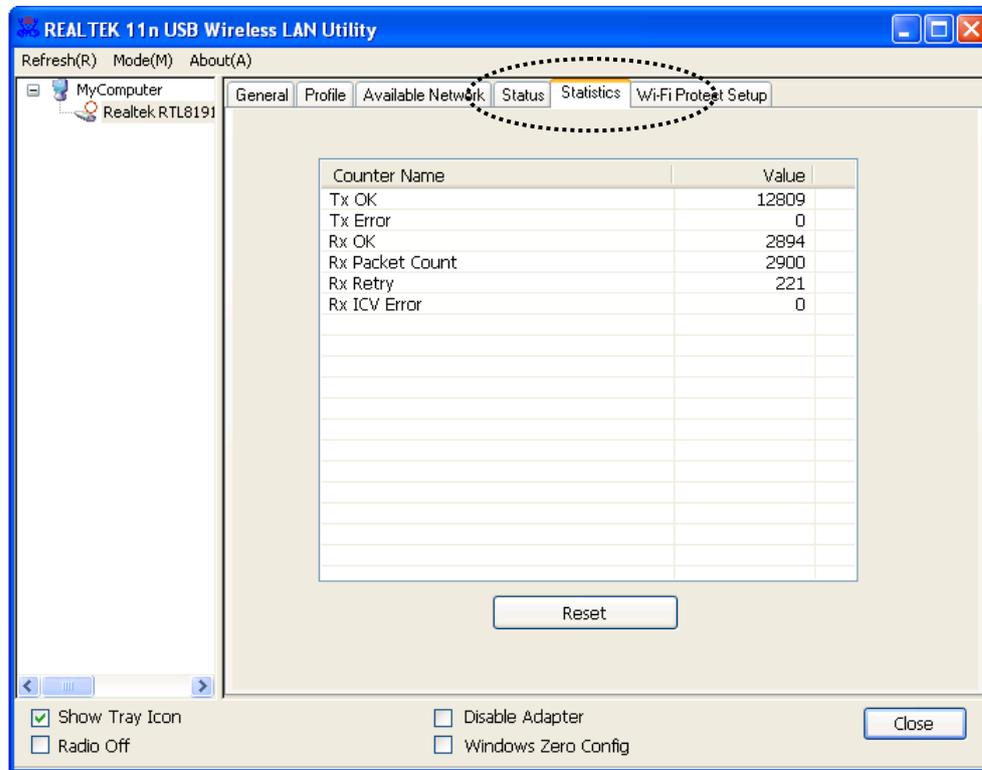
All connection-related statistics is displayed here. You can click 'Reset' button, to reset the statistics of all items back to 0.

2-5 Miscellaneous Settings

There are few functions provided by Realtek configuration utility, you can access these functions from the bottom of configuration menu:
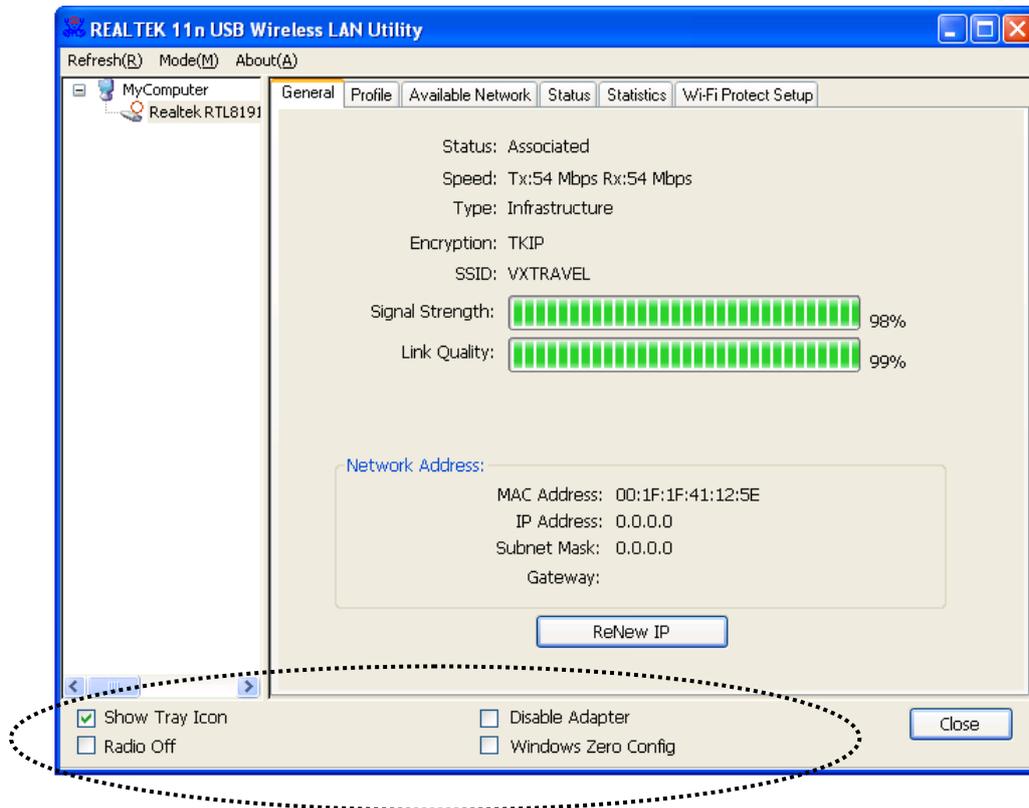
The descriptions of these function are listed as follow:

Show Tray Icon	Check this box to show an icon on system tray. **HERE!** Uncheck this box to hide it.
Radio Off	Switch wireless radio off. Wireless network functionalities are disabled.
Disable Adapter	Disable wireless network adapter. All functionalities of configration menu will

	disappear. To resume, unckeck 'Disable Adapter'.
Windows Zero Config	Use Windows Zero Configuration to manage wireless connections. See section 2-2-2.

2-6 Establish a Secure Connection with AP by WPS

Wi-Fi Protected Setup (WPS) is the latest wireless network technology which makes wireless network setup become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption by yourself. All you have to do is to go to the WPS setup page of this wireless adapter, click a button, and then press a specific button or enter a set of 8-digit code on the wireless access point you wish to establish a secure connection - just three simple steps!

For older wireless access points, it's possible to perform a firmware upgrade to become a WPS-enabled access point. Since they may not have a hardware button to press for WPS setup, you can use an alternative WPS setup method - input the pin code. Every WPS-compatible wireless network adapter support pin code configuration method; you can just input the code to wireless access point, and the wireless access point and wireless network adapter will do the rest for you.

This wireless network adapter is compatible with WPS. To use this function, the wireless access point you wish to connect to must support WPS function too. Now, please follow the following instructions to establish secure connection between WPS-enabled wireless access point and your wireless network adapter.

This wireless network adapter supports 2 kinds of WPS: PIN code and Push-Button.

Follow the following instructions to setup WPS:

1. Right-click Realtek configuration utility icon, and click 'Open Config Utility'.

2. Click 'Wi-Fi Protect Setup' menu.
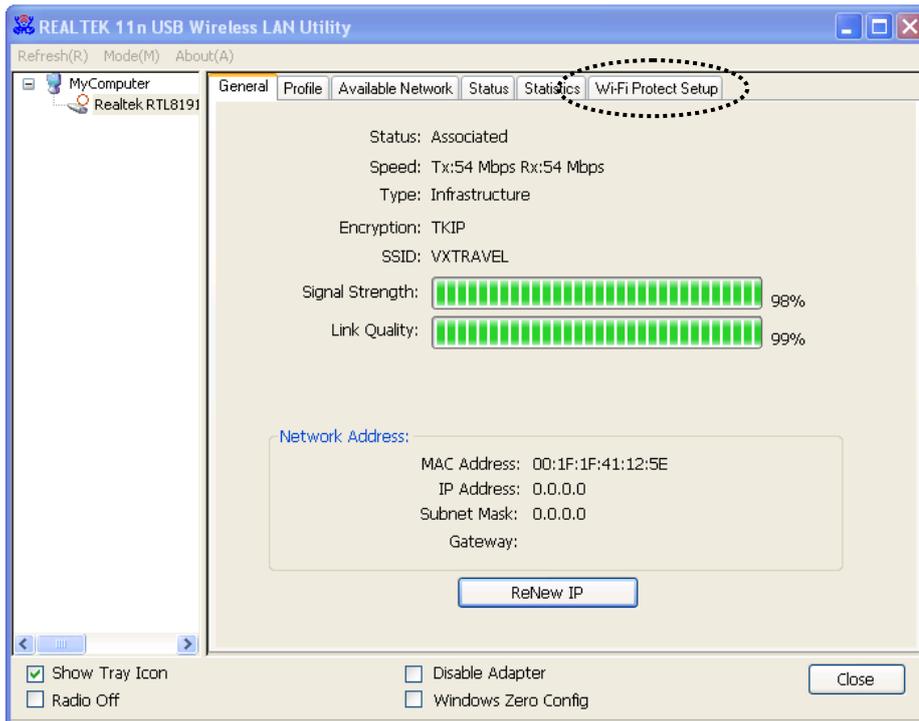
3. You can use PIN code or Push-Button configuration, and WPS-compatible wireless access point must use the same type of WPS. For instructions on setup each type of WPS, see next 2 chapters for detailed instructions.
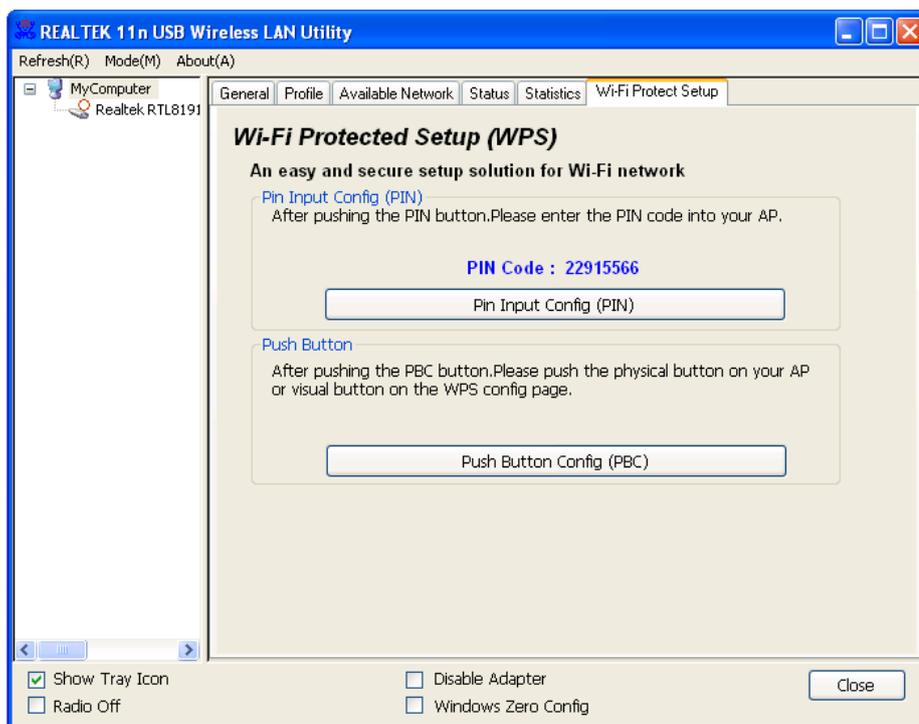
2-6-1 PIN Code

To use PIN Code, please click 'Pin Input Config (PIN)' button:
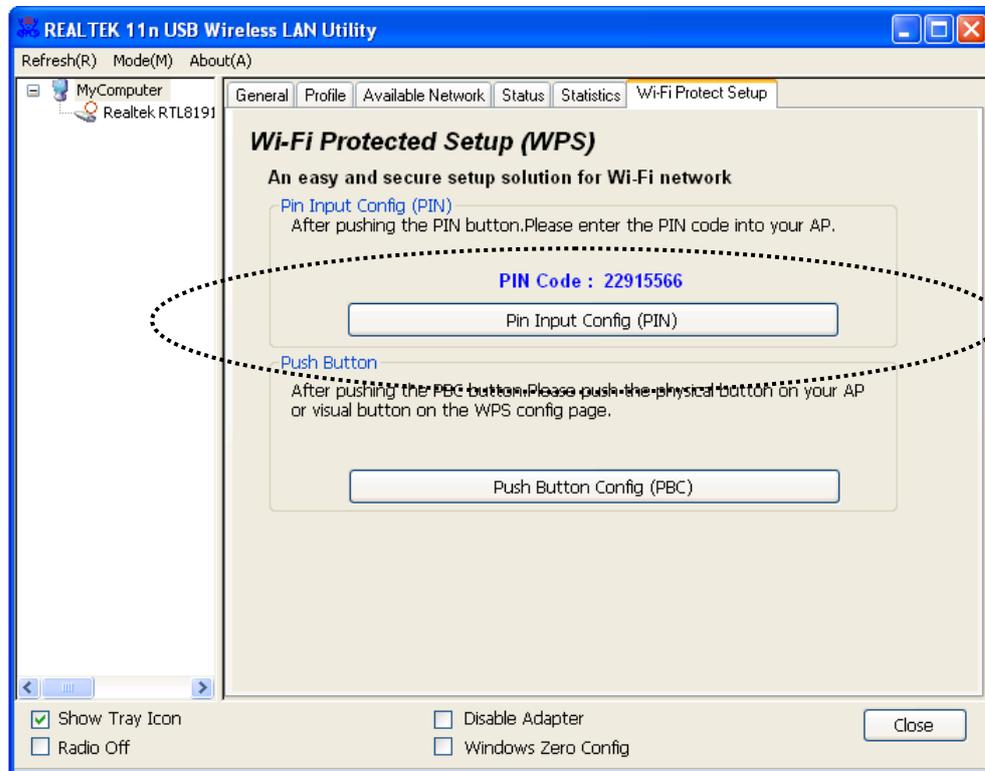
You'll be prompted to select an access point you wish to connect. If you know its SSID, click 'Yes', otherwise click 'No'.
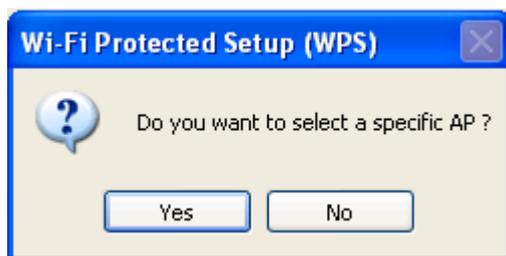
If you select 'Yes', a list of all WPS-compatible AP nearby will be displayed; you can click 'Refresh' to rescan, then select an AP and click 'Select' button.
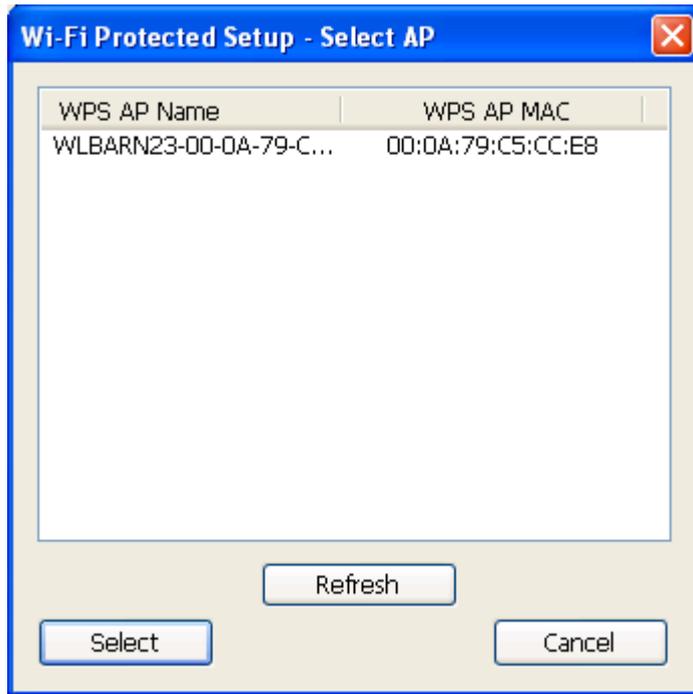
If you select 'No', wireless network adapter will prompt you to enter 8-digit PIN code into your AP, without selecting an AP in advance.

After you select 'Yes' or 'No' in previous step, network adapter will attempt to connect to WPS-compatible AP, and an 8-digit number will appear. Please input this number to AP's configuration menu within 2 minutes, and network adapter will establish secure connection with AP automatically.

To stop this procedure before connection is established, click 'Cancel'.
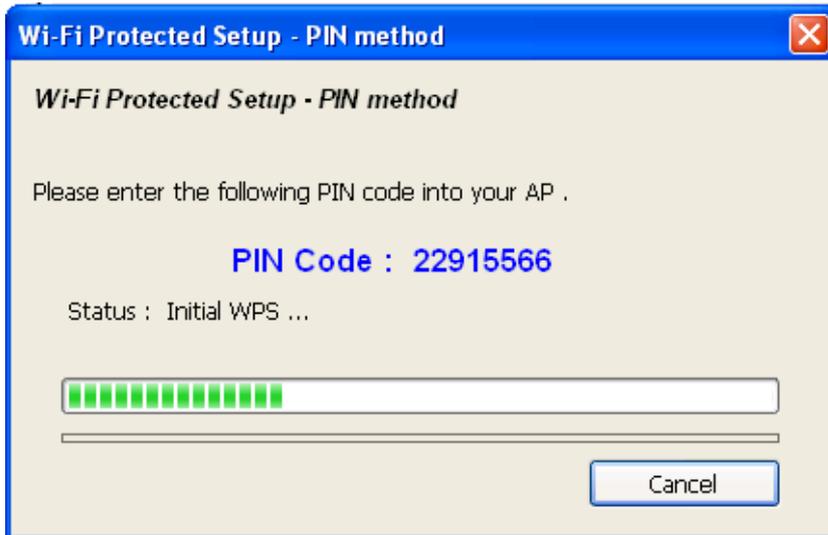
2-6-2 Push Button

To use Push-Button WPS configuration, please click 'Push Button Config (PBC)' button. This is the easiest way to establish secure connection by WPS, but if there're more than one WPS-compatible AP using Push-Button config, please use PIN Code instead.
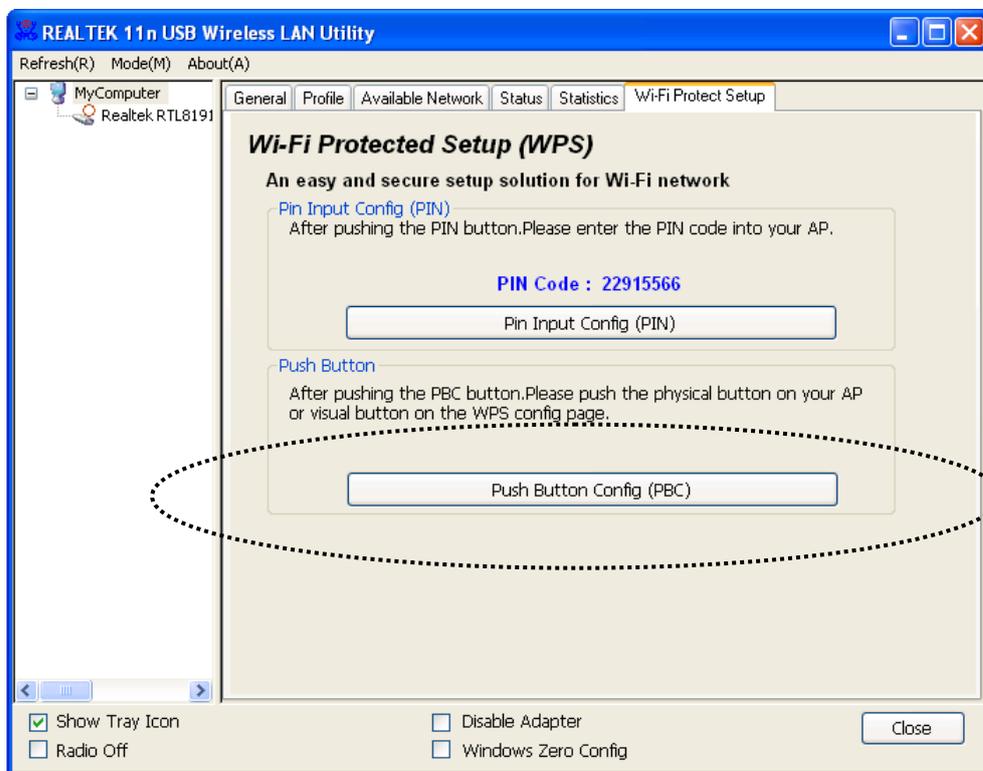
After you click Push Button Config, a message box will appear:
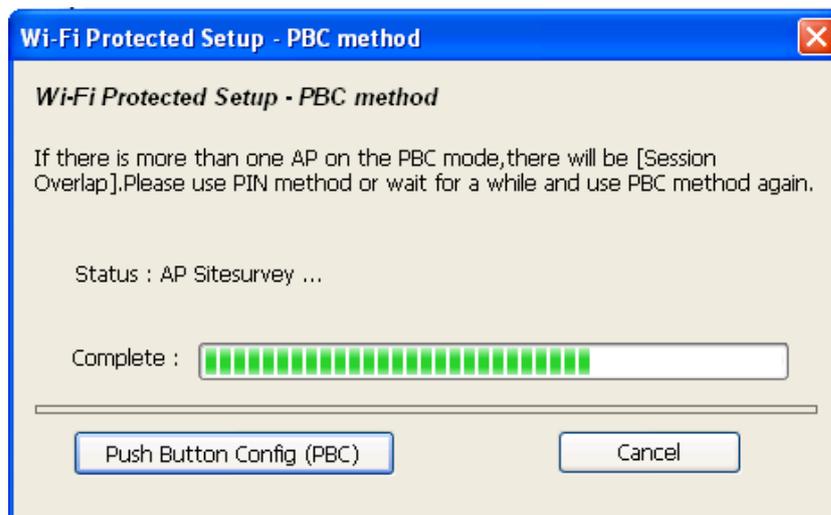
Please activate Push-Button function on wireless access point now, and wireless network adapter will establish secure connection with access point within one minute.

CHAPTER III: Soft-AP Function

Excepting become a wireless client of other wireless access points, this wireless adapter can act as a wireless service provider also! You can switch this wireless adapter's operating mode to 'AP' mode to simulate the function of a real wireless access point by software, and all other computers and wireless devices can connect to your computer wirelessly, even share the internet connection you have!

Please follow the instructions in following chapters to use the AP function of your wireless adapter.

3-1 Switch to AP Mode and Station Mode

The operating mode of the wireless adapter is 'Station Mode' (becoming a client of other wireless access points) by default.

Please follow the following instructions to switch to AP mode:

1. Right-click Realtek configuration utility icon, and click 'Open Config Utility'.

2. Select 'Mode', and then select 'Access Point'.
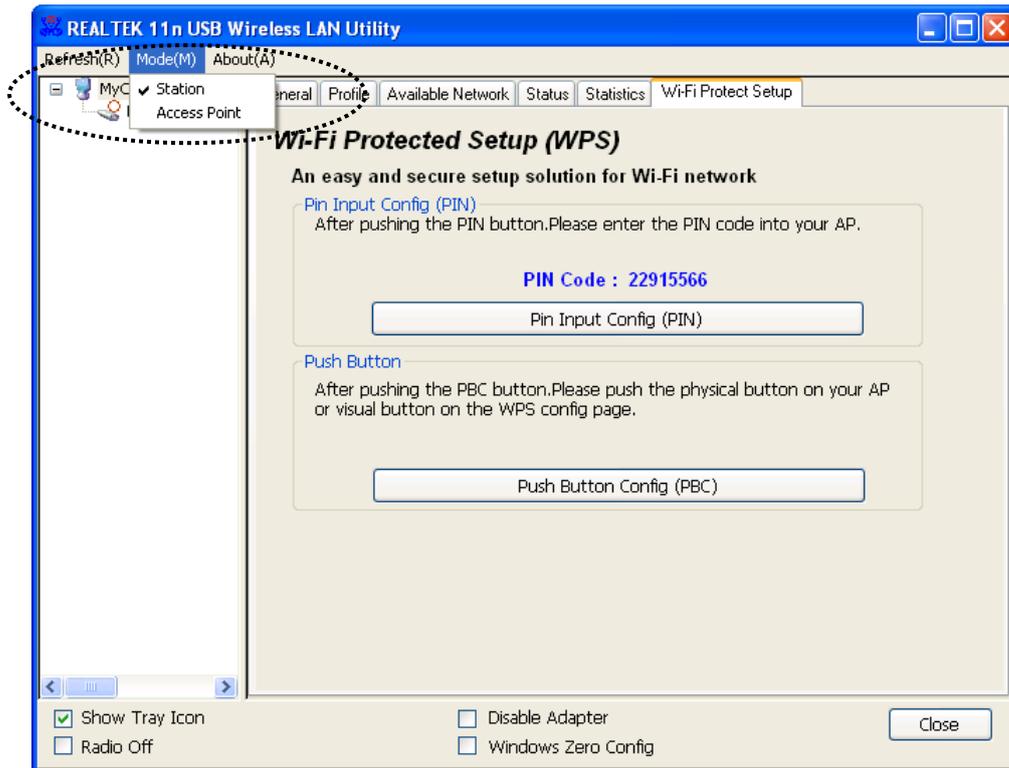
It requires few seconds to switch to AP mode, please be patient.
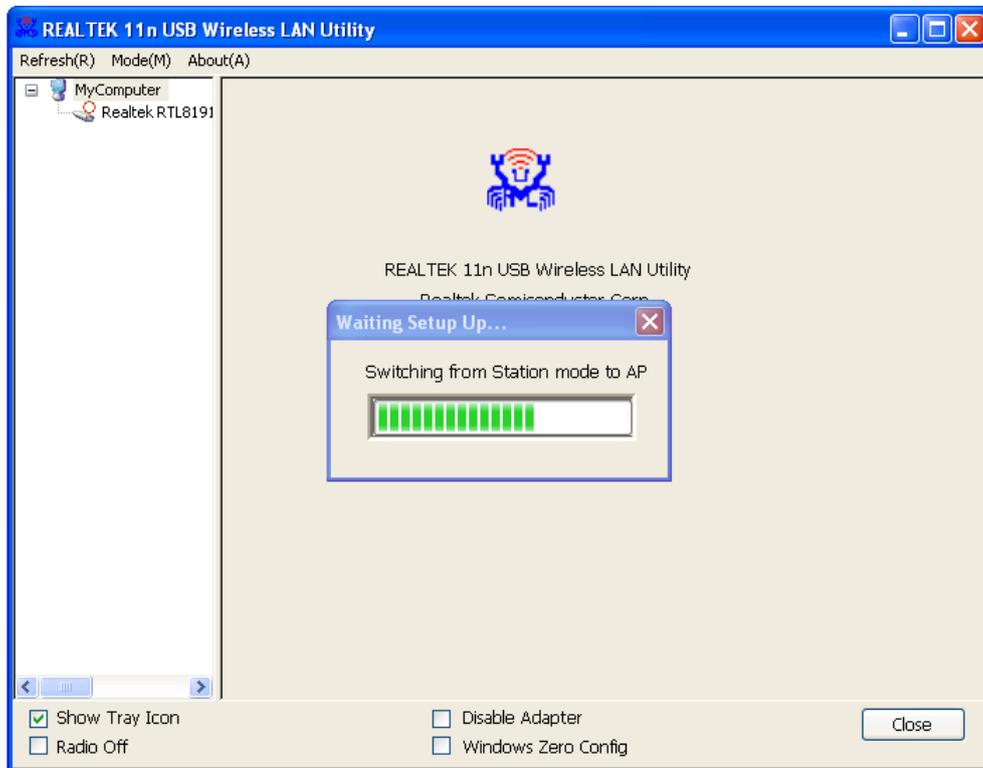
After mode switch is complete, you'll see general information of software AP, which shows AP's SSID and connected wireless clients.
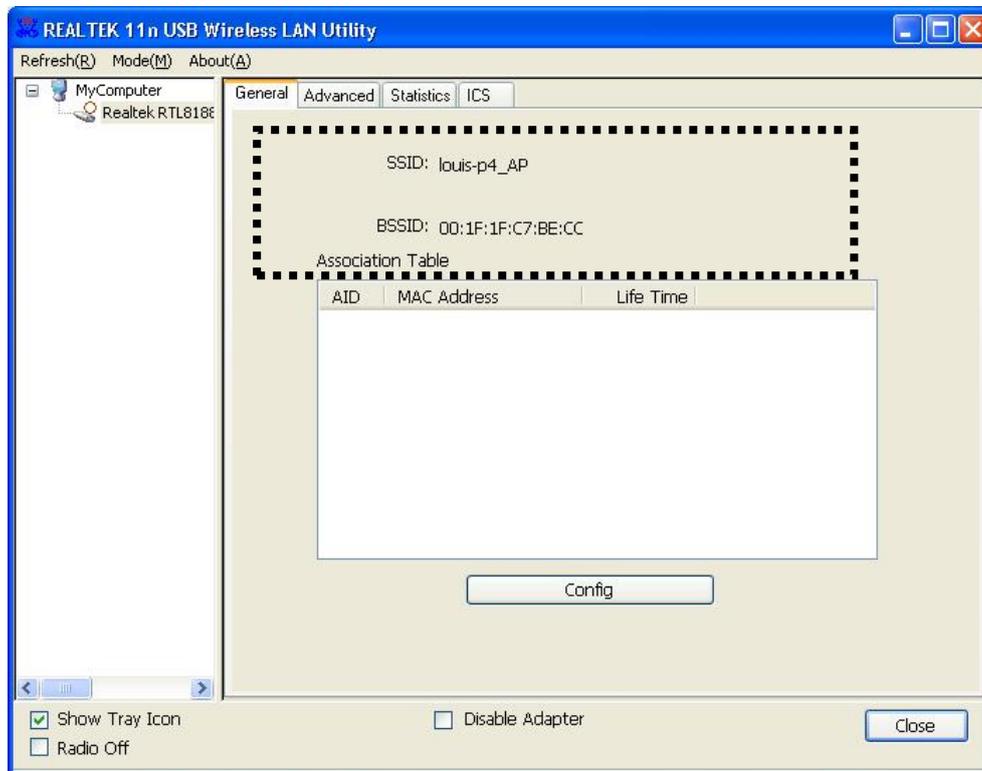
3-1-1 Configure SSID and Channel

To configure software AP, click 'Config' button:
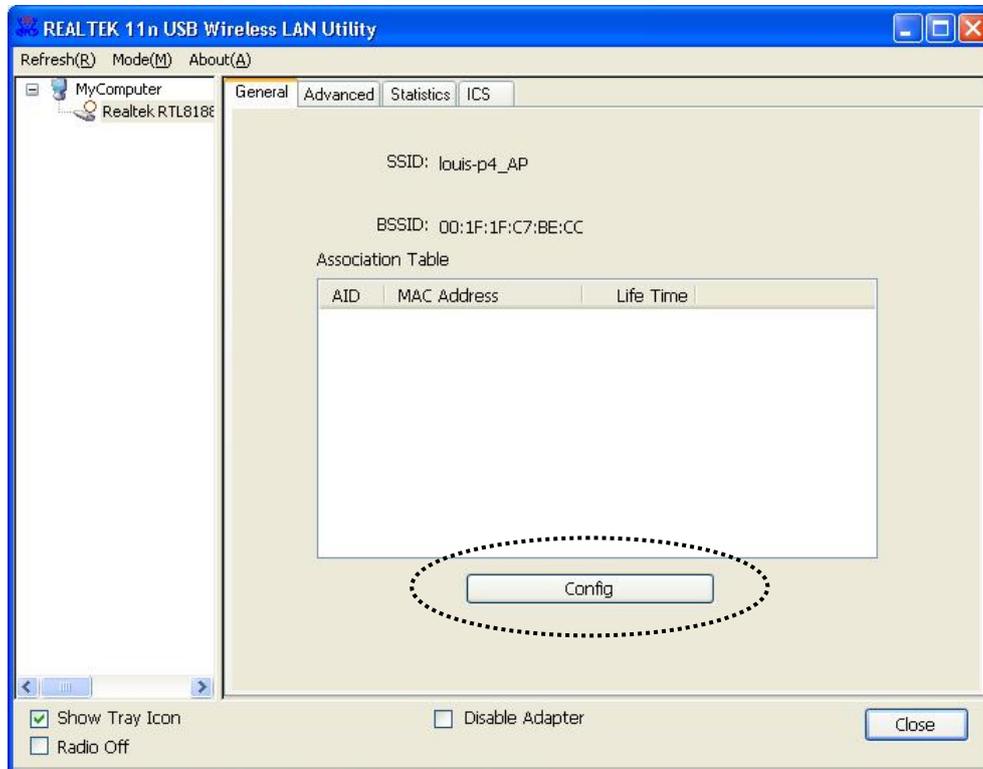
The 'Wireless Network Properties' is displayed.

Note that Ad-Hoc mode is not available when network adapter is in AP
mode. The description of major setup items are listed below:

Network Name (SSID)	Please input the SSID (the name used to identify this wireless access point) here. Up to 32 numerical characters can be accepted here, excepting space.
Channel	Please select the wireless channel you wish to use, from 1 to 13.

To save changes, click 'OK'; otherwise click 'Cancel' to leave this menu
and keep settings untouched.

3-1-2 Setup Soft-AP Security

To setup security options for Soft-AP, configure 'Wireless Network Security' section as follow:
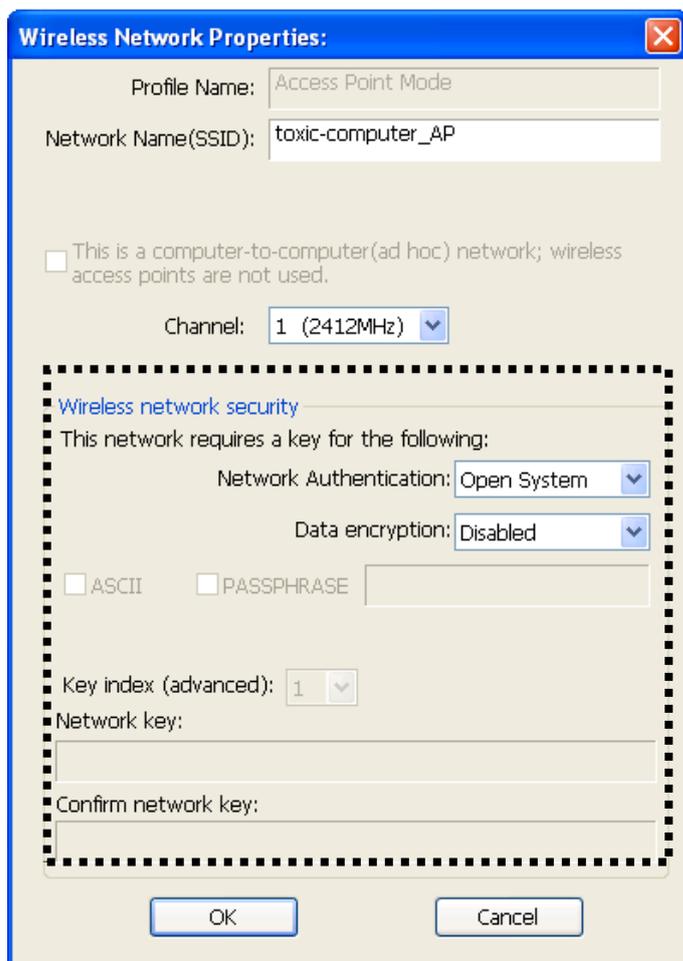
The description of setup items about wireless security are listed below:

Network Authentication	Select network authentication mode from dropdown menu.
Data Encryption	Select data encryption method from dropdown menu.
ASCII / PASSPHRASE	If the encryption method is WEP, check either 'ASCII' or 'PASSPHRASE' box and input it in the box as WEP passphrase.
Key Index	Select WEP key index (1-4). If you don't know which one you should use, select 1.

Network key / Confirm network key	IF network authentication mode is WPA, please input WPA passphrase in both box.

To save changes, click 'OK'; otherwise click 'Cancel' to leave this menu and keep settings untouched.

3-2 Advanced Settings

If you want to setup advanced settings of software access point, select 'Advanced' menu. If you don't know the meaning and affects of these settings, keep them untouched.
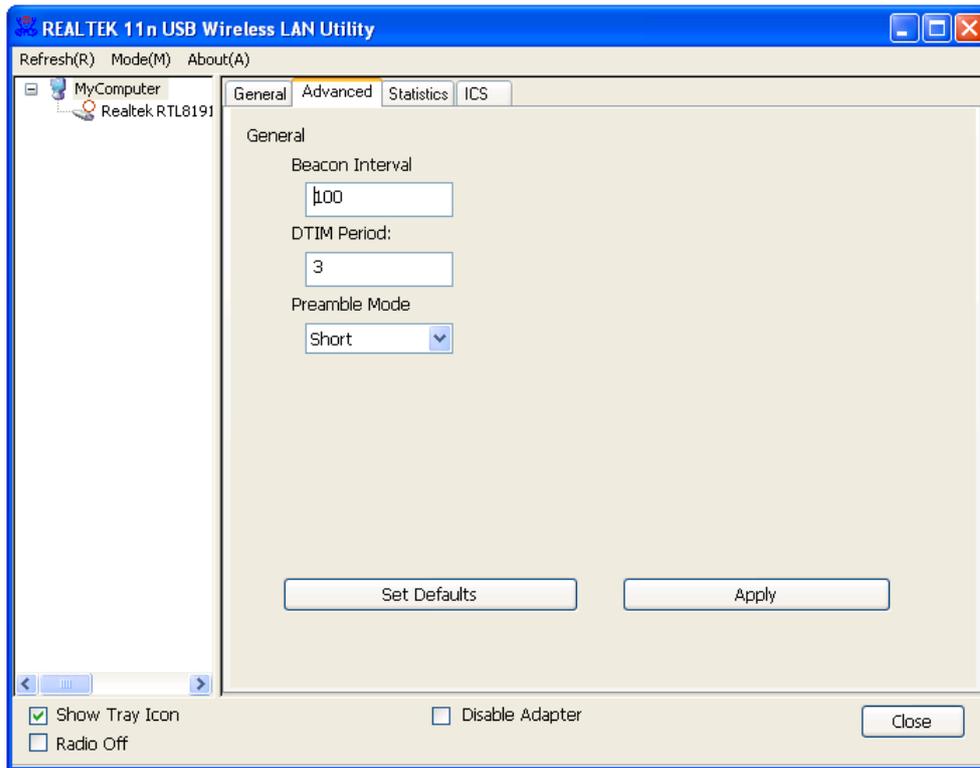
The description of all setup items are listed below:

Beacon Interval	Please input wireless beacon time interval here.
DTIM Period	Please input DTIM (Delivery Traffic Indication Message) here.
Preamble Mode	Select wireless frame preamble mode (long or short) from dropdown menu.
Set Defaults	Reset all settings back to factory default value.
Apply	Save changes.

If you changed any setting here and cause problem on communicating with wireless clients, click 'Set Defaults' to reset all settings back to default setting.

3-3 Wireless Statistics

Select 'Statistics' menu and the data statistics about software access point will be displayed.
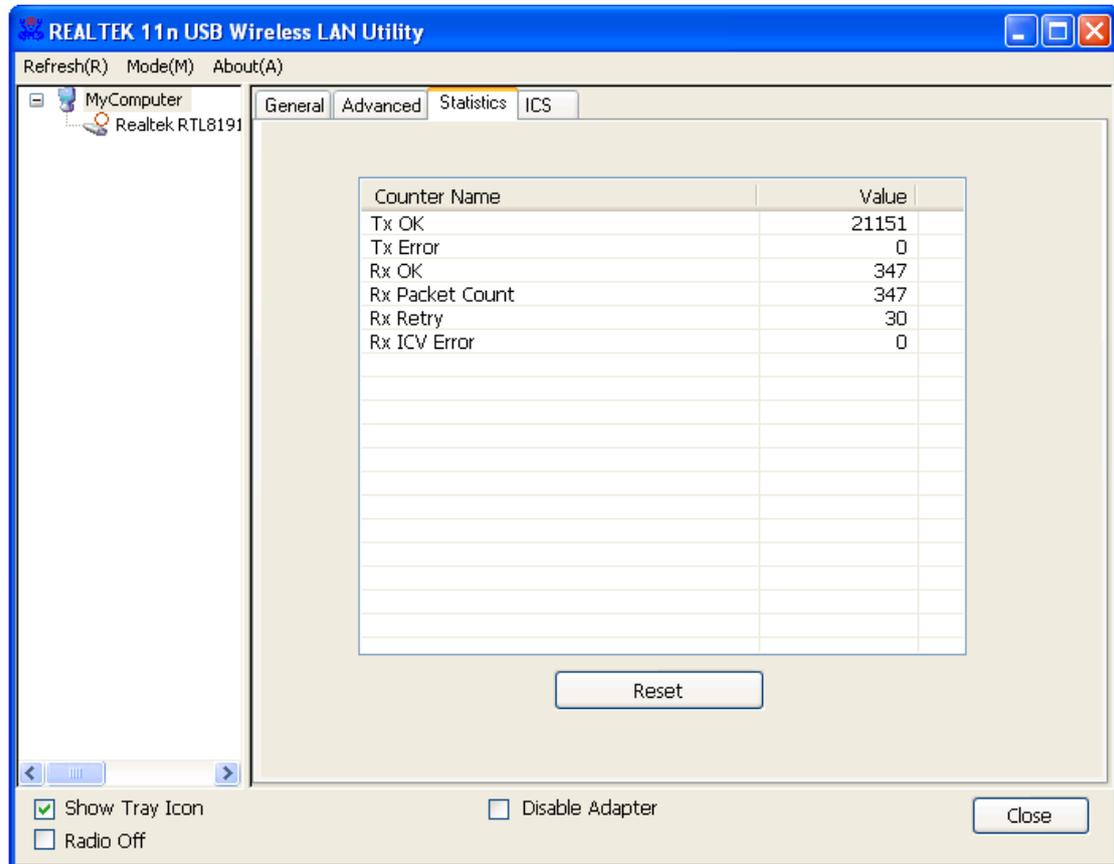
Click 'Reset' to reset the value of every item back to '0'.

3-4 Internet Connection Sharing (ICS)

In this page, you can assign a network adapter on your computer as the path for all wireless clients to get connected to Internet.

If you have only one network adapter (except this software access point), you don't have to select network adapter here; if you have more than one network adapter, select the one you wish to be used as Internet gateway.
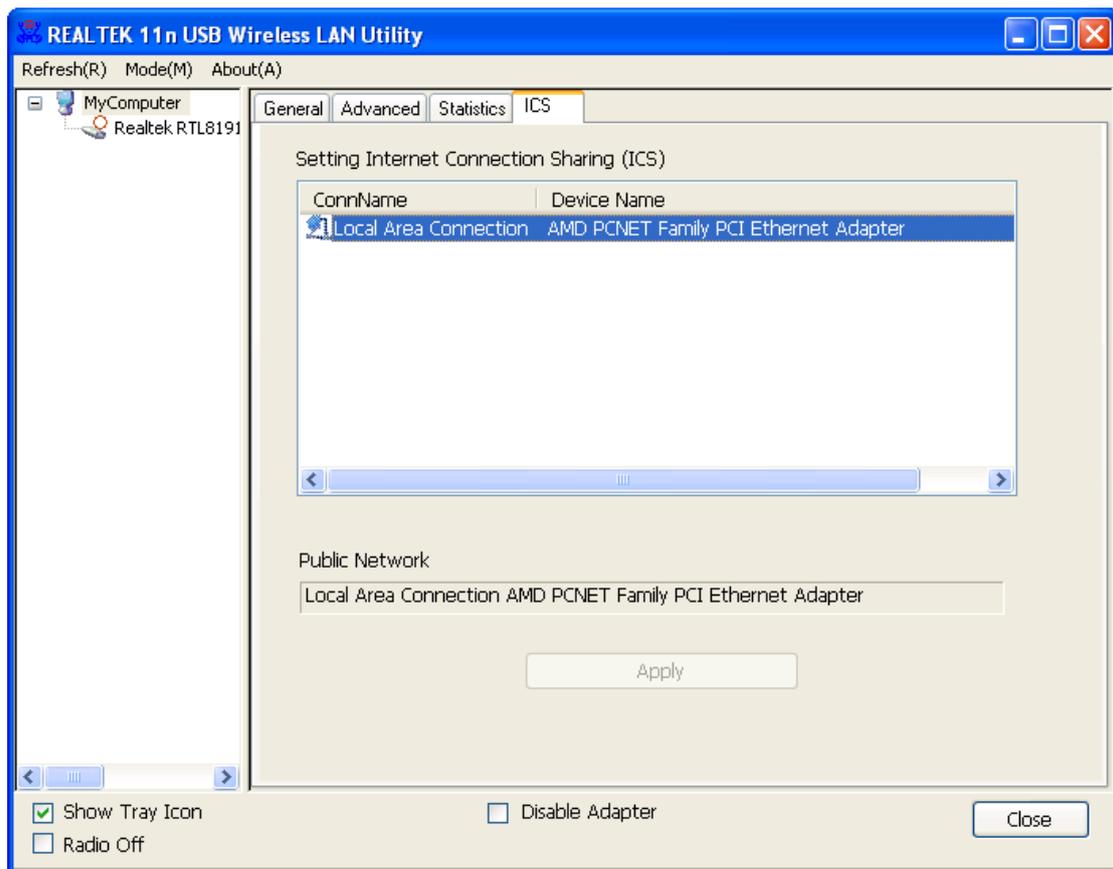
Click 'Apply' to save changes ('Apply' is grayed out when no changes are made in this page).

CHAPTER IV: Appendix

4-1 Hardware Specification

Standards: IEEE 802.11a/b/g/n/ac

Interface: USB 3.0 (USB 2.0 Compatible)

Frequency Band: 2.4000~2.4835GHz (subject to local regulations)

                     5.150~5.825GHz (subject to local regulations)

Data Rate:

       11a: 6/9/12/24/36/48/54Mbps;

       11b: 1/2/5.5/11Mbps; 11g: 6/9/12/24/36/48/54Mbps

       11n (20MHz): MCS0-15, up to 144Mbps

       11n (40MHz): MCS0-15, up to 300Mbps

       11ac (80MHz): VHTMCS0-9, up to 867Mbps

Securities: WEP 64/128, WPA, WPA2 and IEEE 802.1x

Antenna: 2 internal PIFA antennas (2.4G/5G 2dBi)

Drivers: Windows XP / Vista / 7 / 8, Linux, MAC OS

LED: Link/Act/WPS

TX Power: 2.4GHz: 11b(11M): 16±1.5 dBm , 11g(54M): 14±1.5 dBm

                 11n(20MHz, MCS7): 14±1.5 dBm,

                 11n(40MHz, MCS7): 12±1.5 dBm

         5GHz: 11a(54M): 12±1.5 dBm,

               11n(20MHz, MCS7): 10±1.5 dBm,

               11n(40MHz, MCS7): 10±1.5 dBm

               11ac(80MHz, VHTMCS9): 10±1.0 dBm

RX Sensitivity: 2.4GHz: 11b(11M): -79±2 dBm, 11g(54M): -65±2dBm

                 11n(20MHz, MCS7): -64±2dBm,

                 11n(40MHz, MCS7): -61±2dBm

         5GHz: 11a(54M): -70±2dBm,

               11n(20MHz, MCS7): -67±2dBm,

               11n(40MHz, MCS7): -64±2dBm,

               11ac(80MHz, VHTMCS9): -51±2dBm

Dimension: 87.1 (L) x 27.2 (W) x 17.2 (H) mm

Temperature: 32~104°F (0 ~ 40°C), Humidity: 10-95% (Non-Condensing)

Certification: FCC, CE

4-2 Troubleshooting

If you encounter any problem when you're using this wireless network adapter, don't panic! Before you call your dealer of purchase for help, please check this troubleshooting table, the solution of your problem could be very simple, and you can solve the problem by yourself!

Scenario	Solution
I can't find any wireless access point / wireless device in 'Site Survey' function.	1. Click 'Rescan' for few more times and see if you can find any wireless access point or wireless device. 2. Please move closer to any known wireless access point. 3. 'Ad hoc' function must be enabled for the wireless device you wish to establish a direct wireless link. 4. Please adjust the position of network adapter (you may have to move your computer if you're using a notebook computer) and click 'Rescan' button for few more times. If you can find the wireless access point or wireless device you want to connect by doing this, try to move closer to the place where the wireless access point or wireless device is located.
Nothing happens when I click 'Open Config Utility'	1. Please make sure the wireless network adapter is inserted into your computer's USB port. 2. Reboot the computer and try again. 3. Remove the adapter and insert it into another USB port. 4. Remove the driver and re-install. 5. Contact the dealer of purchase for help.
I cannot establish connection with a certain wireless access point	1. Click 'Add to Profile' for few more times. 2. If the SSID of access point you wish to

Scenario	Solution
	connect is hidden (nothing displayed in 'SSID' field in 'Site Survey' function), you have to input correct SSID of the access point you wish to connect. Please contact the owner of access point to ask for correct SSID.
	3. You have to input correct passphrase / security key to connect an access point with encryption. Please contact the owner of access point to ask for correct passphrase / security key.
	4. The access point you wish to connect only allows network adapters with specific MAC address to establish connection. Please go to 'Status' menu and write the value of 'MAC Address' down, then present this value to the owner of access point so he / she can add the MAC address of your network adapter to his / her access point's list.
The network is slow / having problem when transferring large files	1. Move closer to the place where access point is located.
	2. There could be too much people using the same radio channel. Ask the owner of the access point to change the channel number.
	Please try one or more solutions listed above.

4-3 Glossary

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 adapter, 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).

14. What is WPS?
WPS stands for Wi-Fi Protected Setup. It provides a simple way to establish unencrypted or encrypted connections between wireless clients and access point automatically. User can press a software or hardware button to activate WPS function, and WPS-compatible wireless clients and access point will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.