

WUBR-502GN
Wireless-GN USB Dongle

User's Manual

Version 1.0

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise without the prior writing of the publisher.

JULY 2008

Contents

1. Introduction	4
2. Wireless LAN Basics.....	5
3. Installation for Windows platform.....	6
3.1. Installation Overview.....	6
3.2. Install Procedure for Windows.....	7
3.3 Uninstall Procedure.....	13
4. Connect to Wireless Access Point	14
4.1 Connect to Wireless Access Point	15
4.2 Using Windows Zero Configuration	19
4.3 Connection Profile Management.....	23
4.4 View Network Statistics and Link Status	31
4.5 Advanced Settings	34
4.6 QoS Setting.....	36
4.7 WPS Configuration.....	38
4.8 About	43
5. Soft-AP Function:	44
5.1 Switch to AP Mode and Basic Configuration.....	44
5.2 Security Settings	47
5.3 Access Control	49
5.4 Connection table	51
5.5 Event Log	53
5.6 Statistics	54
6. APPENDIX	55
6.1 Hardware Specification.....	55
6.2 Troubleshooting	56
6.3 Glossary	58

1. Introduction

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

Package Contents

Please make sure you have the following in the box:

- ◆ Wireless-GN USB Dongle
- ◆ Protection Cap
- ◆ Quick installation guide
- ◆ User manual / device driver CDROM

Note: if anything is missing, please contact your vendor

2. Wireless LAN Basics

Wireless LAN (Local Area Networks) systems offer a great number of advantages over a traditional, wired system. Wireless LANs (WLANs) are more flexible, easier to setup and manage and often more cost effective than their wired equivalence.

Using radio frequency (RF) technology, WLANs transmit and receive data over the air, minimizing the need for wired connections. Therefore, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs.

With wireless LANs, users can access shared information without looking for a place to plug in and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, convenience and cost advantages over traditional wired networks:

- **Mobility** - Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- **Installation Speed and Simplicity** - Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- **Installation Flexibility** - Wireless technology allows the network to go where wires cannot go.
- **Reduced Cost-of-Ownership** - While the initial investment required for wireless LAN hardware might be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs will be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds, and changes.
- **Scalability** - Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer to full infrastructure networks, also allow roaming over a broad area.

3. Installation for Windows platform

The following section will assist you in installing wireless LAN Adapter successfully. You will first install software (Utility) and then insert / attach the Wireless LAN Adapter to your system, and finally set the network properties to accommodate resource sharing and select the type of wireless network that you wish to install. The Wireless LAN card can easily be installed and used, without bothering to connect cables for keeping your computer to use network resources.

3.1. Installation Overview

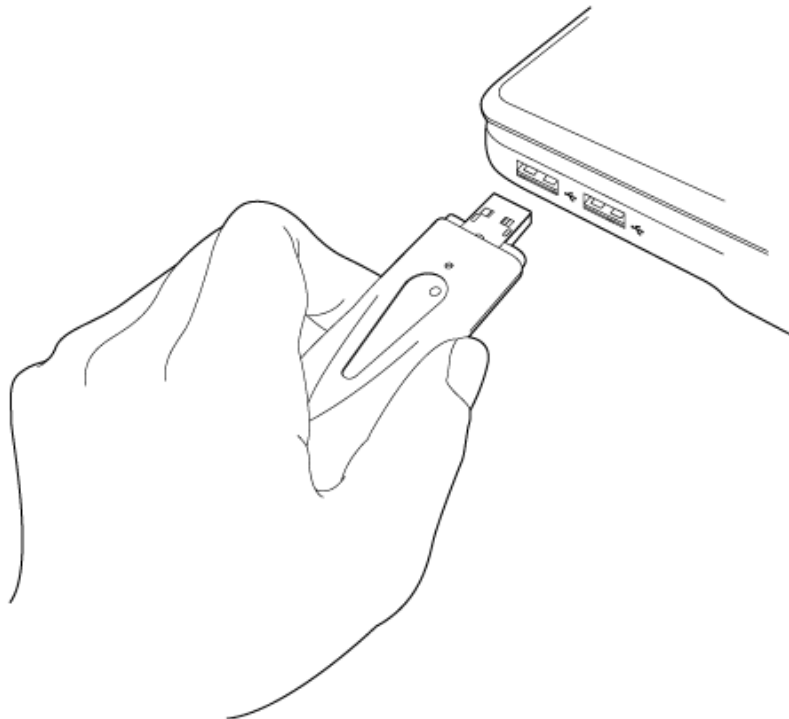
Here are some steps you will perform in establishing your wireless network connection:

- Install the Access Point at first. AP is needed in case of Infrastructure network mode.
- Install the software using the Install CD.
- Install the Wireless LAN Card.
- Install the network protocol(s) required to communicate on your network. Most likely you will need the TCP/IP protocol.

3.2. Install Procedure for Windows

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

1. Insert the USB wireless network card into an empty USB 2.0 port of your computer when computer is switched on. Never use force to insert the card, if you feel it's stuck, flip the card over and try again.



2. The following message will appear on your computer, click 'cancel'.



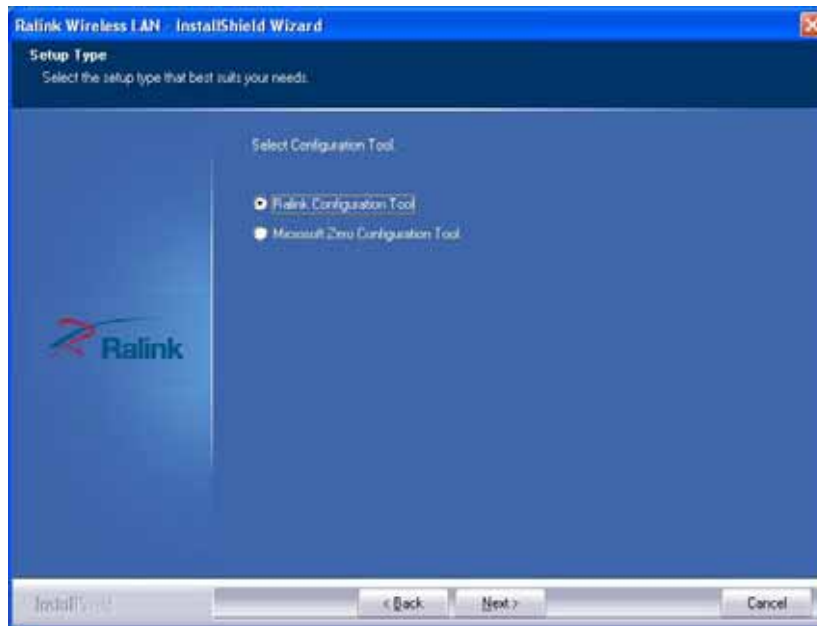
3. Insert the given Install CD in the CD-ROM, and wait for the Autorun prompt. If Autorun does not work, please browse the CD content and double click the “ Autorun.exe ”.



4. Click the “Driver” for beginning the installation.

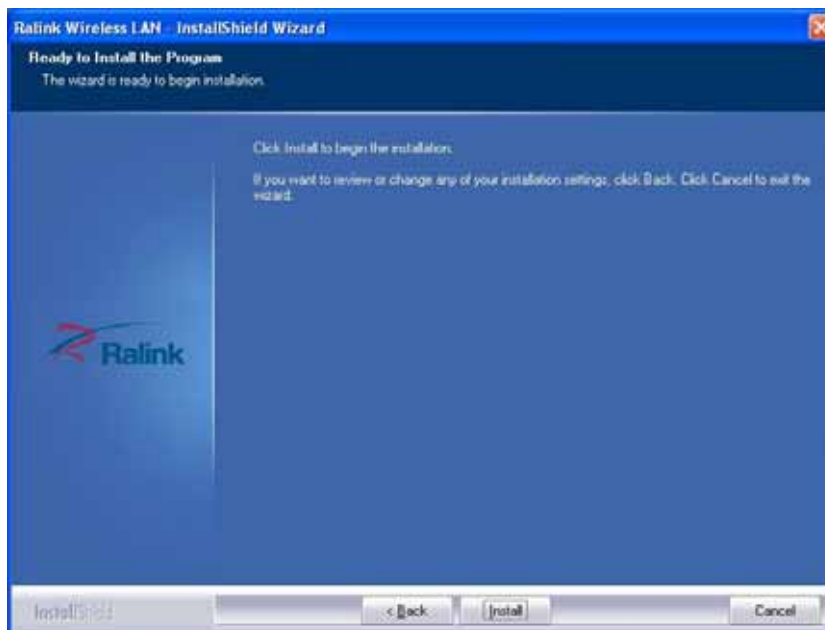


5. You can choose the configuration tool used to configure the wireless network card here. It's recommended to select 'Ralink Configuration Tool', which provides fully access to all function of this wireless network card. If you prefer to use the wireless configuration tool provided by Windows XP or Vista, please select 'Microsoft Zero Configuration Tool', then click 'Next'.



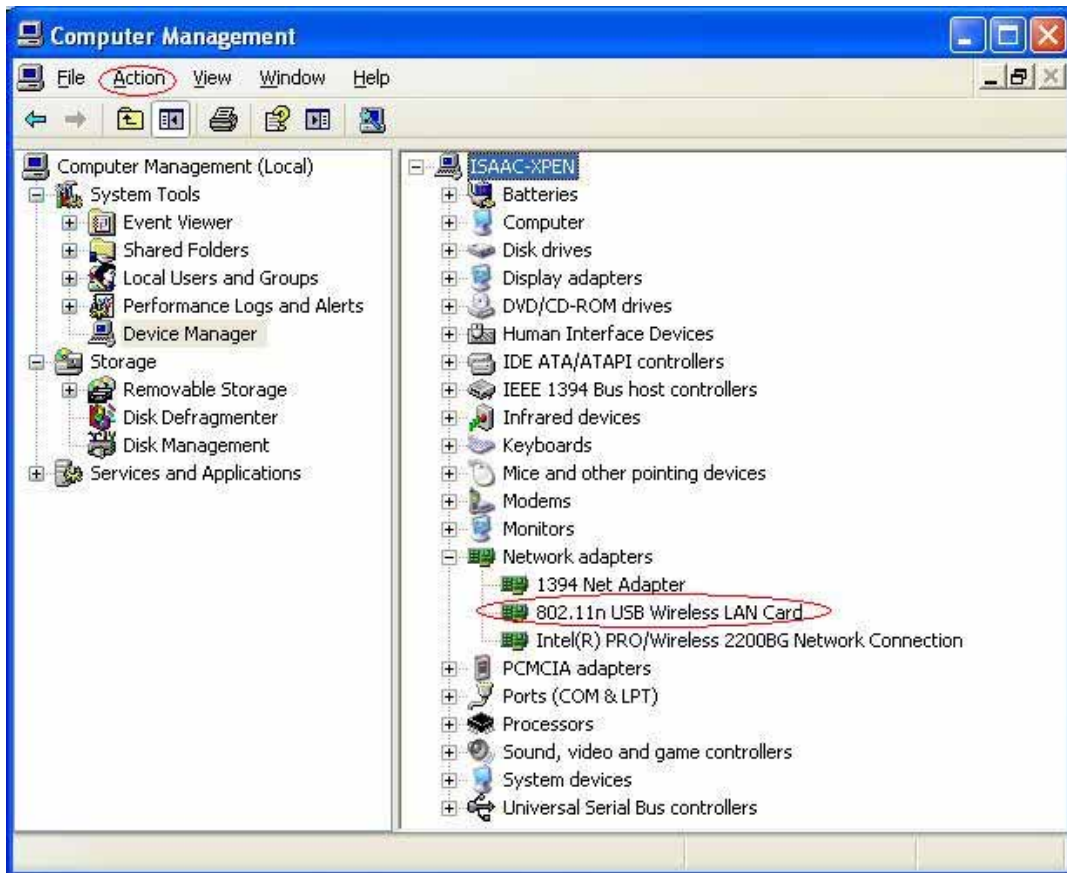
When you select one mode, please click 'Next' to continue. If you see 'Found New Hardware' message again, please ignore it and wait.

7. Please wait while the install procedure is running. When you see this message, please click 'Finish' to complete the driver installation process.

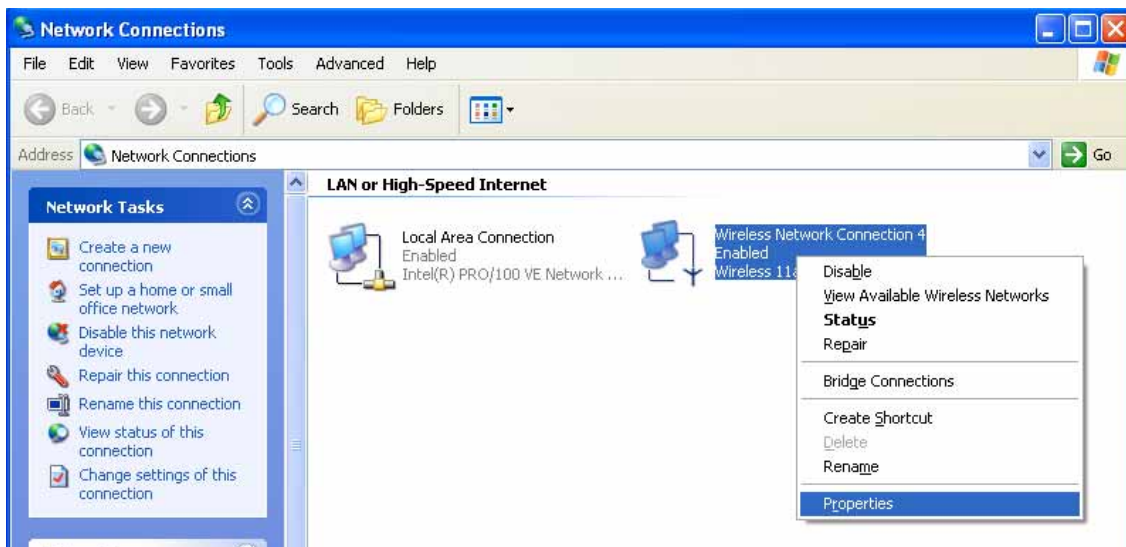


Note: If the wireless network card is PCI interface, then you should shut down your computer first then power on your computer after you complete the card insertion.

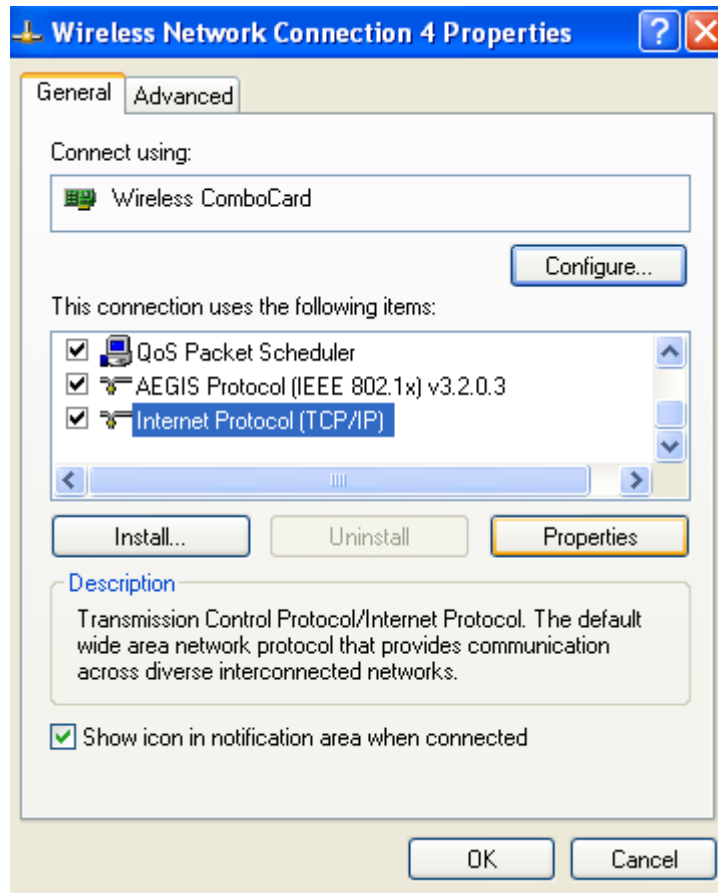
8. Click the right button of mouse on **My Computer** → **Manage** → **Device Manager**. Check whether it has WLAN adapter in one of the sockets or not. If you find **Wireless 11n USB Dongle** in one of the sockets, it means the card is detected properly. If you cannot find this adapter on device manager, please click the **Action** → **Scan for hardware changes** to search again. If this adapter is shown with yellow exclamation mark, please remove it and click the **Action** → **Scan for hardware changes** to search this hardware again for proper hardware installation.



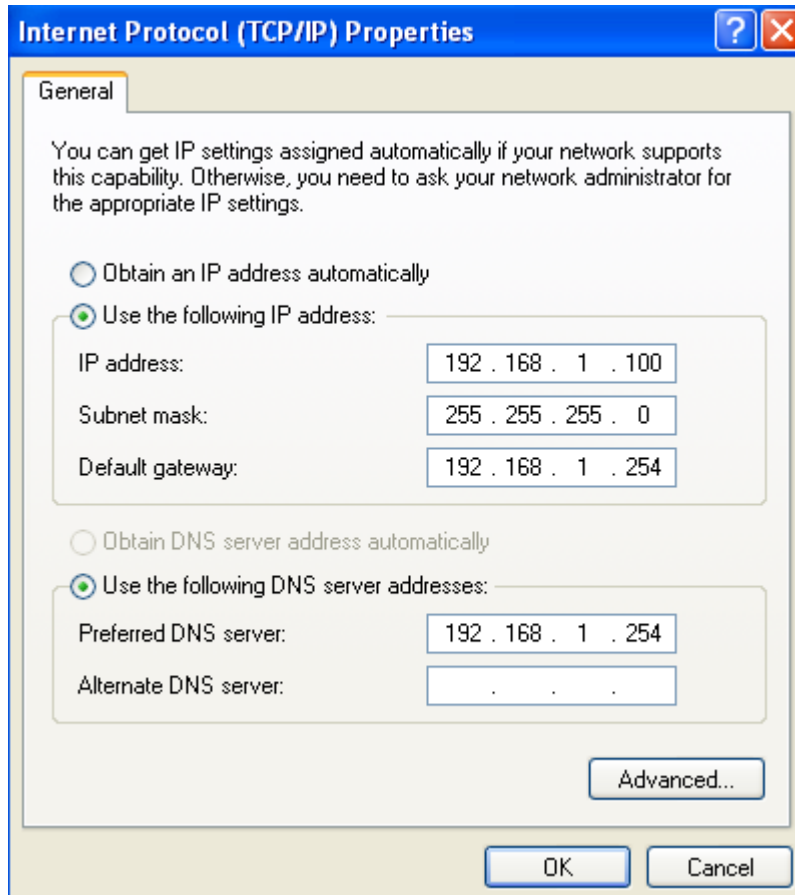
9. Click **Start** → **Settings** → **Network Connections** or right click mouse on the **My Network Places (Network Neighborhood)** for TCP/IP setting.



10. Click **Properties** from the pop up menu. Select the **Internet Protocol(TCP/IP)** and click Properties button.



11. You can select either **Obtain an IP address automatically** or **Use the following IP address setting**. If your choice is the second one then entering the **IP address**, **Subnet mask**, **Default gateway** and **DNS**. After setting these parameters appropriately, click OK to make the changes work.



Note: Above figure is an example for IP address setting. Please use the one of your own !

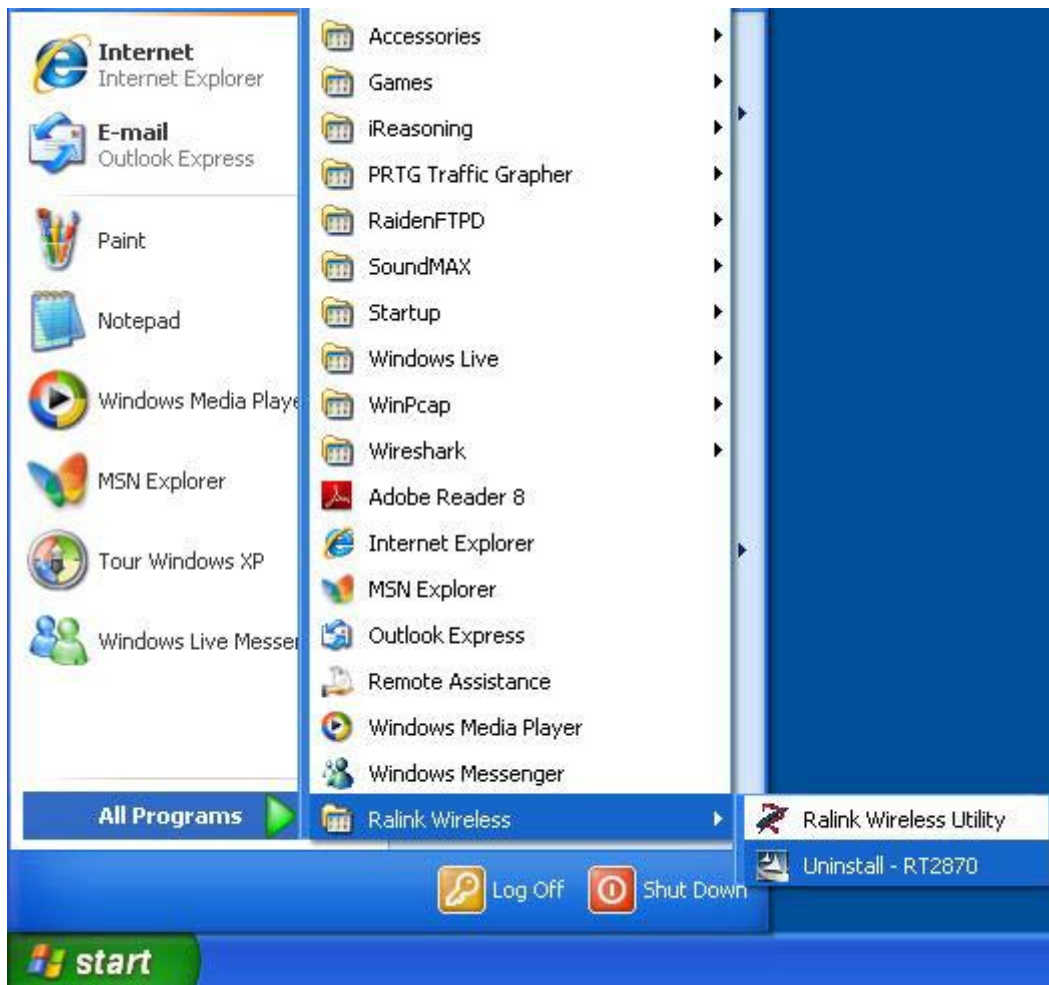
3.3 Uninstall Procedure

Step 1:

If you want to uninstall the WLAN adapter, just simply click

Start → Program → Ralink Wireless → Uninstall – RT2870

It shall uninstall all related programs.




Step 2:

Restart your Computer.

4. Connect to Wireless Access Point

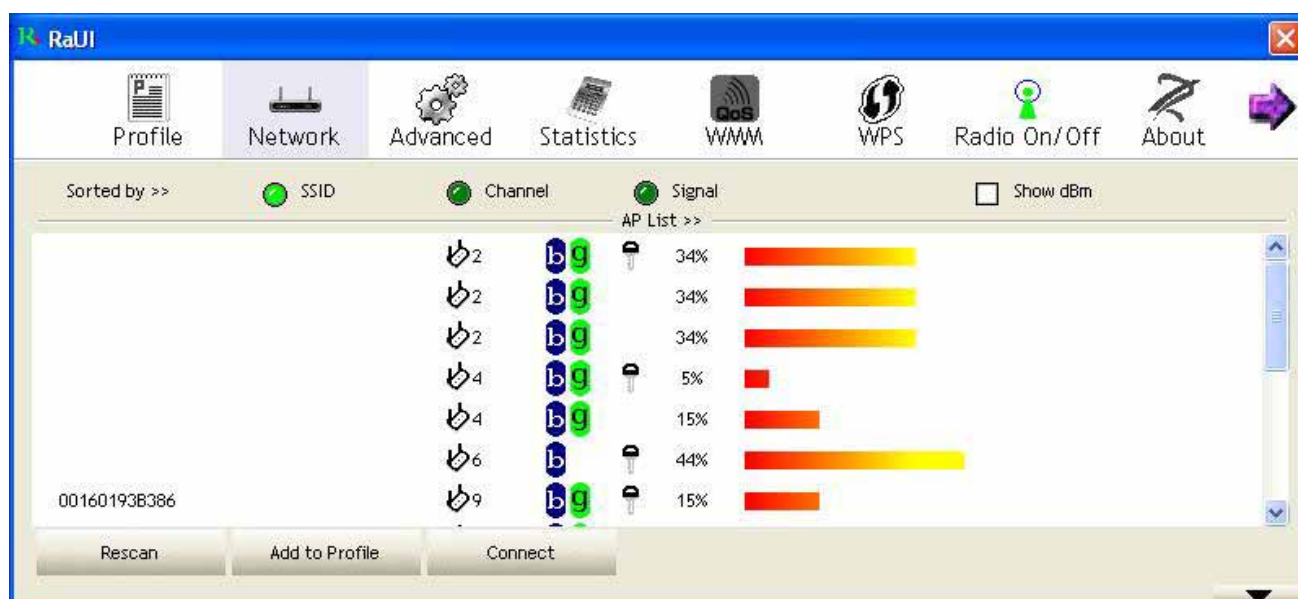
Wireless network adapter uses its own management software. All functions controlled by user are provided by this application.

Usually this application starts automatically, or click  icon from Start Menu to start the Utility application.

A new icon -  should appear in your Icon tray if your WLAN adapter is working properly. If the icon is in red color, it means that WLAN adapter is under poor signal or the connection is unavailable.



User can navigate through “sheets” by clicking tabs; “X” button will minimize the window. To provide more link information, click “More...” button. Below description explains the usage of this utility.

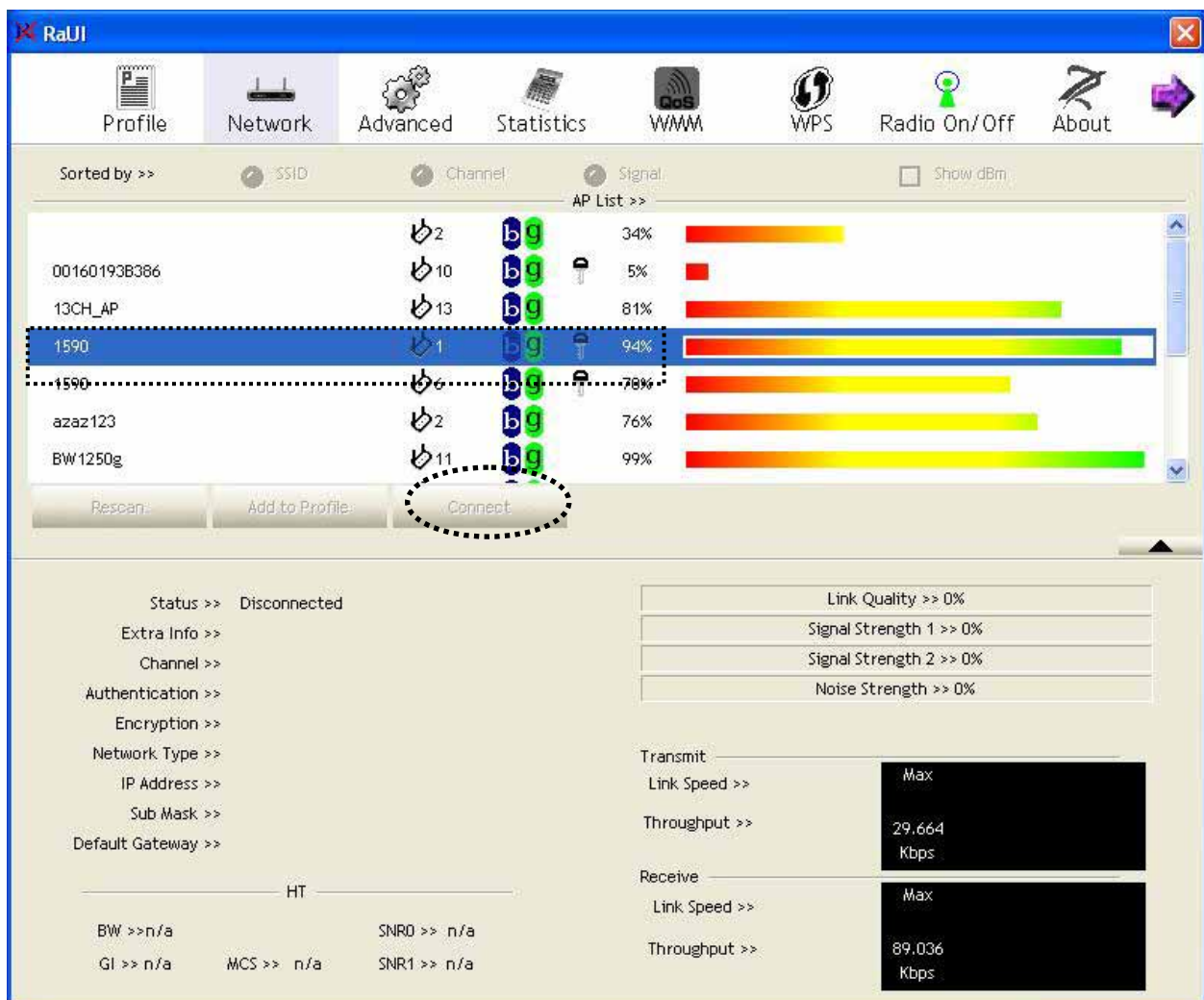


4.1 Connect to Wireless Access Point

Configuration utility will scan for all wireless access points automatically. Scan results will be displayed here, please check if the wireless access point with the SSID (the name of wireless access point) you preferred is shown here.

If the wireless access point you wish to connect does not show here, please click 'Rescan' to try again, until the one you preferred is displayed. You may have to click 'Rescan' for more than two times before you can see the access point you wish to use here sometimes.

1. Click the wireless access point or network device you wish to connect, it will be highlighted, then click 'Connect'.

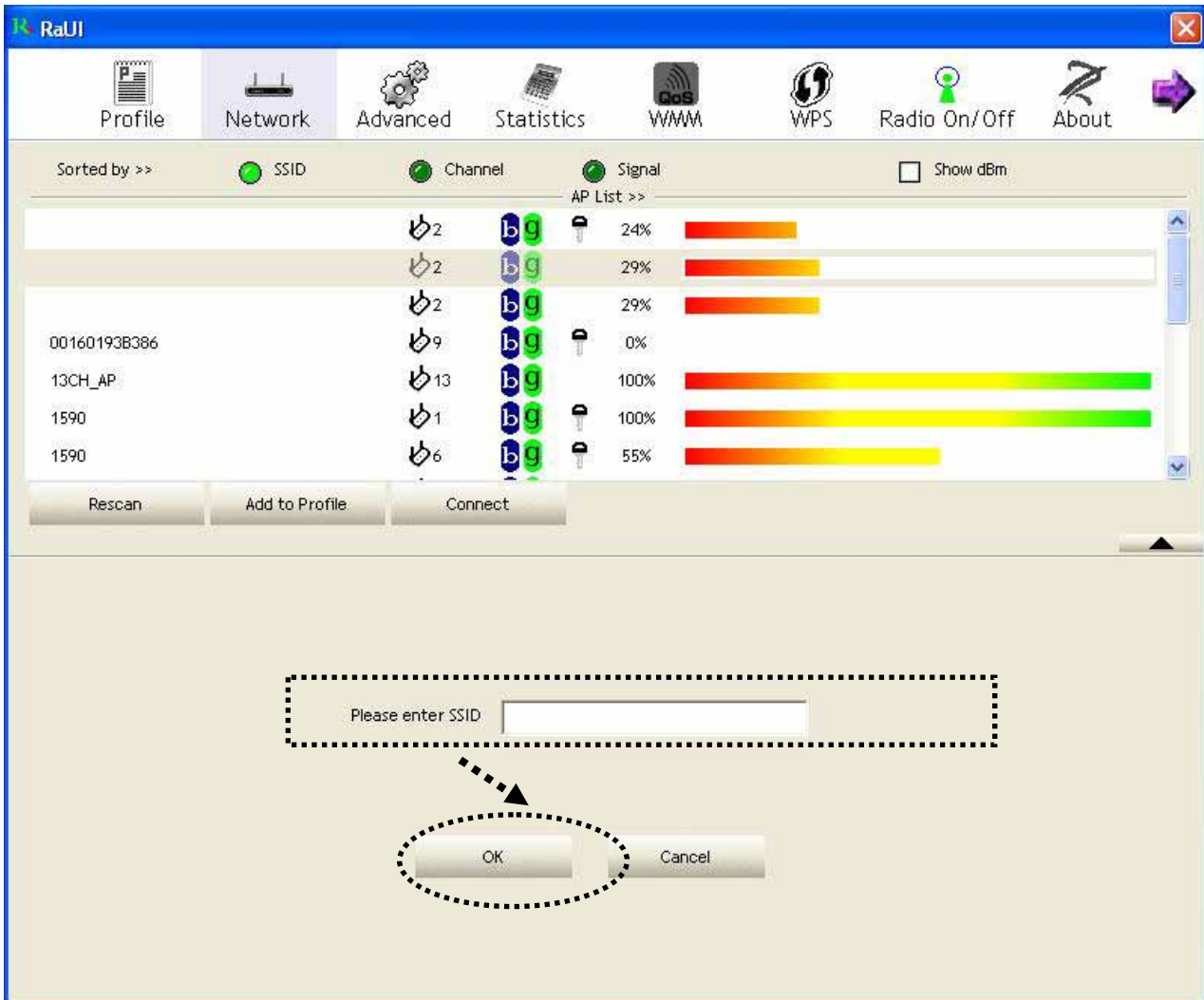


If the access point you selected does not enable encryption (The content of 'Encryption' field of the access point you selected is 'None', you'll be connected to this wireless access point within one minute. Please jump to step 4.

If the access point you selected enables encryption, please proceed to next step.

2. If the wireless access point does not have SSID, you'll be prompted to input it here. Please ask the owner of wireless access point and input the exact SSID here, then click 'OK' when ready. If the SSID you provided here is wrong, you'll not be able to connect to this access point.

If the wireless access point you selected have SSID, please skip this step.



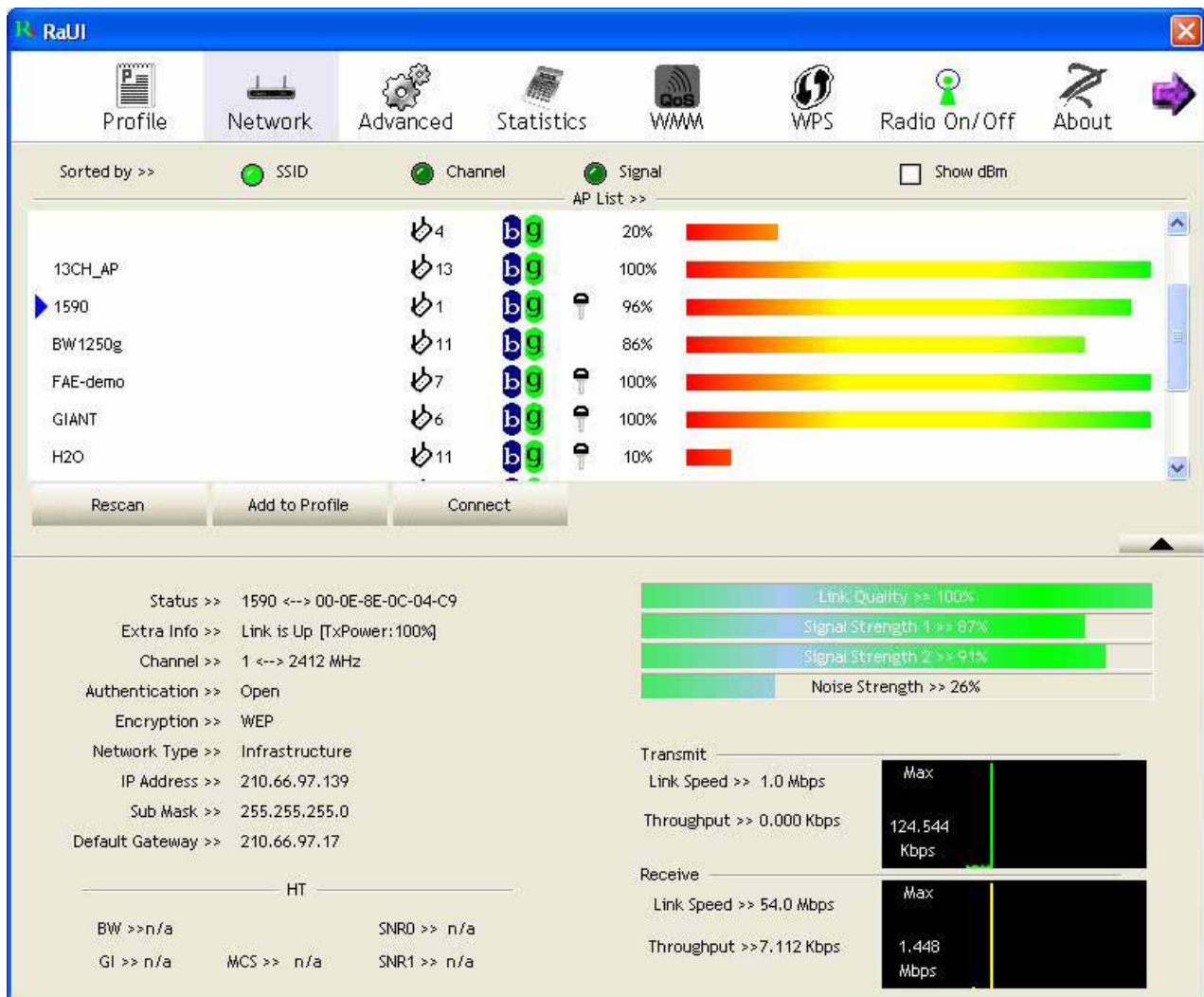
3. If the wireless access point uses encryption, you have to input WEP passphrase or WPA preshared key. Please ask the owner of the wireless access point you want to connect, and input the correct passphrase / preshared key here, then click 'OK'. If the value you inputted here is wrong, you will not be able to connect to this wireless access point.

Authentication type is selected automatically, please don't change it.

If the access point you selected does not enable encryption and does not require authentication, please skip this step.



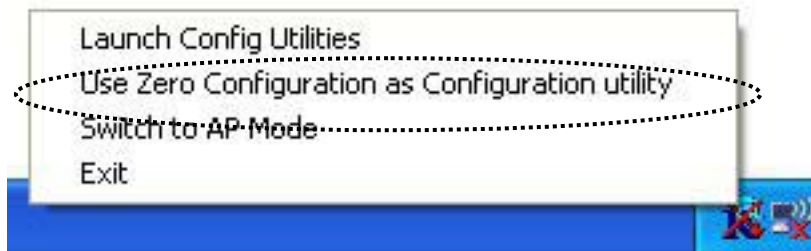
4. You'll see 'Status' (SSID and MAC address of the wireless access point or wireless device you connected to) message displayed at lower-left corner of configuration utility, congratulations, you're successfully connected to the access point or wireless device you selected!



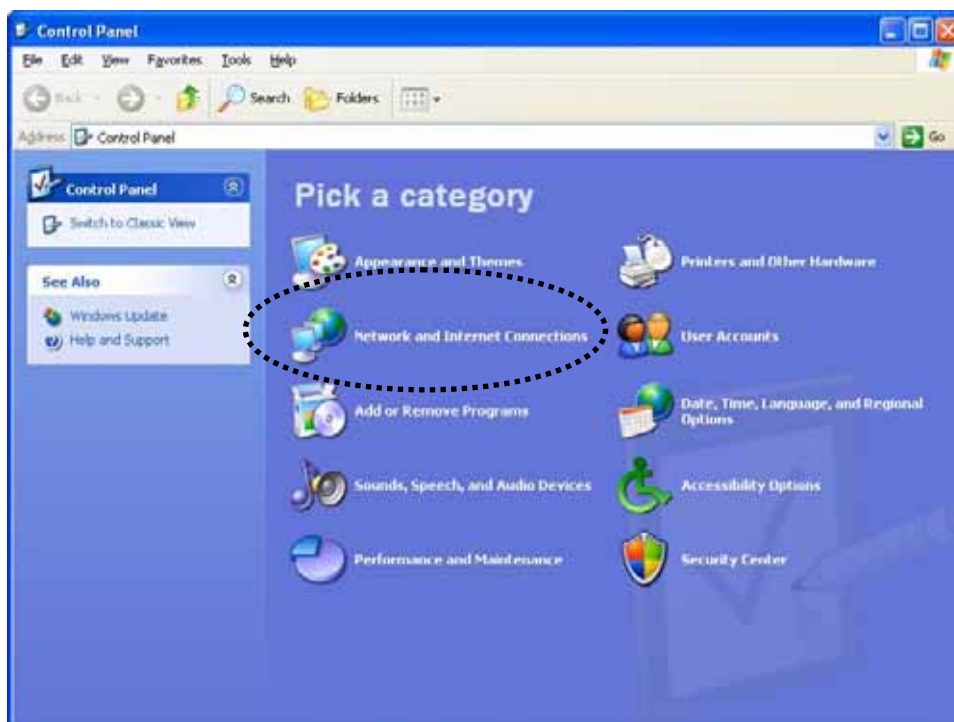
4.2 Using Windows Zero Configuration

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 Ralink configuration utility icon and select 'Use Zero Configuration as Configuration utility'.



2. Click '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.



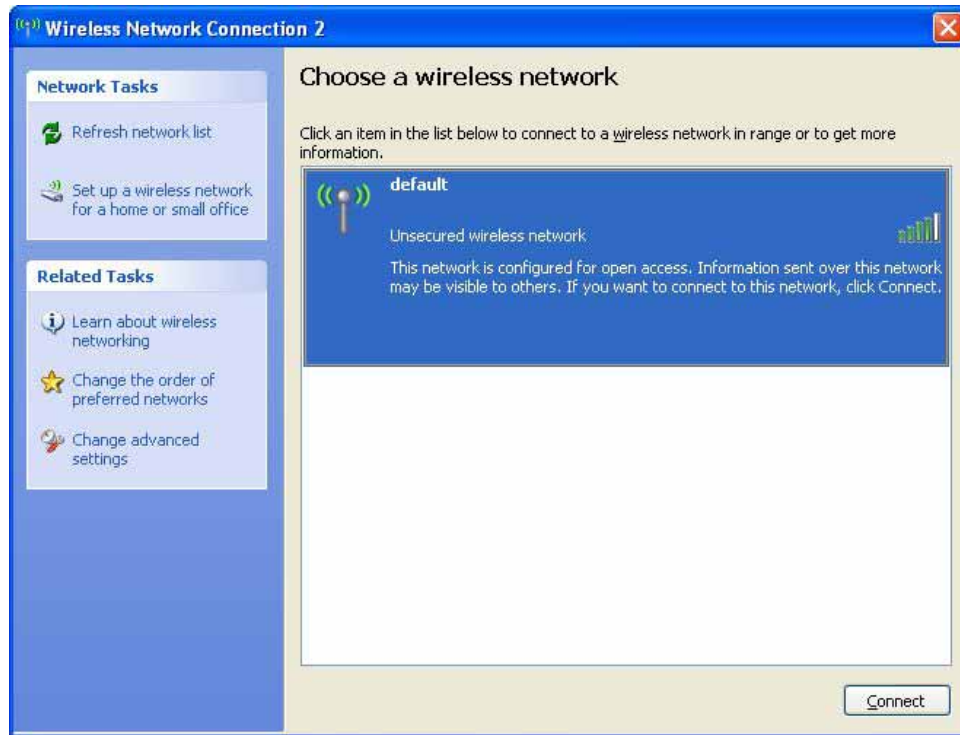
3. Click 'Connect to a network' under 'Network Connections'



4. Right-click 'Wireless Network Connection' (it may have a number as suffix if you have more than one wireless network card, please make sure you right-click the 'Ralink 802.11n Wireless LAN Card'), then select 'View Available Wireless Networks'.



5. 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 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'.

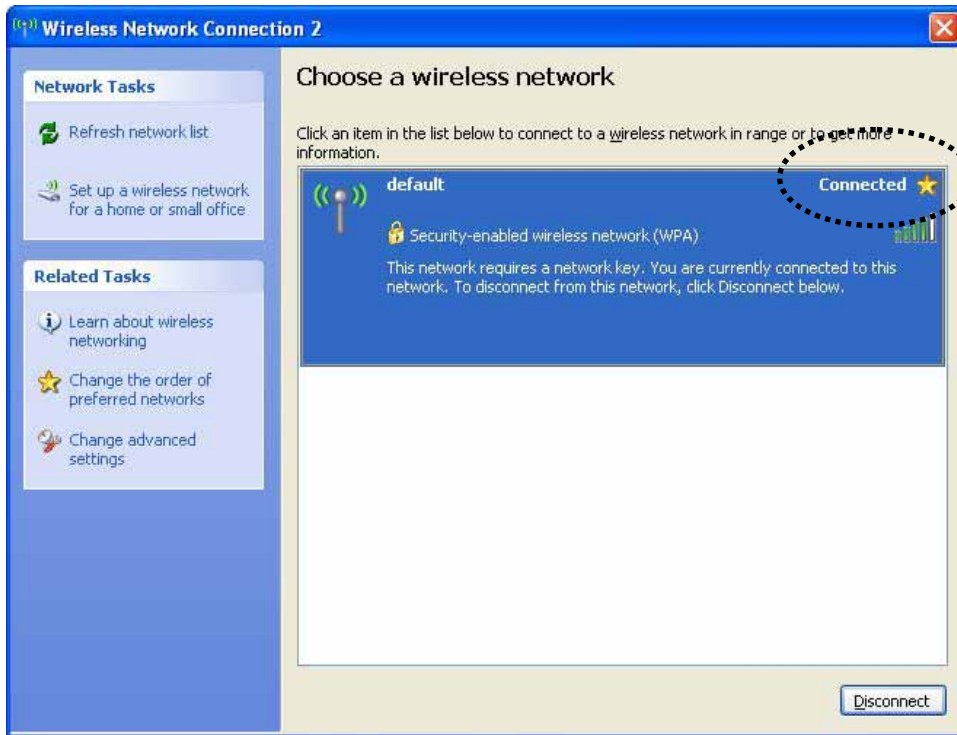


6. If the access point is protected by encryption, you have to input its security key or passphrase here. It must match the encryption setting on the access point.

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



7. If you can see 'Connected' message, the connection between your computer and wireless access point is successfully established.

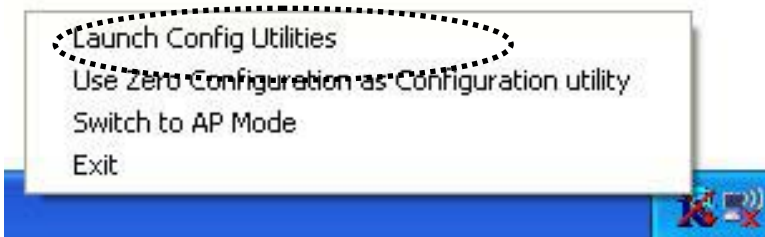


4.3 Connection Profile Management

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 etc, etc.) as a profile for every access point, so you don't have in input these parameters every time you want to connect to a specific wireless access point.

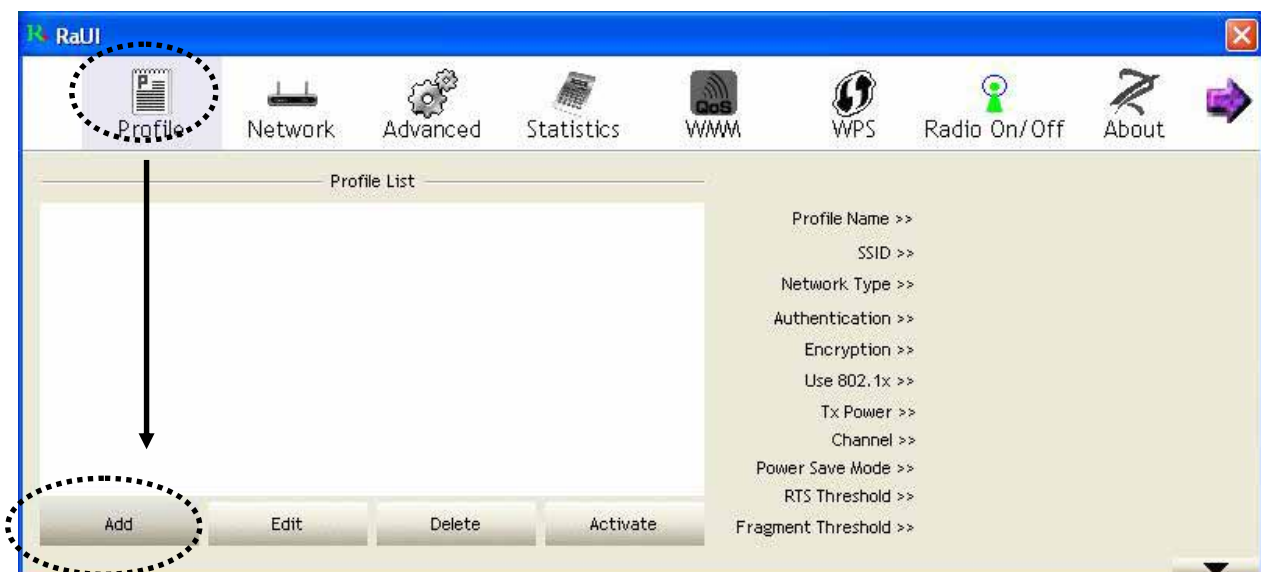
◆ Make a profile for an access point or wireless device

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.

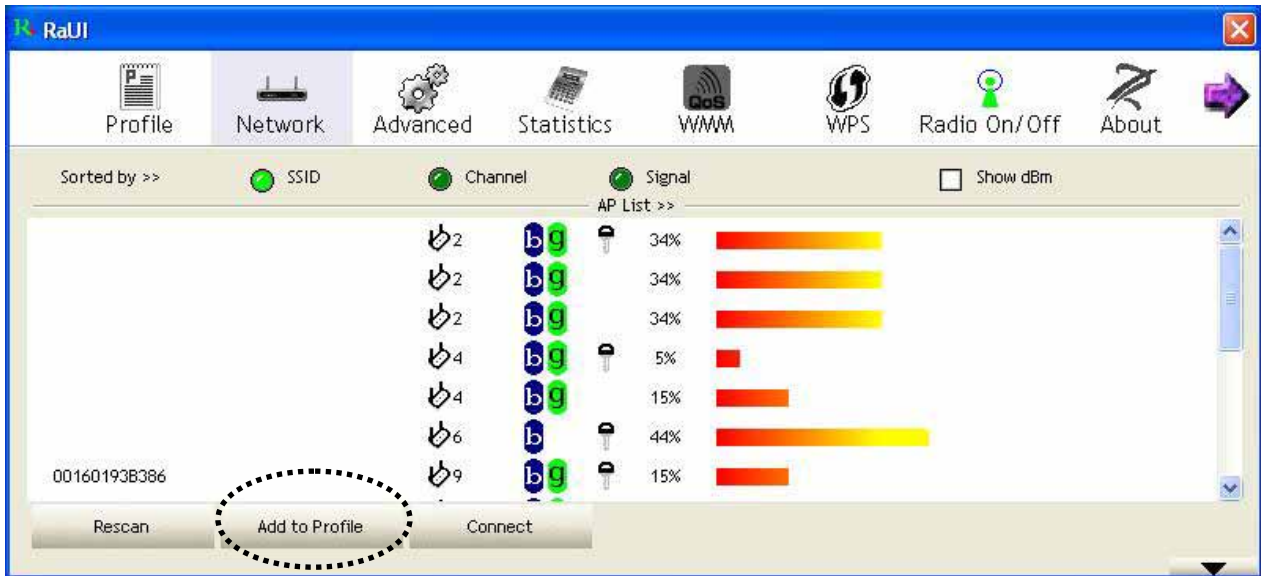


2. There are two ways to add a new connection profile:
Create a new profile,
or
Add a profile from an existing wireless access point or wireless device

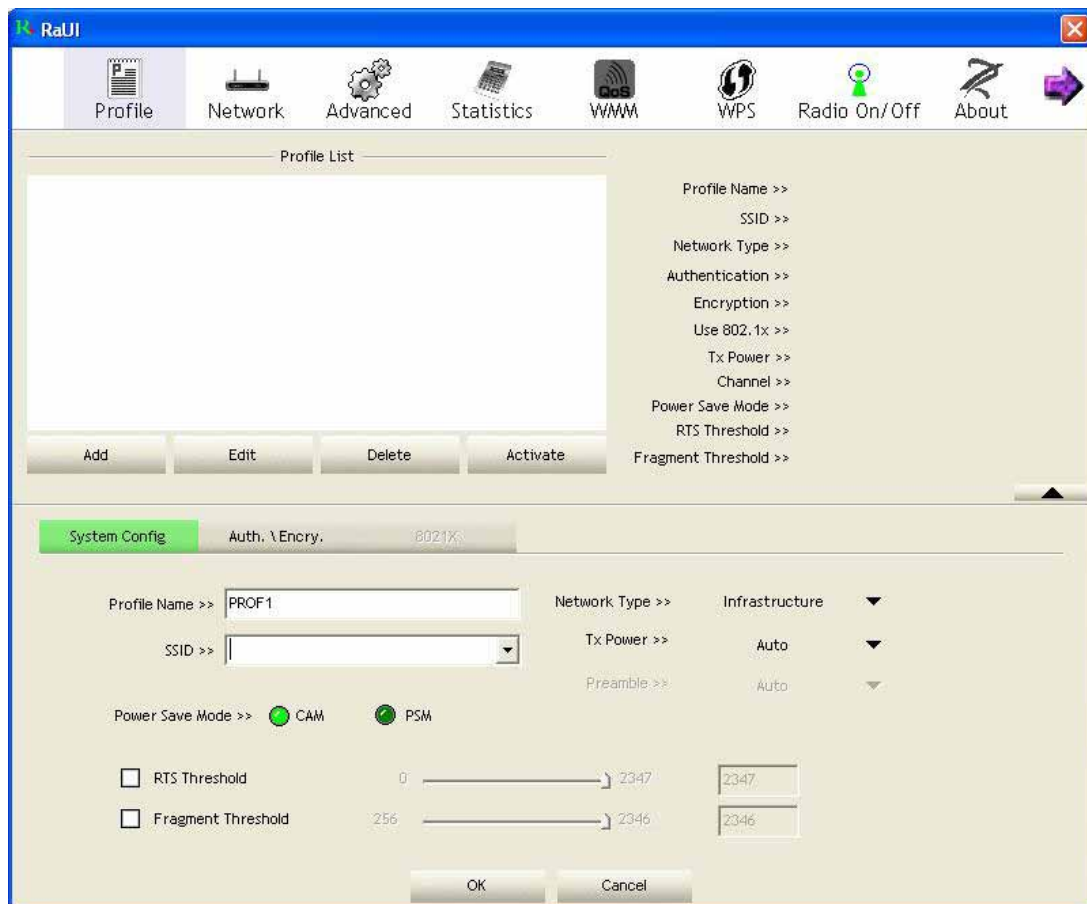
If you want to click new profile, click 'Profile' tab, then click 'Add' button:



Or, you can add a connected wireless access point or wireless device to a profile by clicking 'Site Survey' tab, then click 'Add to Profile' button:



3. And you can set the parameter for this connection here:



Profile Name:

Please give this profile a name, up to 32 alphanumeric characters and symbols are allowed, but space is not allowed.

SSID:

The SSID of the wireless access point or wireless device you selected will be displayed here. But if the SSID of access point or wireless device is not available, you have to input it here manually.

Power Saving Mode:

Please select CAM (constantly awake mode, keep the wireless radio activity when not transferring data), or PSM (Power saving mode, switches radio off when not transferring data).

It's recommended to choose 'PSM' if you're using this network card with notebook computer to help the battery live longer.

Network Type:

Select network type ('Ad Hoc' or 'Infrastructure'). If you're adding a profile from an existing access point or wireless device, it's automatically selected and you don't have to change it.

Preamble:

This option is only available when the network type is 'Ad hoc'. You can select 'Auto' or 'Long Preamble'. Please select 'Auto' if you don't know what it is.

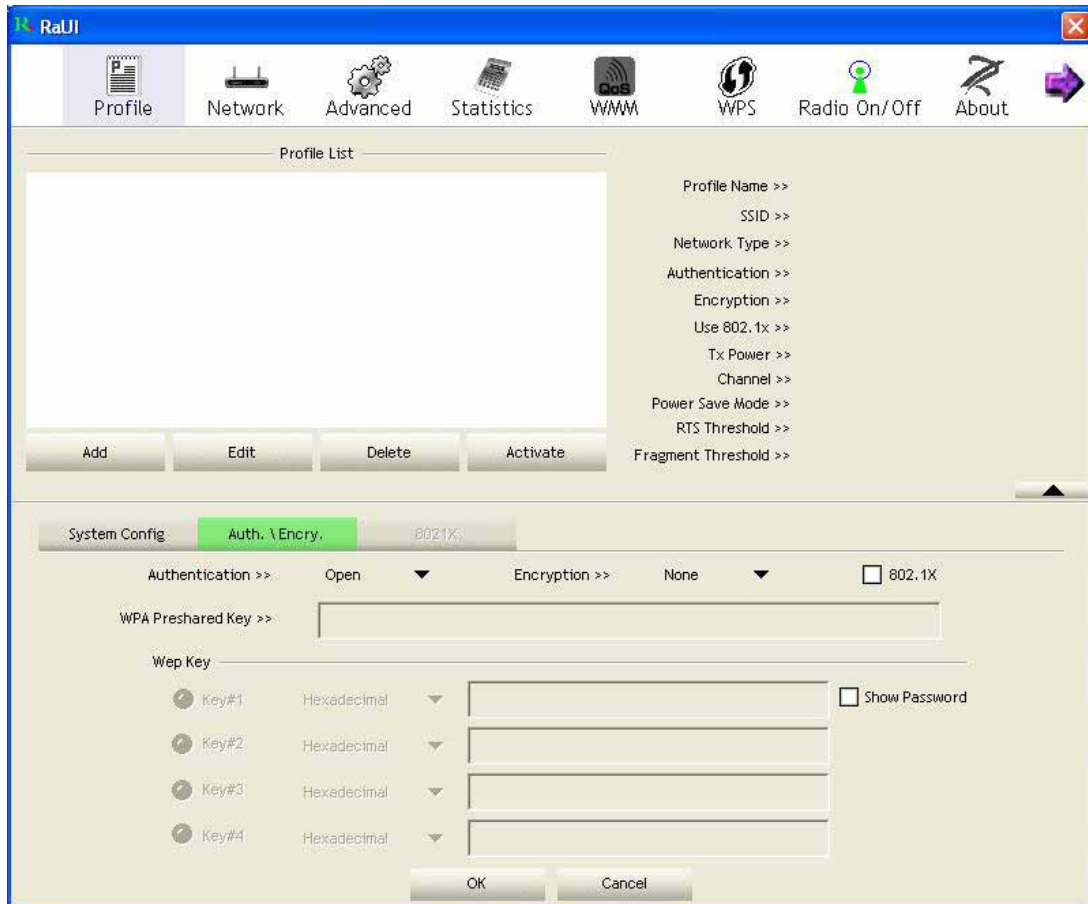
RTS Threshold:

Check the box and you can set RTS threshold manually here. Do not modify default setting unless you know what it is.

Fragment Threshold:

Check the box and you can set fragment threshold manually here. Do not modify default setting unless you know what it is.

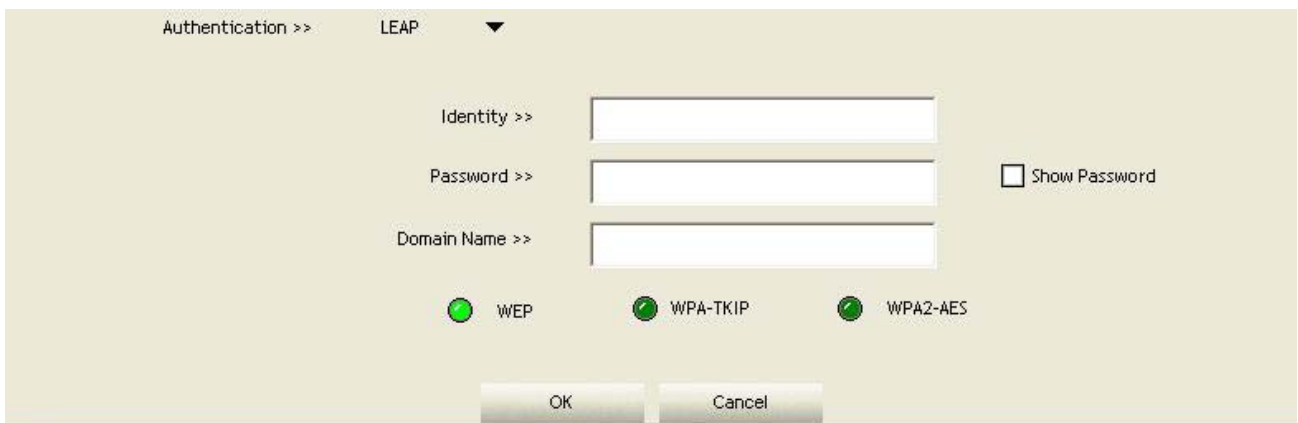
Now click 'Auth.\ Encry.' tab, and set the encryption and authentication settings.



Authentication:

Select the authentication type of the wireless access point or wireless device you wish to connect. If you're adding a profile from an existing access point or wireless device, the value will be selected automatically, and please do not modify it.

If you select 'LEAP', the following message will be displayed. Please input LEAP identity, password, domain name, and select encryption type. You can check 'Show Password' box so the password you inputted will be displayed as you type, but not replace by asterisk.



Encryption:Select the encryption type of the wireless access point or wireless device you wish to connect. If you're adding a profile from an existing access point or wireless device, the value will be selected automatically, and please do not modify it.

WPA Preshared Key:

Input WPA preshared key here. If encryption is not enabled, or you select 'WEP' as encryption type, this field will be disabled and grayed out.

WEP Key:

You can select key type (Hex or ASCII) and input WEP key here. If encryption is not enabled, or you select 'WPA' as encryption type, this field will be disabled and grayed out.

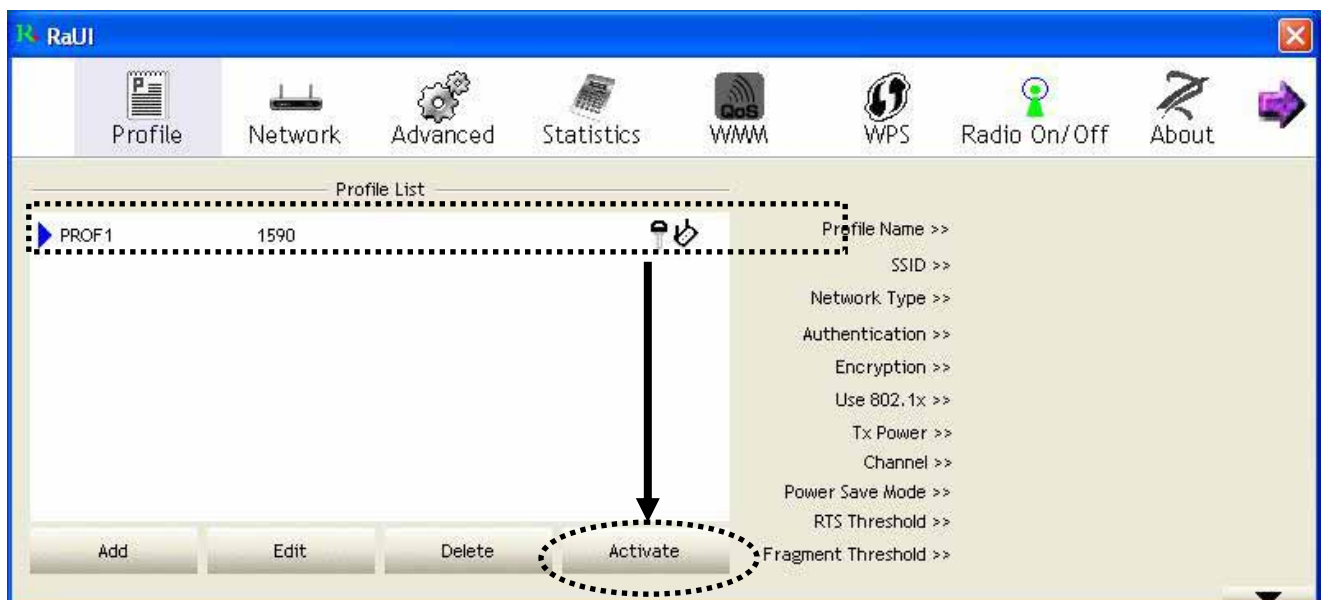
Show Password:

Check this box and all passphrases or security keys you inputted will be displayed as you type, but not replace your input with asterisk.

802.1x:

Enable 802.1x wireless authentication. Please click '802.1x Setting' button to set 802.1x parameters. (See next section).

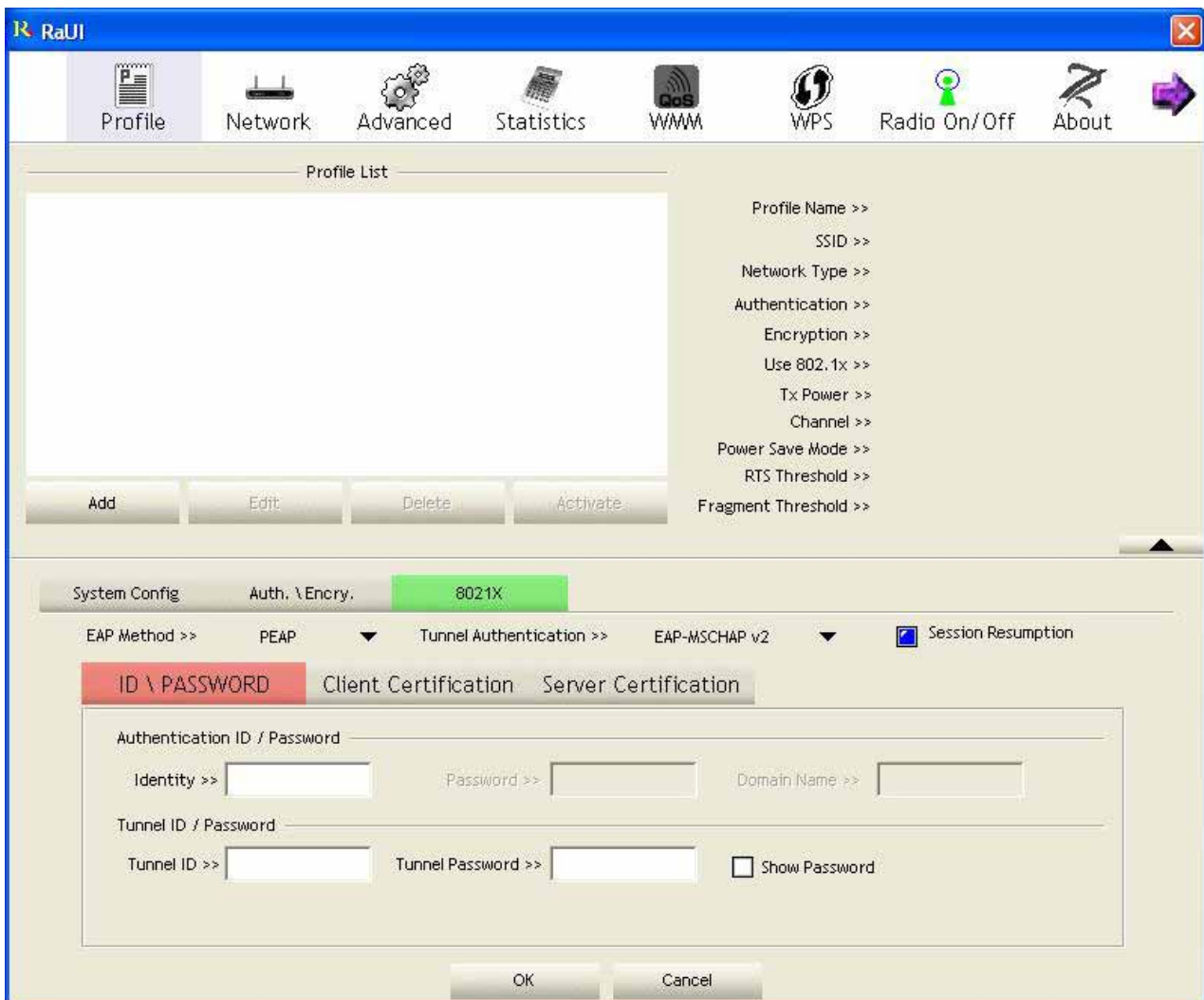
After you finish all settings, click 'OK' to save settings and exit. The profile you just created will be displayed:



Select the profile you wish to use, and click 'Activate' to use the profile you selected. If you want to change the connection parameters of a specific profile, just select it and click 'Edit' button, you'll be prompted to input the connection parameters, just like you're creating a new profile. If you no longer need a profile, select the profile then click 'Delete'.

◆ Using 802.1x – Certification

After you click '802.1x Setting', a new window will appear:



EAP Method:

Please select an 802.1x authentication type here. The type you select here must be identical to the type of the 802.1x authentication type you're using.

Session Resumption:

You can enable or disable session resumption here. If you don't know you should enable session resumption or not, please ask your 802.1x authentication administrator.

Identity:

Please input 802.1x identity here.

Password:

Please input the password of 802.1x identity here.

Domain Name:

Please input the domain name of 802.1x authentication here. This field will be grayed out when authentication type is not 'EAP-FAST'.

Client Certification:

If the authentication type you use is 'PEAP' or 'TTLS', you can use the certificate stored on your computer. If the authentication type you use is 'TLS/Smart Card', this box is always checked.

Allow unauthenticated provision mode:

This box is always checked and can not be modified.

Use protected authentication credential:

If the authentication type you use is 'EAP-FAST' you can use protected authentication credential by check this box.

Remove:

Remove the credential you imported previously.

Import:

Import the authentication credential file (PAC or al file format), you'll be prompted to select a credential file from your computer.

Tunnel Authentication:

You can select the protocol of tunneled authentication here. This pull down menu is only available when authentication type you use is 'PEAP' or 'TTLS'. When you use 'EAP-FAST' as authentication type, the protocol setting is always 'Generic Token Card' and can not be changed.

Tunnel ID:

Please input the identity of tunneled authentication

Tunnel Password:

Please input the password of tunneled authentication

Password Mode:

Please select the password mode of 'EAP-FAST' authentication mode. This setting is hidden when the authentication type is not 'EAP-FAST'.

After you finish all settings, click 'OK' to save settings and exit.

◆ Using 802.1x - CA Server

If you want to use CA server, please click 'Server Certification' tab. And the following message will be displayed:

Use certificate chain:

Check this box to enable the use of certificate chain.

Certificate Issuer:

Please select the issuer of certificate from this dropdown menu.

Allow intermediate certificates:

Check this box if you wish to allow intermediate certificates.

Server name:

Input the server name of CA server here.

Server name must match:

Check this box and the wireless configuration utility will check if the server name of CA server exactly you set here is exactly matched with the CA server connected to. If they don't match, connection will be dropped.

Domain name must end in specified name:

Check this box and the wireless configuration utility will check the end of domain name. If there's anything wrong, connection will be dropped.

After you finish all settings, click 'OK' to save settings and exit.

4.4 View Network Statistics and Link Status

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

◆ Network Statistics

Please follow the following instructions to check network statistics:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



2. Click 'Statistics' tab, and the statistics of wireless connection will be displayed:



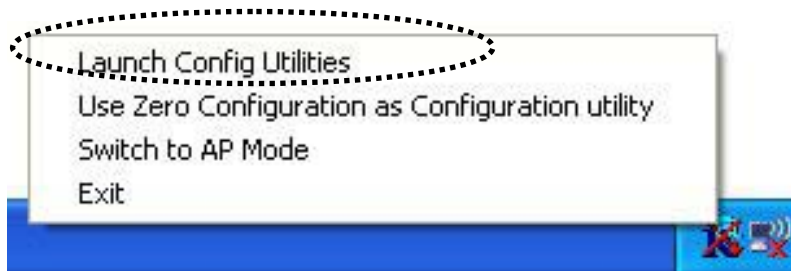
All connection-related statistics is displayed here. You can click 'Reset Counter' to reset the statistics of all items back to 0.

Click 'X' to close the window.

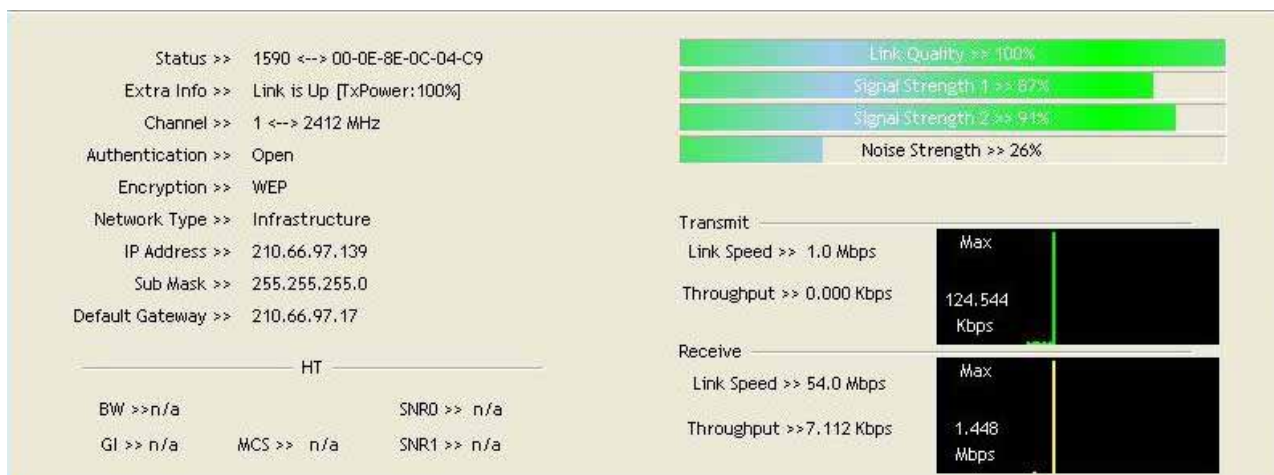
◆ Link Status

Please follow the following instructions to check network statistics:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



2. Click ' ' tab, and information about current wireless connection will be displayed:



These information displayed here are updated every second, and here are descriptions of every item:

Status:

Displays the SSID and BSSID of connected wireless access point or wireless device (displayed as SSID <-> BSSID as shown in above picture. If there's no active connection currently, 'Disconnected' will be displayed here.

Extra Info:

Displays the link status ('Link is up' or Link is down', and the radio transmitting power of your network card.

Channel:

Displays the radio channel being used now.

Link Speed:

Displays the link speed of data transmitting (Tx, in Mbps) and receiving (Rx, in Mbps). Link speed is the maximum available data transfer speed of the wireless connection, and depends on the radio signal quality of wireless connection.

Throughput:

Displays the rate of data transmitting (Tx, in Kbps) and receiving (Rx, in Kbps).

Link Quality Displays link quality (radio signal quality). When the link quality is better, the wireless link speed will be better, too. Link quality is displayed by percentage and a descriptive word (Good, normal, weak, and low).

Signal Strength 1:

Displays the radio signal strength of built-in antenna 1.

Signal Strength 2:

Displays the radio signal strength of built-in antenna 2.

Noise Level :

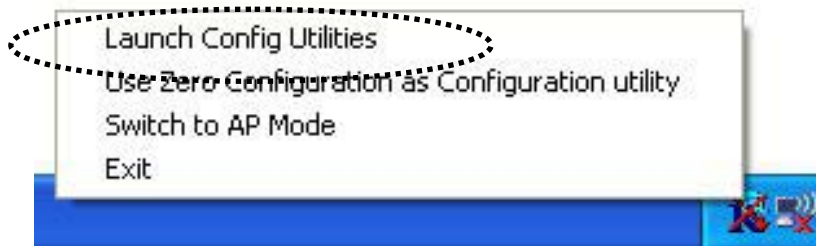
Displays the percentage or level of noise (unusable) signal. If the value of this item is high, data transfer rate will drop.

4.5 Advanced Settings

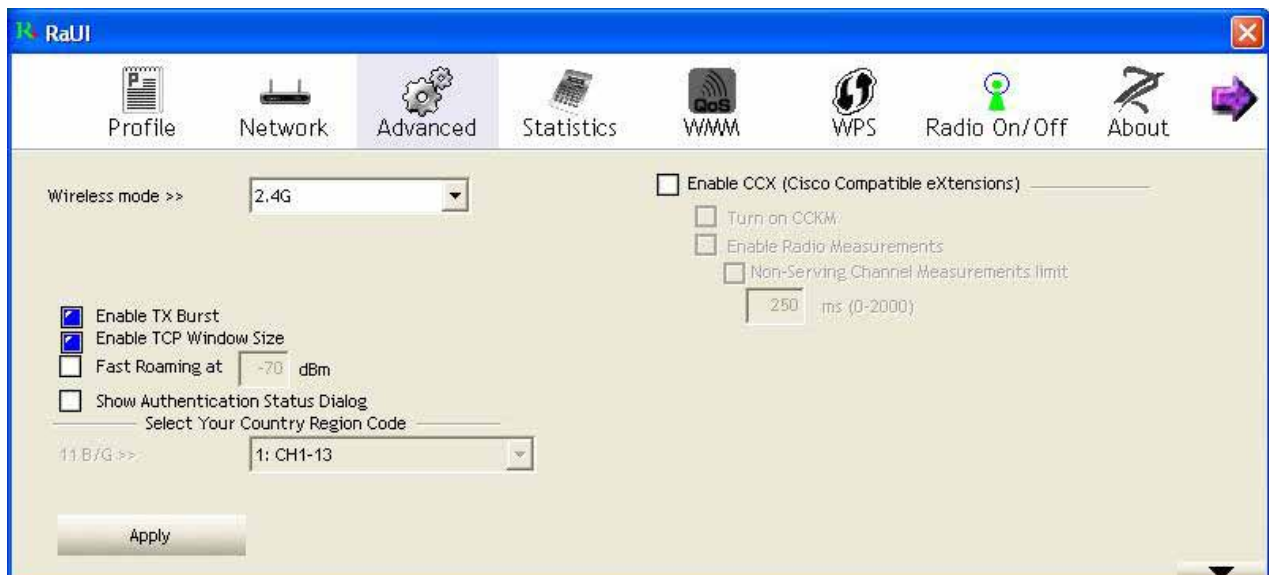
This wireless network card provides several advanced settings for experienced wireless users. You can change these settings to increase data transfer performance, or change operation mode.

Please follow the following instructions to set advanced wireless settings:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



2. Click 'Advanced' tab, and the following settings will appear:



Wireless mode:

Select wireless operation mode, available options are 802.11 B/G mix, 802.11 B only, and 802.11 B/G/N mix. You can select 802.11 B/G/N mix to maximize wireless compatibility with wireless access points and other wireless devices. Anyway, you can set this setting to '802.11 B only' when you're going to communicate with old 802.11b wireless devices and you got problem using other two modes.

TX BURST

Check this box to accelerate the data transmit rate. It may not work with all wireless access point and wireless devices.

Enable TCP Window Size:

Check this box and the configuration utility will adjust TCP window size automatically, to get better performance. It should be safe for most of wireless environments, but if you found some problem on data transfer, uncheck this box.

Fast Roaming at:

Check this box and you can adjust the threshold of when this wireless network card should switch to another wireless access point with better signal quality. Only adjust value when you understand what it means.

Show Authentication Status Dialog:

When your computer is being authenticated by wireless authentication server, a dialog window with the process of authentication will appear. This function is helpful to find out the problem when you can not be authenticated, and you can provide this information to authentication server's administrator for debugging purpose.

Enable CCX:

Enable Cisco Compatible eXtensions. CCX is a wireless feature developed by Cisco used to improve the wireless performance with CCX compatible wireless devices. Check this box if you need to connect to CCX-compatible wireless devices.

Turn on CCKM:

Check this box to enable CCKM (Cisco Centralized Key Management), which enables wireless clients to roam between CCKM-enabled access points in very short time.

Enable Radio Measurement:

When you're connecting to CCX-compatible access point, check this box to enable radio measurement function to improve wireless connectivity.

Non-Serving Channel Measurements Limit:

When you're connecting to CCX-compatible access point, check this box to enable measurement on unused radio channels to improve wireless connectivity.

Limit --- milliseconds:

Limit the time used for said measurement to a certain time. Default value is 250.

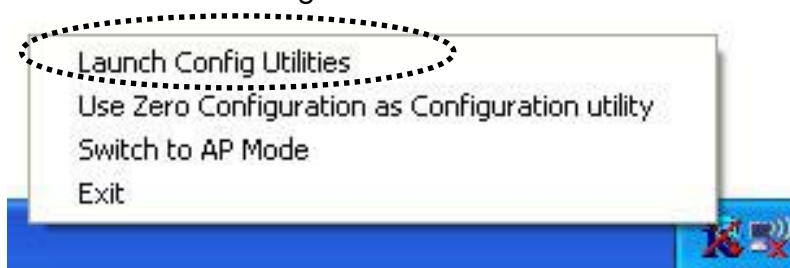
After you finish the settings, click 'Apply' to apply new settings, and click 'OK' to close configuration utility.

4.6 QoS Setting

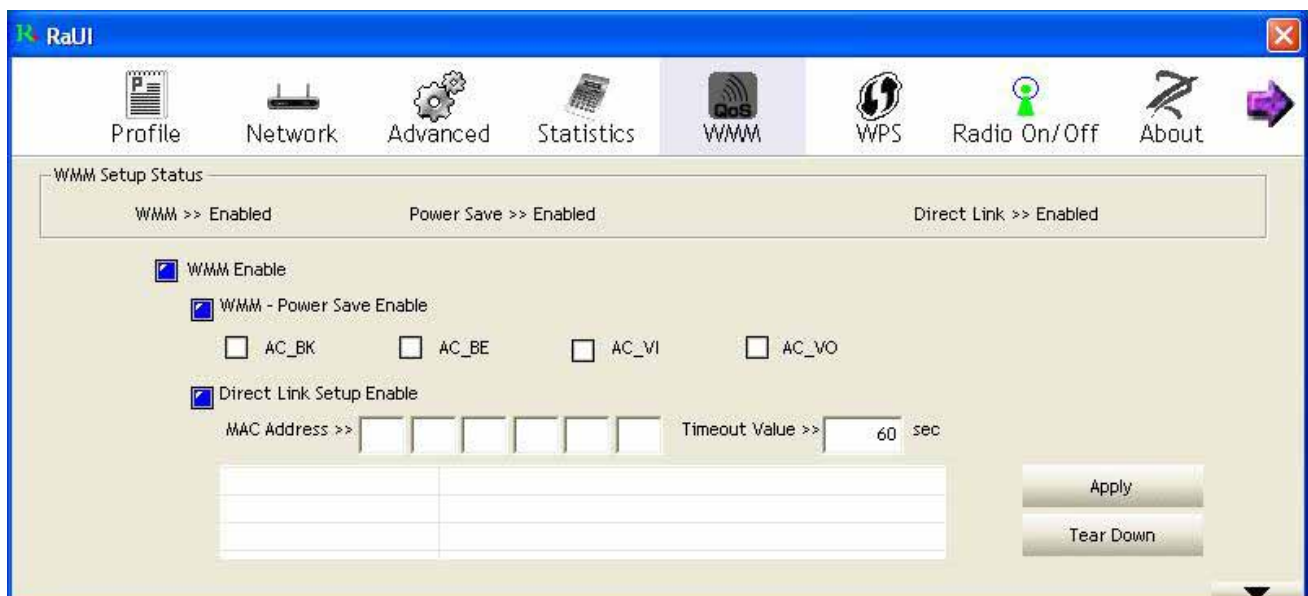
This wireless network card provides QoS (Quality of Service) function, which can improve the performance of certain network applications, like audio / video streaming, network telephony (VoIP), and others. When you enable WMM (Wi-Fi MultiMedia) function of this network card, you can define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.

Please follow the following instructions to set advanced wireless settings:

Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



Click 'QoS' tab, and the following settings will appear:



WMM Enable:

Check this box to enable WMM function. Please click 'Apply' button on the right of this check box after you check or uncheck this box, so corresponding settings in this window will be activated or deactivated respectively.

WMM – Power Save Enable:

Enable WMM power saving mode to save energy and lets your battery live longer. Click this button to select the WMM data type which will suppress the function of power saving. When this kind of data is transferring, power saving function will be disabled. Available data types are AC_BK (Background / Low Priority), AC_BE (Best Effort), AC_VI (Video First), and AC_VO (Voice First).

Direct Link Setup Enable:

Enable or disable direct link setup (DLS) function. This function will greatly improve the data transfer rate between WMM-enabled wireless devices. Please click 'Apply' button on the right of this check box after you check or uncheck this box, so corresponding settings in this window will be activated or deactivated respectively.

MAC Address:

Input the MAC address of another WMM-enabled wireless device you wish to establish a direct link here, then click 'Apply' to add this MAC address to DLS address table.

Timeout Value:

Input the timeout value of this WMM-enabled direct link wireless device. If the wireless device is not responding after this time, it will be removed from DLS table.

Tear Down:

If you want to remove a specific wireless device from DLS table, select the device and click this button to remove it.

After you finish the settings, click 'Apply' to close configuration utility.

4.7 WPS Configuration

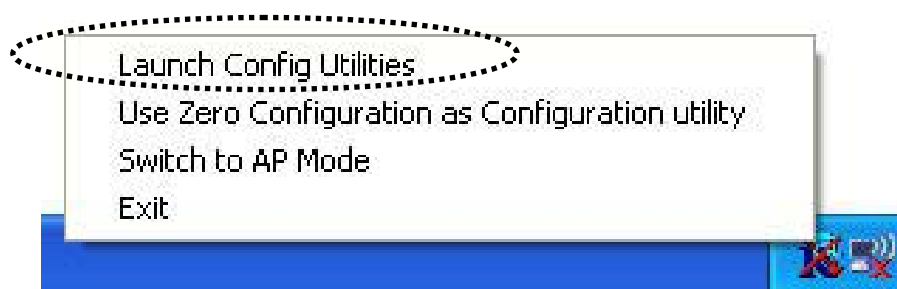
Wi-Fi Protected Setup (WPS) is the latest wireless network technology which makes wireless network setup become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption. All you have to do is go to the WPS setup page of this wireless card, click a button, and then press a specific button 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 card comes with a unique WPS pin code; you can just input the code to wireless access point, and the wireless access point and wireless network card will do the rest for you.

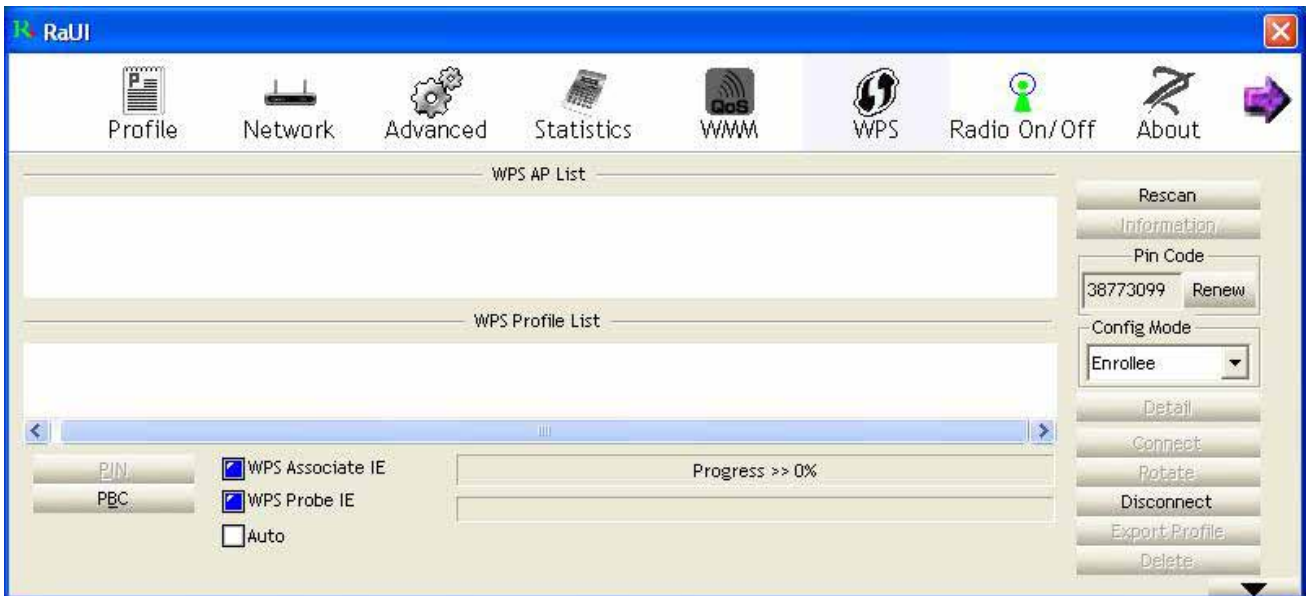
This wireless network card is compatible with WPS. To use this function, the wireless access point you wish to connect to must support WPS function too. Now, please follow the following instructions to establish secure connection between WPS-enabled wireless access point and your wireless network card:

◆ WPS Setup - PBC (Push-Button Configuration)

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



2. Click 'WPS Configuration' tab, and the following settings will appear:



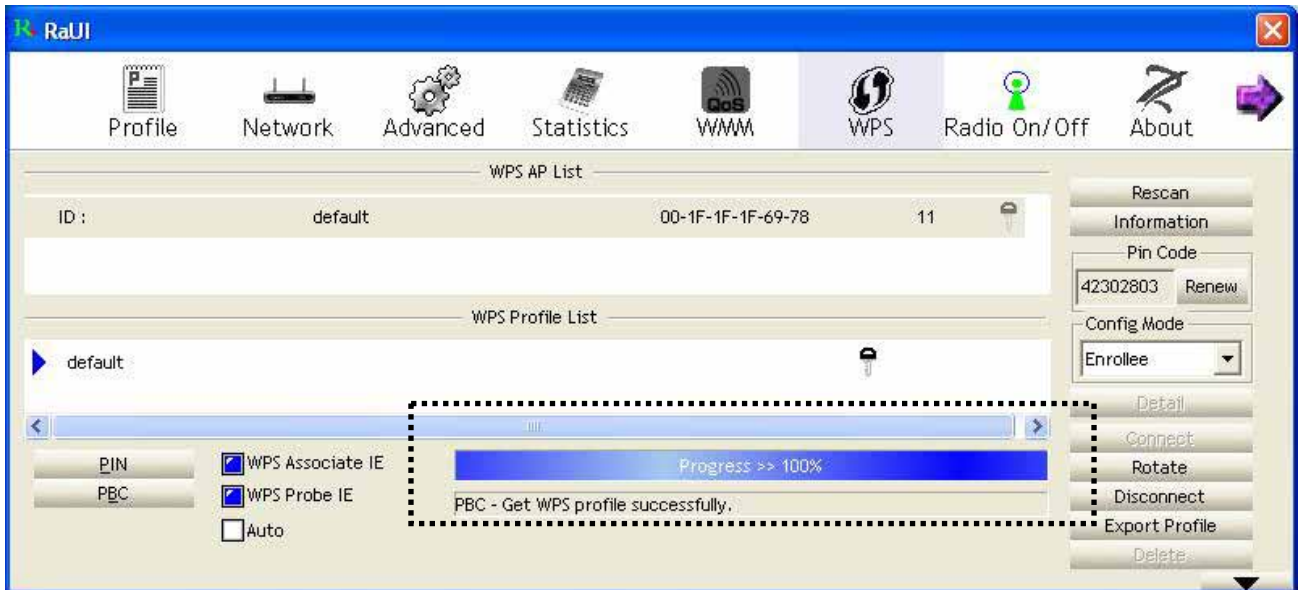
3. Set 'Config Mode' to 'Enrollee', and then push the 'WPS' button on your wireless access point (the button used to activate WPS standby mode may have another name), or use other way to start WPS standby mode as the instruction given by your wireless access point's user manual.

4. Before you start to establish the wireless connection by using WPS, you can click 'Rescan' button to search for WPS-enabled access points near you, to make sure the WPS function of your access point is activated.



All access points with WPS function enabled will be displayed. Please make sure the access point you wish to connect is displayed. If not, please click 'Rescan' few more times. You can also click 'Information' button to see the detailed information about selected access point.

5. Start PBC pairing procedure at access point side (please refer to the instruction given by your access point's manufacturer), then click 'PBC' button in wireless configuration utility to start to establish wireless connection by WPS. Please be patient (This may require several seconds to one minute to complete). When you see 'WPS status is connected successfully' message, means the connection between your wireless network card and access point is successfully connected by WPS, and the information about access point you connected to will be displayed.



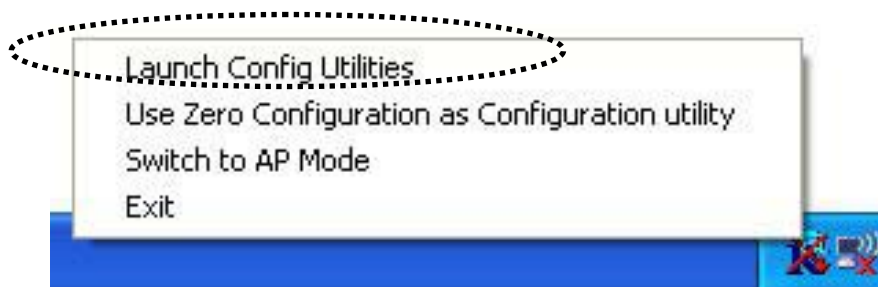
Sometime WPS may fail, and you can click 'PBC' button few more times to try again. When an access point is connected, you can click 'Disconnect' to disconnect your wireless network card from a connected access point, or select another WPS-enabled wireless access point, then click 'Connect' to establish connection to selected access point, if there are more than one WPS-enabled access point found. You can also click 'Rotate' button, and next access point on the list will be selected to establish connection.

If you want to delete a found access point from the list, select it and click 'Delete' button.

◆ WPS Setup - PIN

If the wireless access point you wish to connect supports PIN, please follow the following instructions to establish connection to it:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



2. Click 'WPS Configuration' tab, and the following settings will appear:



The PIN number of your wireless network card is an eight-digit number located at the upper-right position of configuration utility. Remember it, and input the number to your wireless access point as the WPS PIN code (Please refer to the user manual of your wireless access point for instructions about how to do this).

3. Click 'PIN' button now, and wait for few seconds to one minute. If a wireless access point with correct PIN code is found, you'll be connected to that access point:



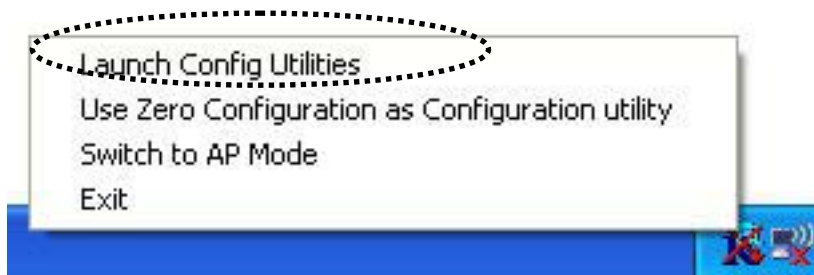
You may have to click 'PIN' for few more times to try again. If you still can not connect to access point by this way, please make sure the PIN code you provided to access point is correct.

4.8 About

The 'About' tab provides you the information about version numbers of configuration utility, firmware, and other important information about your wireless network card.

Please follow the following instructions to see these information:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.



2. Click 'About' tab, and the following settings will appear:



If you need assistance about network problem, you'll need these values. You can also click 'WWW.RALINKTECH.COM' button to go to the web site of network card driver manufacturer and get more information about your wireless network card.

Please click 'OK' to close configuration utility

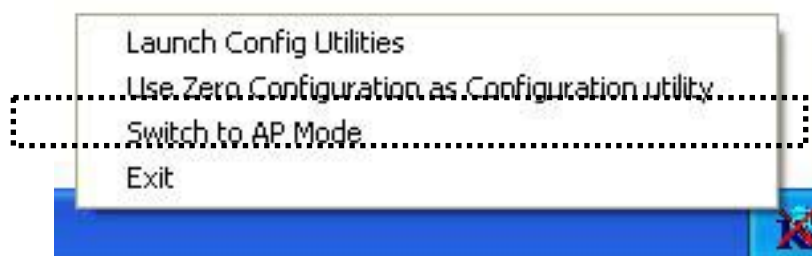
5. Soft-AP Function:

Excepting become a wireless client of other wireless access points, this wireless card can act as a wireless service provider also! You can switch this wireless card'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 card.

5.1 Switch to AP Mode and Basic Configuration

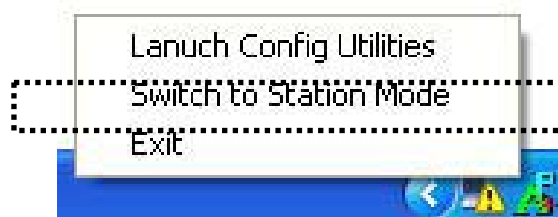
The operating mode of the wireless card is 'Station Mode' (becoming a client of other wireless access points) by default. If you want to switch to AP mode, please right-click Ralink utility icon, and select 'Switch to AP Mode'.



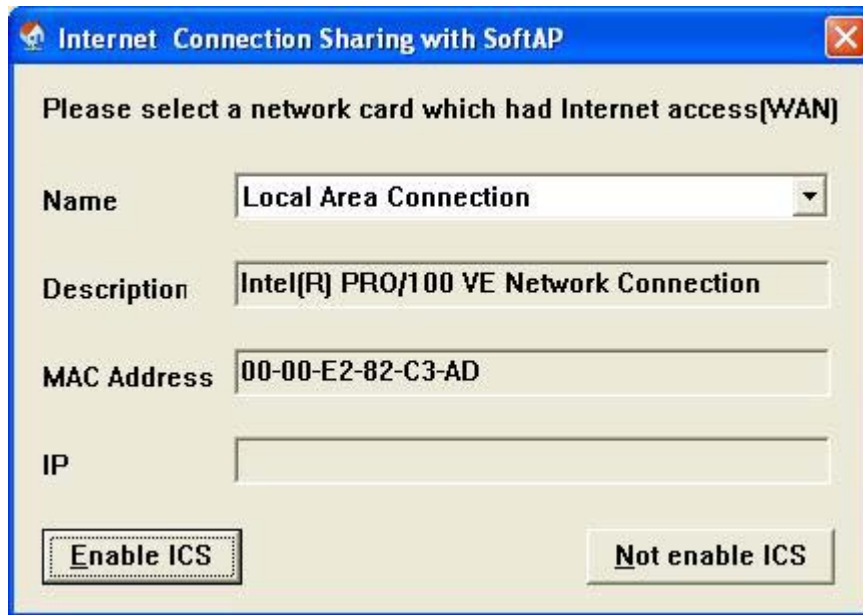
After you select 'Switch to AP Mode', the Ralink utility icon will change:



Which indicated the wireless card is operating in AP mode now. If you want to switch the wireless card back to station mode (become a client of other wireless access points), click 'Switch to Station Mode'.

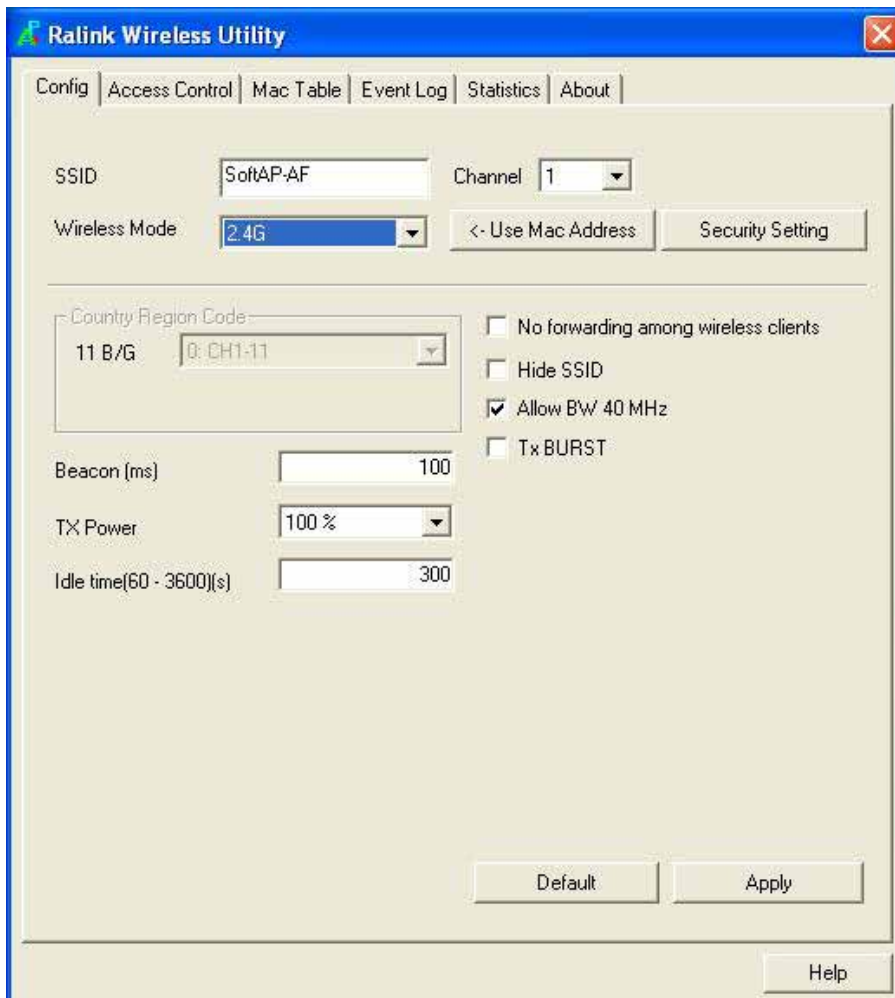


A configuration window will appear after you switch the operation mode to 'AP' or click 'Launch Config Utilities' after you right-click the Ralink configuration utility, which asks you to assign an existing network card with internet connection:



If your computer has another network card which is connected to Internet, please select it from 'Name' dropdown menu, and click 'Enable ICS'; if your computer does not have another network card with Internet connection, please click 'Not enable ICS'.

After you click 'Enable ICS' or 'Not enable ICS', you'll see the basic configuration menu of the AP function:



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.

TX Rate:

Please select the data transfer rate here. The maximum TX rate you can select here depends on the wireless mode you're using. It's safe to select 'Auto' to let wireless card select a proper TX rate according to the strength and quality of radio signal. When the wireless mode is set to '802.11 B/G/N Mix', TX Rate will be set to 'Auto' and cannot be changed.

Channel:

Please select the wireless channel you wish to use. The number of channels available here will vary depends on the setting of 'Country Region Code'.

Wireless Mode:

Please select the wireless operating mode. You can limit the type of wireless client to 802.11b or 802.11g only, or allow 802.11b/g, and 802.11b/g/n clients. It's safe to select '802.11 B/G/N mix' to allow all kinds of wireless client to connect to your computer, unless you want to limit the type of wireless client allowed to connect to your computer.

Use Mac Address:

Click this button to use the MAC address of the wireless card as SSID. A prefix of 'AP' will be added.

Security Setting:

Set the security options (wireless data encryption) Please refer to chapter 3-2 'Security Settings' for details.

Country Region Code:

Available options are 0-7, which will affect the available wireless channels you can use:

0: FCC (US, Canada, and other countries uses FCC radio communication standards)

1: ETSI (Europe)

2: SPAIN

3: FRANCE

4: MKK

5: MKKI (TELEC)

6: ISERAL (Channel 3 to 9)

7: ISERAL (Channel 5 to 13)

The operating frequency channel will be restricted to the country / region user located before importing.

Wireless Protection:

Wireless protection will prevent data collision when there are both 802.11b and 802.11g clients. You can select 'Auto' to let configuration utility to decide to use wireless protection or not. You can also select 'ON' or 'OFF' to force the use of wireless protection or not.

Beacon(ms):

You can define the time interval that a beacon signal should be send. Default value is 100. Do not modify this value unless you know what will be affected.

Idle Time:

Select the idle time of your wireless network card. Default value is 300. Do not modify this value unless you know what will be affected.

No forwarding among wireless clients:

Check this box and wireless clients will not be able to share data with each other.

Hide SSID:

Check this box and the SSID will not be broadcasted to the public. Your wireless clients must know the exact SSID to be able to connect to your computer. This option is useful to enhance security level.

Allow BW 40 MHz:

Check this box to allow BW 40MHz capability.

Default:

Click this button to restore all settings in this page back to default value.

Apply:

Click this button to activate current settings. To exit, click 'X' button at the upper-right corner of configuration window.

5.2 Security Settings

This wireless card supports wireless encryption in AP mode, which will encrypt the data being transferred over the air to enhance data security level. It's recommended to enable data encryption unless you wish to open your computer (and its internet connection) to the public.

When you click 'Security Setting' in Ralink configuration utility, the following window will appear:



Authentication Type:

Please select a wireless authentication type you wish to use. Available options are 'Open', 'Shared', 'WPA-PSK', 'WPA2-PSK', and 'WPA-PSK / WPA2-PSK'. If you want to disable wireless data encryption, you must select 'Open' or 'Shared'.

Encryption Type:

Please select an encryption mode. The available options in this setting item will vary depending on the authentication type you select. If you select 'Not Use', data will not be encrypted and people with some networking knowledge will be able to read the data you

transfer with proper tool.

NOTE: WPA encryption is safer than WEP, however, some older wireless clients don't support WPA encryption.

WPA Pre-shared Key:

Please input the WPA pre-shared key here. Only clients with the same pre-shared key you inputted here will be able to connect to your computer. This setting is only available when you select one of WPA encryptions.

Group Rekey Interval:

You can specify the time interval to re-issue the key to your wireless clients here. You can click the button '10 seconds' or 'Kpackets' to change the unit of time interval. (every 10 seconds or a thousand data packets times the value you specified in 'Group Rekey Interval' field)

Wep Key #1 ~ #4:

Please input the WEP encryption key here when you select 'WEP' as encryption type.

There are 2 types of WEP key: Hex (number 0 to 9, and ASCII characters A to F) and ASCII (all alphanumerical characters plus symbols). Please select the type of WEP key first, and then input the WEP key according to the type of WEP key you selected.

If you want to use WEP 64 bits encryption, please input 10 characters if you select HEX, or input 5 characters if you select ASCII; If you want to use WEP 128bits encryption, please input 26 characters if you select HEX, or input 13 characters if you select ASCII. 128 bits encryption is safer then 64 bits, but the data transfer speed will be slightly reduced.

Show Password:

Check this box and the WPA pre-shared key orWEP key you inputted will be shown, but not replaced by asterisk (*).

OK:

Click this button to save changes you made in this page.

Cancel:

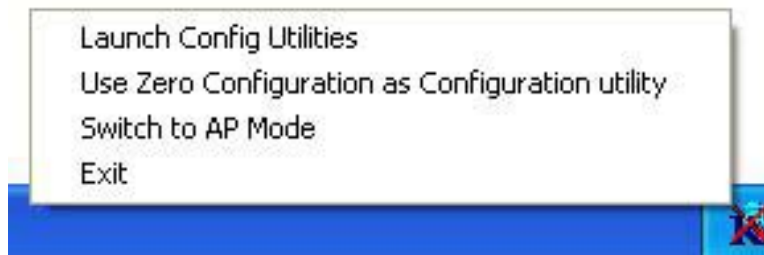
Click this button to discard all changes you made in this window.

5.3 Access Control

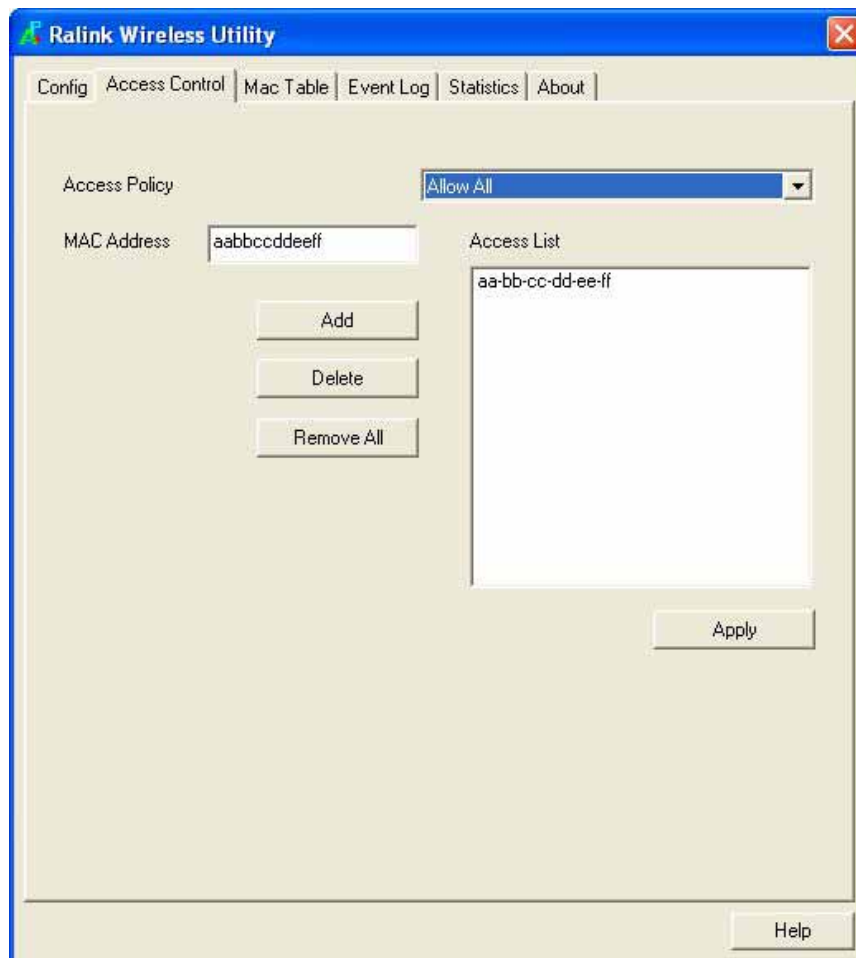
If you're not going to open your computer and wireless resources to the public, you can use MAC address filtering function to enforce your access control policy, so only wireless clients with MAC address you defined by this function can be connected to your software access point.

Please follow the following instructions to set access control based on MAC address:

1.Right-Click Ralink configuration utility icon, and select 'Launch Config Utilities'



2. Click 'Access Control' tab, and the following messages will appear:



Access Policy:

Select the policy type of your access rule:

Disable: Allow any wireless client with proper authentication settings to connect to this access point.

Allow All: Only allow wireless clients with MAC address listed here to connect to this access point.

Reject All: Reject wireless clients with MAC address listed here to be connected to this access point.

MAC address:

Input the MAC address of the wireless client you wish to allow or reject here. No colon (:) or hyphen (-) required.

Add:

Add the MAC address you inputted in 'MAC address' field to the list.

Delete:

Please select a MAC address from the list, then click 'Delete' button to remove it.

Remove All :

Delete all MAC addresses in the list.

Apply:

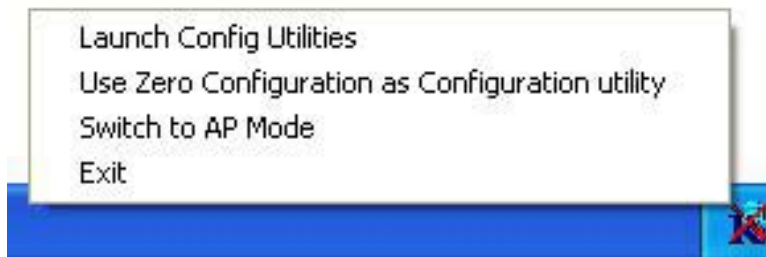
Save and apply changes you made.

Displays additional information of this wireless Connection, like current wireless operating mode and data transfer rate.

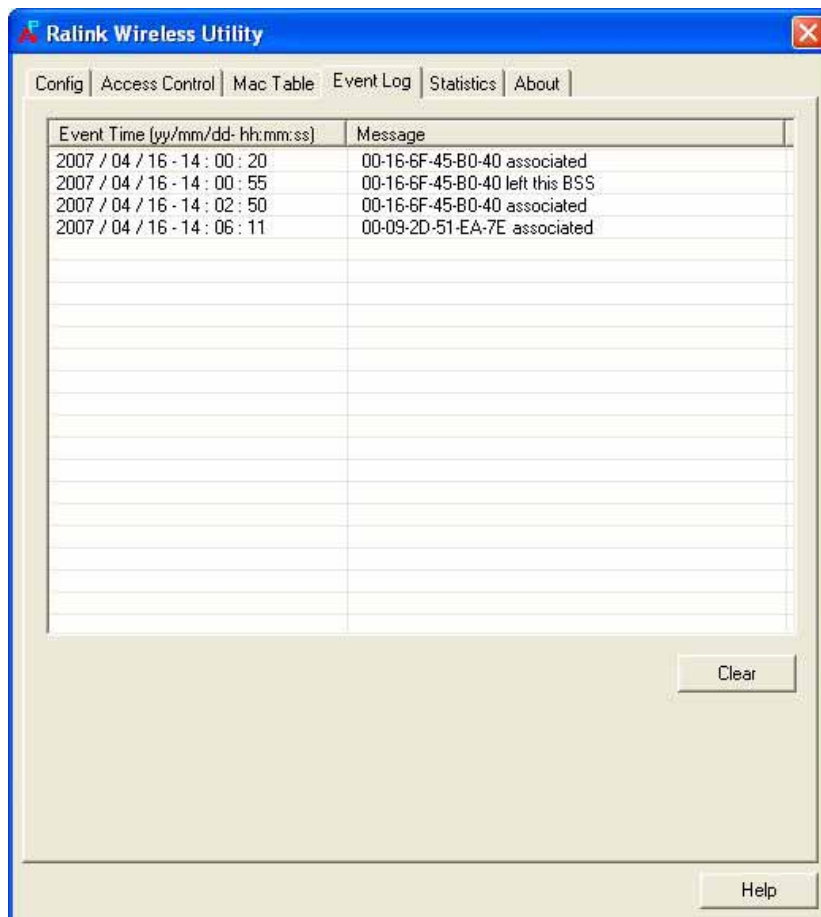
5.5 Event Log

This software access point will log all wireless-related activities as a log. You can follow the following instructions to view the content of the event log:

1. Right-Click Ralink configuration utility icon, and select 'Launch Config Utilities'



2. Click 'Event Log' tab, and the event log will be displayed:

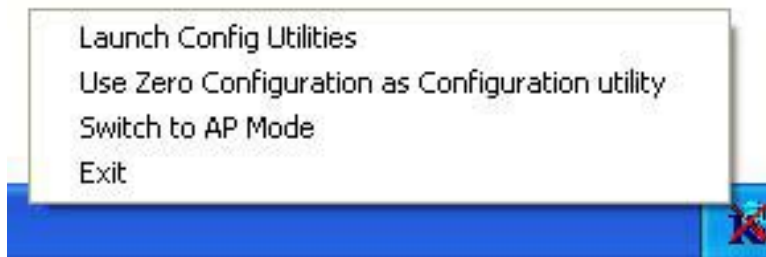


You can click 'Clear' to remove all entries in the log.

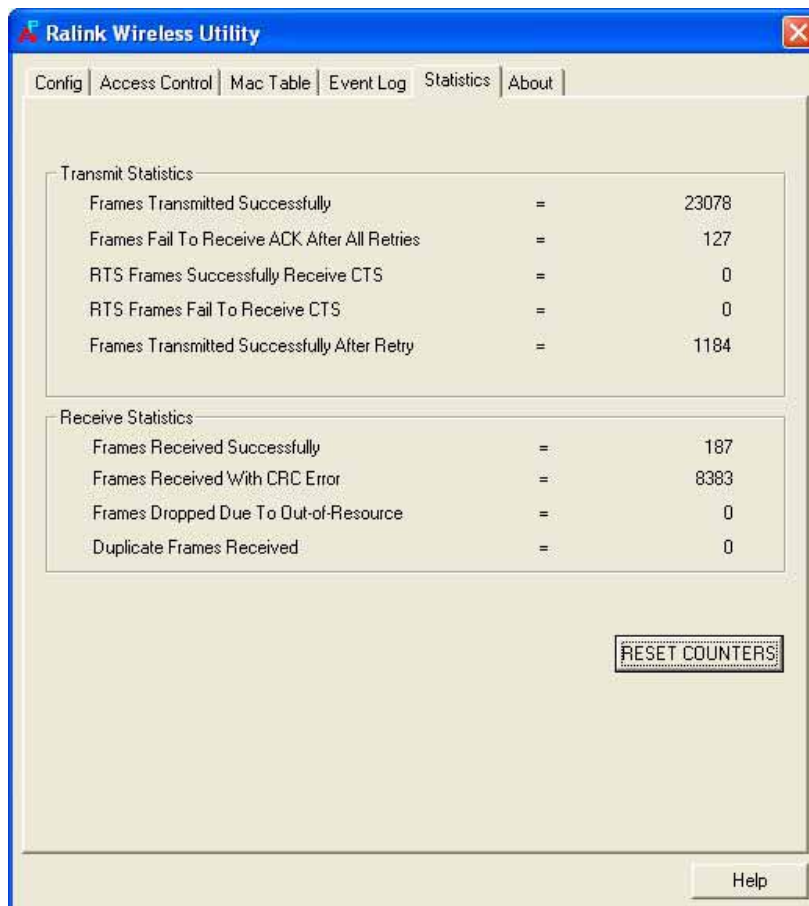
5.6 Statistics

If you want to know detailed information about how your software access point works, you can follow the following instructions to view the statistics of the access point:

1. Right-Click Ralink configuration utility icon, and select 'Launch Config Utilities'



3. Click 'Statistics' tab, and the event log will be displayed:



You can click 'RESET COUNTERS' button to reset all counters to zero.

6. APPENDIX:

6.1 Hardware Specification

Standards: IEEE 802.11b/g/Draft-N

Interface: USB 2.0 (USB 1.1 Compatible)

Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)

Data Rate: 11b: 1/2/5.5/11Mbps

11g: 6/9/12/24/36/48/54Mbps

11n (20MHz): MCS0-15, 32 with Half Guard Interval Support (up to 144Mbps)

11n (40MHz): MCS0-15, 32 with Half Guard Interval Support (up to 300Mbps)

Securities: WEP 64/128, WPA, WPA2

Cisco CCX Support

Antenna: Internal 2 Antennas with One TX and Two RX

Drivers: Windows 2000/XP/2003/Vista Server

LEDs: Link/Activity

Temperature: 32~131°F (0 ~ 55°C)

Humidity: 10-95% (NonCondensing)

Certification: FCC, CE

6.2 Troubleshooting

If you encounter any problem when you're using this wireless network card, 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!

1. I can't find any wireless access point / wireless device in 'Site Survey' function.

Answer:

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 card (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.

4. Nothing happens when I click 'Launch config utilities'

Answer:

1. Please make sure the wireless network card is inserted into your computer's USB port. If the Ralink configuration utility's icon is black, the network card is not detected by your computer.
2. Reboot the computer and try again.
3. Remove the card and insert it into another USB port.
4. Remove the driver and re-install.
5. Contact the dealer of purchase for help.

5. I can not establish connection with a certain wireless access point

Answer:

1. Click 'Connect' for few more times.
2. If the SSID of access point you wish to 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 cards with specific MAC address to establish connection. Please go to 'About' tab and write the value of 'Phy_Address' down, then present this value to the owner of access point so he / she can add the MAC address of your network card to his / her access point's list.

6. The network is slow / having problem when transferring large files

Answer:

1. Move closer to the place where access point is located.
2. Enable 'Wireless Protection' in 'Advanced' tab.
3. Try a lower TX Rate in 'Advanced' tab.
4. Disable 'Tx Burst' in 'Advanced' tab.
5. Enable 'WMM' in 'QoS' tab if you need to use multimedia / telephony related applications.
6. Disable 'WMM – Power Save Enable' in 'QoS' tab.
7. 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.

6.3 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 card, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure?

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

6. What is BSS ID?

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

7. What is WEP?

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

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

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

10. Can Wireless products support printer sharing?

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

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

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

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

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

13. What is Spread Spectrum?

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

14. What is WMM?

Wi-Fi Multimedia (WMM), a group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different

latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

15. What is WMM Power Save?

WMM Power Save is a set of features for Wi-Fi networks that increase the efficiency and flexibility of data transmission in order to conserve power. WMM Power Save has been optimized for mobile devices running latency-sensitive applications such as voice, audio, or video, but can benefit any Wi-Fi device. WMM Power Save uses mechanisms included in the IEEE 802.11e standard and is an enhancement of IEEE 802.11 legacy power save. With WMM Power Save, the same amount of data can be transmitted in a shorter time while allowing the Wi-Fi device to remain longer in a low-power “dozing” state.

16. What is GI?

GI stands for Guard Interval. It's a measure to protect wireless devices from cross-interference. If there are two wireless devices using the same or near channel, and they are close enough, radio interference will occur and reduce the radio resource usability.

17. What is STBC?

STBC stands for Space-Time Block Coding, which is a technique used to transfer multiple copies of data by multiple antenna, to improve data transfer performance. By using multiple antennas, not only data transfer rate is improved, but also the wireless stability.

18. 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.

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 generate, 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 EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C.

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

The WUBR-502GN(FCC ID: RYK-WUBR502GN) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

EC Declaration of Conformity

Name applicant:

8F., No.257, Sec. 2, Tiding Blvd., Neihu District, Taipei City 11493, Taiwan (R.O.C.)

Hereby declares under sole responsibility that product

Brand name:

SparkLAN

Product number:

WUBR-502GN

Product description:

Wireless-GN USB Dongle

To which this declaration relates complies with the requirements of the following standards:

EN 60950-1: 2001+A11:2004

EN 301 489-1 V1.6.1 (2005-09)

EN 301 489-17 V1.2.1 (2002-08)

EN 50371 (2002)

EN 300 328 V1.7.1 (2006-10)

This certifies that the designated product as described above complies with the directives described above and carries the CE marking accordingly.

This declaration has been signed under responsibility of the manufacturer / importer.

Test laboratory: Advanced Data Technology Corporation

Lab Address: No. 47, 14th Ling, Chia Pau Tsuen, Linko Hsiang 244, Taipei Hsien, Taiwan.
ROC

Name manufacturer / importer:

Sparklan Communications, Inc.

Aug 31 ,2008

Mike Chen



President

Product article code:

WUBR-502GN

Product description:

Wireless-GN USB Dongle

Product manufacturer / importer:

Sparklan Communications, Inc.

Countries in which the product as described above may be used freely:

Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland & UK.

Countries where usage of the product as described above is prohibited:

None.

Countries where usage of the product as described below is limited:

France: The use of other channels than the channels 10 through 13 is prohibited by law.