Chung Nam Electronics (CNE)
IEEE 802.11b/g/Draft-N Mini PCI WLAN Card
(Model #: WLC-123NR)
Version 0.1
User Manual

April 2008

Table of Contents

Chapter 1: Introduction

1-1 Introduction

The CNE 802.11b/g/Draft-N WLAN Card is a complete wireless high speed Network Interface Card (NIC). It conforms to the IEEE 802.11b/g standard, this wireless network card is also 802.11 Draft-N compatible-data transfer rate 300Mbps, and that's six times faster than 802.11g wireless network! This wireless network card also supports MIMO (Multi-In, Multi-Out) technology, which uses two different radio channels to enhance data transfer rate and wireless coverage and operates in the 2.45GHz ISM frequency bands.

Model: WLC-123NR

Other features of this wireless network card

- QoS function : control the bandwidth required for different application
- 802.11b/g/Draft-N compatible
- Support major encryption methods like WEP, WPA, and WPA2 encryption.
- Mini PCI interface
- Wireless access control – prevent unauthorized network access to your network and computer.

Chapter 2: Installation Procedure

2.1 Installing the software drivers on MS Windows platform

The driver installation procedure on MS Windows platform is described as follows. Windows XP is used as the example. It is similar in other Windows platform (e.g. Windows 2000).

1. Make sure that the miniPCI card has been inserted in your machine properly.

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

3. Insert device driver CDROM into the CD/DVD ROM drive of your computer, and execute 'Setup.exe' program in 'Driver' folder. Please read the end user license agreement and click 'Yes' to accept license agreement.

4. 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'.

5. There are two wireless performance mode you can select here:

   Optimize for WiFi mode   or
   Optimize for performance mode

   If you want to enhance wireless performance, please select 'Optimize for performance mode'. However, wireless compatibility is not guaranteed in this mode. If you want to use this mode, you may not be able to communicate with older wireless devices and wireless access point, such as 802.11b devices, but the data transfer rate will be enhanced in this mode. You can select this mode when you only plan to communicate with 802.11 Draft-N devices.

   If you want to keep compatibility and communicate with older wireless devices, please select 'Optimize for WiFi Mode'.
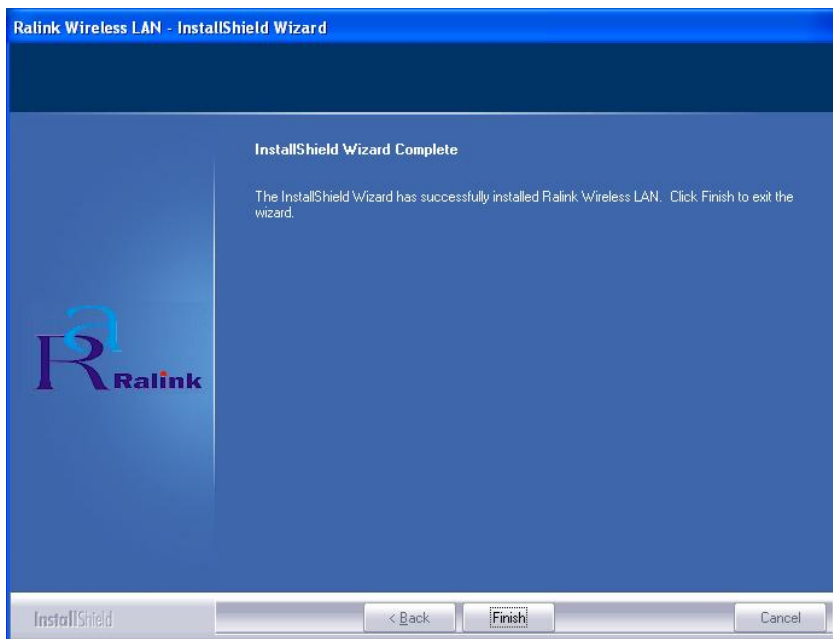
When you select one mode, please click 'Next' to continue. **If you see 'Found New Hardware' message again, please ignore it and wait.**
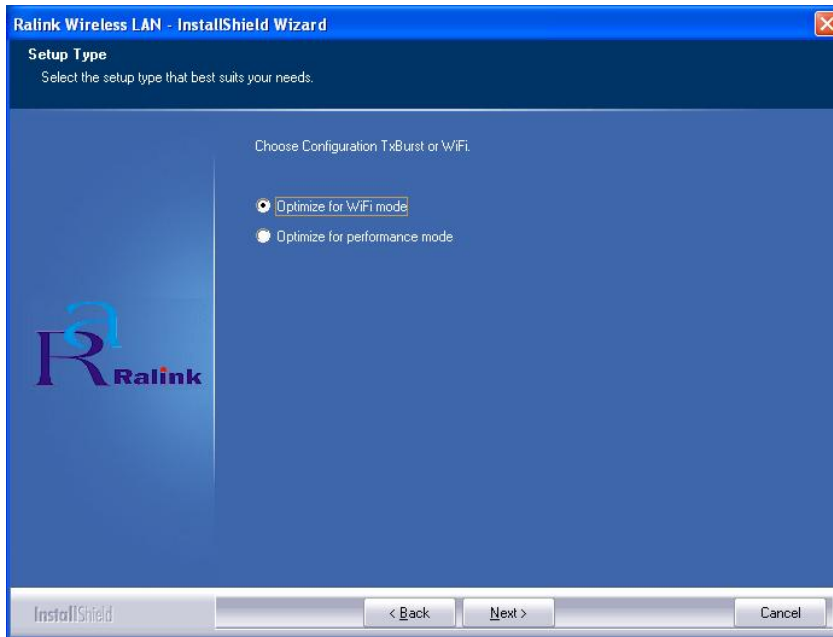
6. Please wait while the install procedure is running. When you see this message, please click 'Finish' to complete the driver installation process.

7. A new icon will appear at lower-right corner of your computer desktop, you can put the mouse cursor on the icon, and the status of wireless card will be displayed as a popup balloon.

HERE!

When you want to configure your wireless connection, please right click on this icon, and a popup menu will appear. You can click 'Launch Config Utilities' to start configuration program.

If you want to close configuration utility, please click 'Exit'.
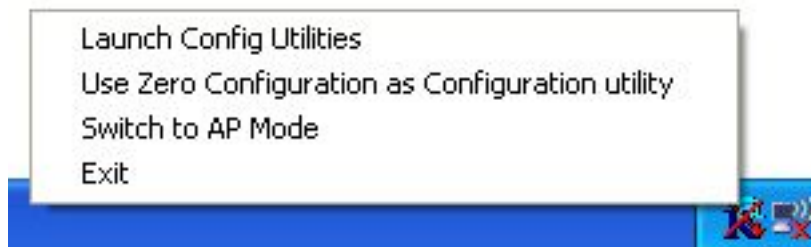
Please note that if you stopped config utility by 'Exit' function, you'll not be able to maintain the wireless link to the access point you wish to use. In this case, you can start config utility again by clicking 'Ralink Wireless Utility' icon from 'Start' -> 'All Programs' -> 'Ralink Wireless', as shown below.
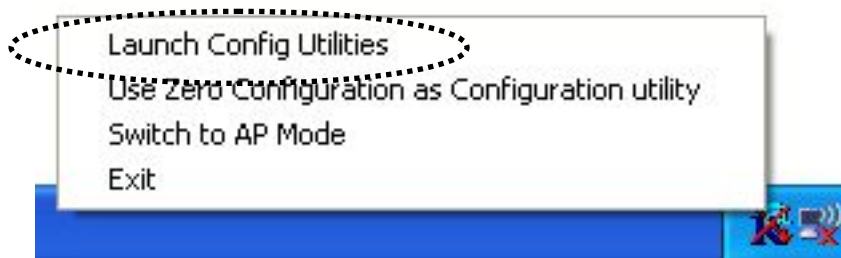
2-2 Connect to Wireless Access Point

After the driver is correctly installed, it will try to connect to any
unencrypted wireless access point automatically. If you want to connect
to a specific wireless access point, or the access point you wish to connect
uses encryption, you have to configure the wireless network card and
input required parameters, to get connected to the wireless access point
you wish to connect.

There are two ways you can configure your wireless network card to
connect to wireless access point: using the Ralink configuration utility
which comes with wireless card driver, and using built-in windows zero
configuration utility.

2-2-1   Using Ralink Utility

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

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

2. 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.

If you still can not see the access point you wish to use after clicking 'Rescan' for more than five times, please move your computer closer to the location where the wireless access point is, or see instructions in chapter 4-2 'Troubleshooting'.
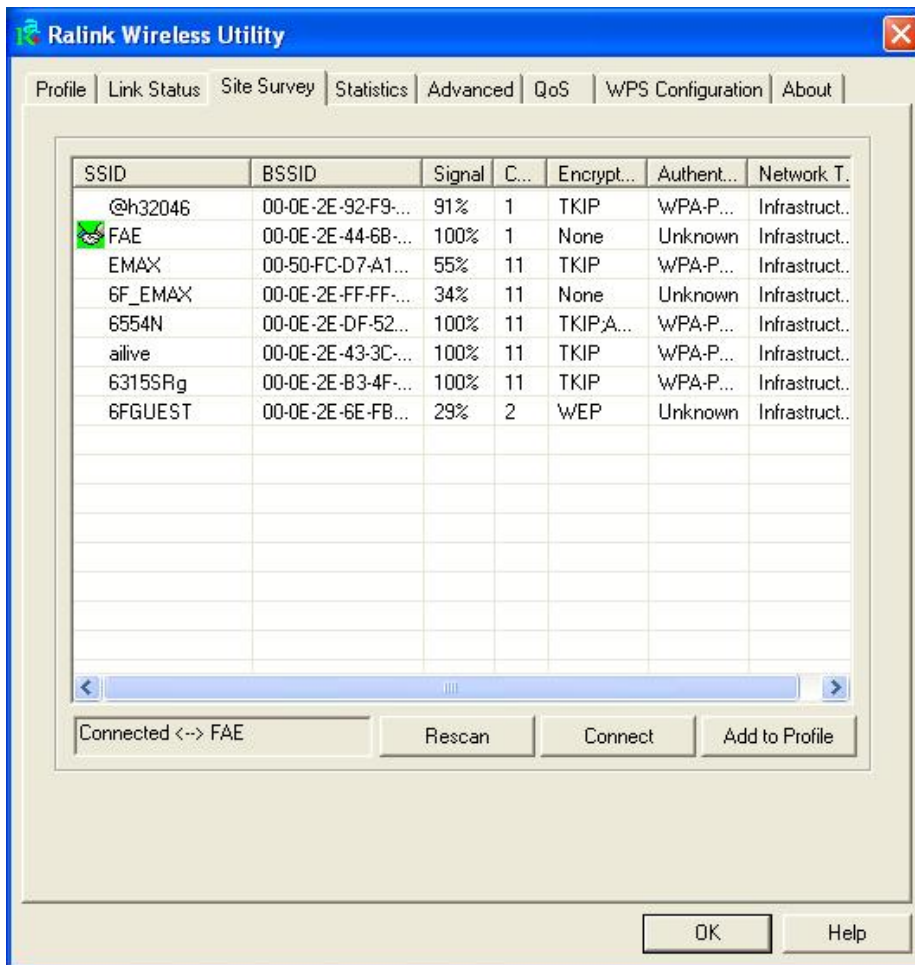
Here are descriptions of every setup item:

SSID: *The Service Set IDentifier of wireless access point or other network device. You can think it as the name of access point of wireless device.*

BSSID: *The MAC address of wireless access point or other network device. Unlike SSID, BSSID of every access*

point or network device is unique, and will not be the same with others. So you can identify a single access point or wireless device from others by BSSID, if they all have the same SSID.

Signal: *Shows the signal strength of access point or wireless device. Larger number means better radio strength, which often means you're not too far from that access point or wireless device.*

Channel: *Shows the channel number that access point or wireless device uses.*

Encryption: *Shows the encryption method that access point or wireless device uses. If the wireless access point does not enable encryption, you'll see 'None' displayed here.*

Authentication: *Shows the authentication mode that access point or wireless device uses. If the wireless access point does not require authentication, you'll see 'Unknown' displayed here.*

Network Type: *Shows the type of wireless connection. If it's a wireless access point, 'Infrastructure' will be displayed here; if it's a computer or network device, 'AdHoc' will be displayed here.*


Tips:
Wireless access point (Infrastructure) is a network device which acts as a bridge, to let wired and wireless network devices communicate with each other.

AdHoc is another connection type. A computer or network device can establish a direct wireless link with other computer or network device directly, without the help of wireless access point.

3. Click the wireless access point or network device you wish to connect, it will be highlighted, then click 'Connect'.
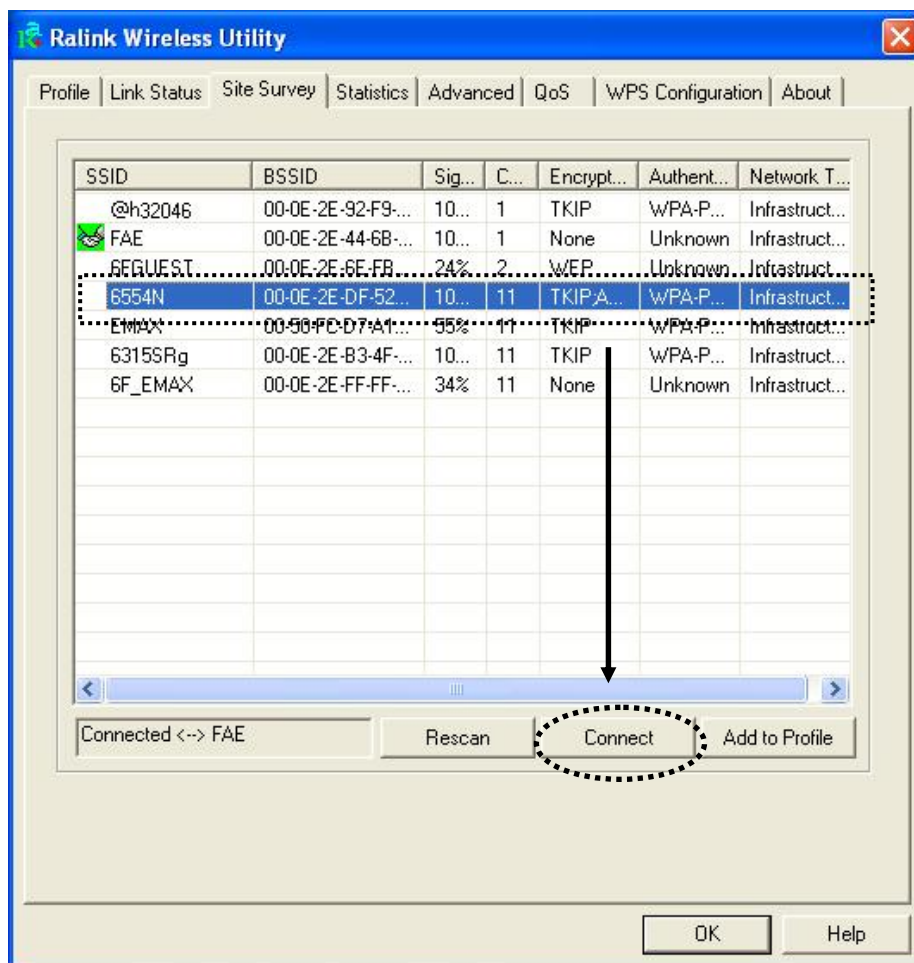
If the access point you selected does not enable encryption (The content of 'Encryption' field of the access point you selected is 'None', you'll be connected to this wireless access point within one minute. Please jump to step 6.

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

4. 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.
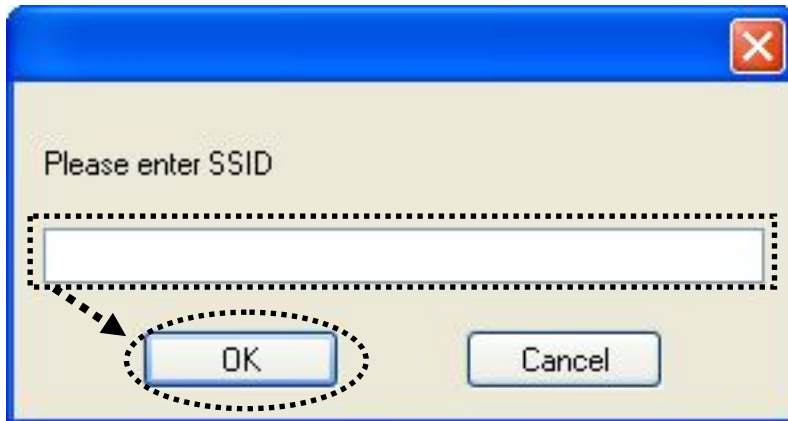
5. If the wireless access point uses encryption, you have to input WEP passphrase or WPA preshared key. Please ask the owner of the wireless access point you want to connect, and input the correct passphrase / preshared key here, then click 'OK'. If the value you inputted here is wrong, you will not 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.

6. You'll see 'Connected <-> SSID' ('SSID' is the SSID 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!
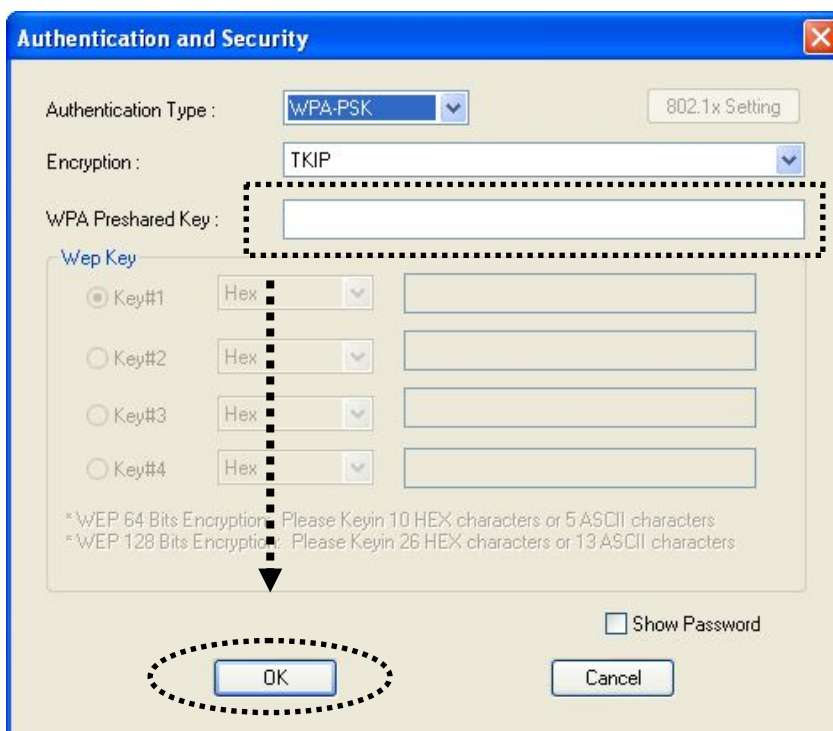
2-2-2 Using Windows Zero Configuration

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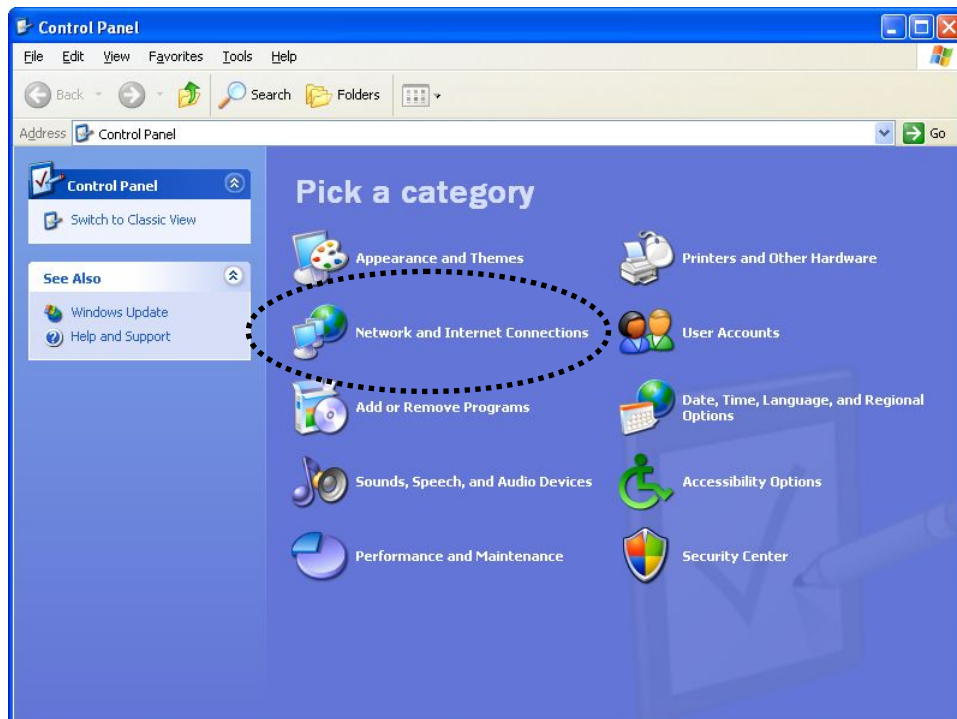
3. Click 'Connect to a network' under 'Network Connections'
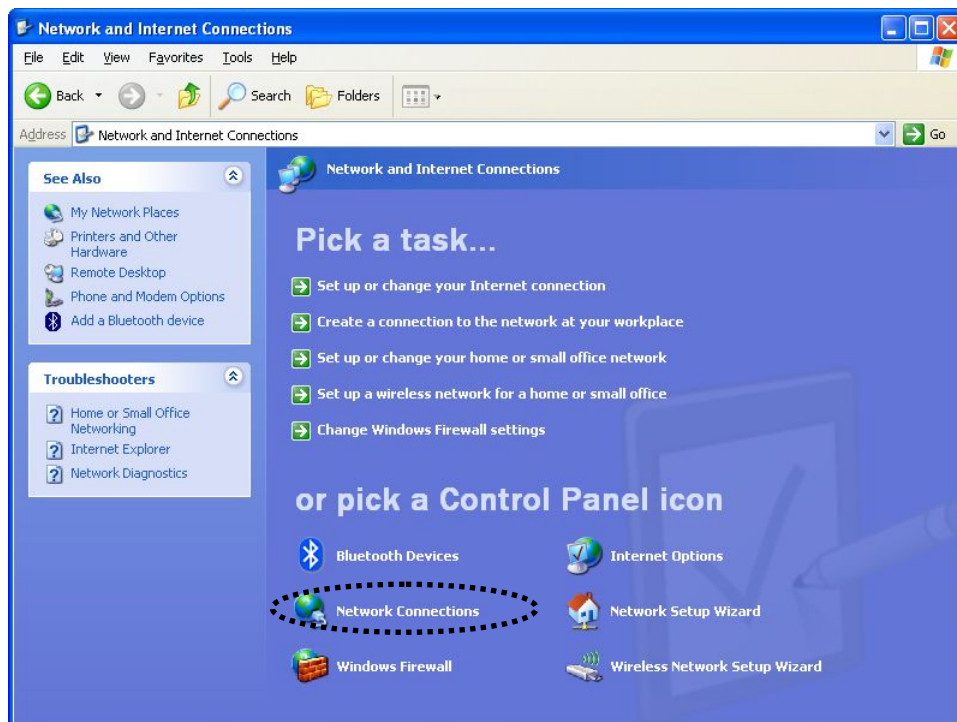
4. Right-click 'Wireless Network Connection' (it may have a number as suffix if you have more than one wireless network card, please make sure you right-click the 'Ralink 802.11n Wireless LAN Card), then select 'View Available Wireless Networks'.

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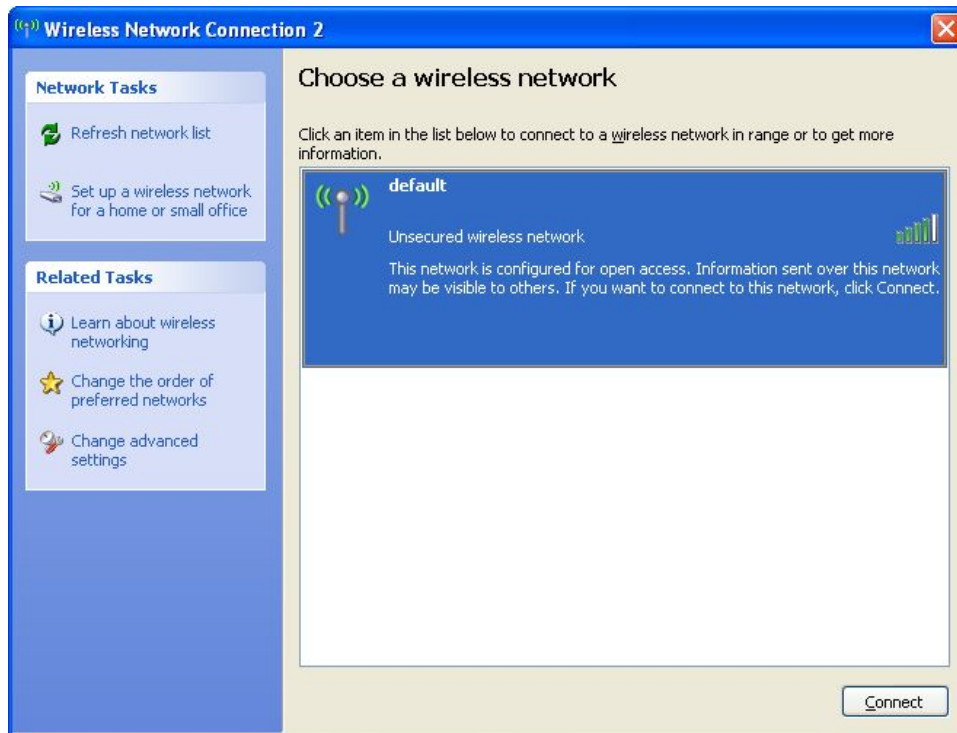
6. If the access point is protected by encryption, you have to input its security key or passphrase here. It must match the encryption setting on the access point.

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.
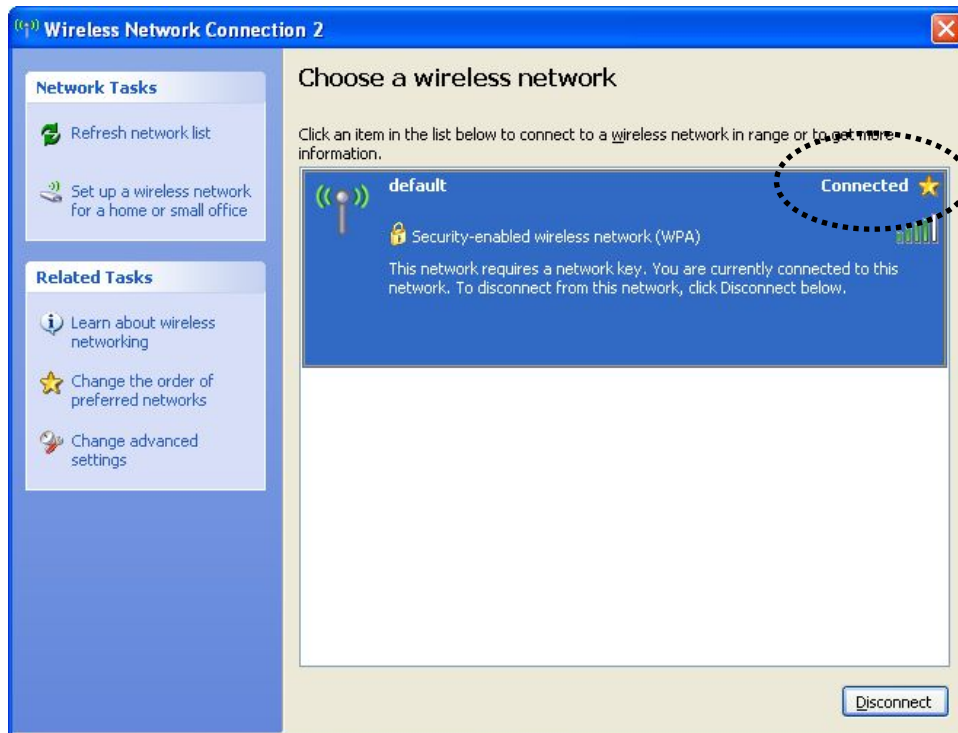
2-3 Connection Profile Management

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 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.

2-3-1 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'.
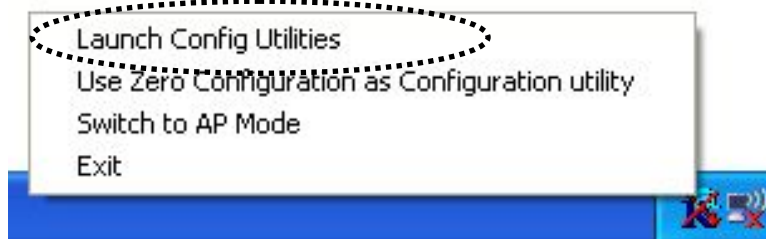
2. There are two ways to add a new connection profile:

   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:

And you can set the parameter for this connection here:

Here are descriptions of every setup items:

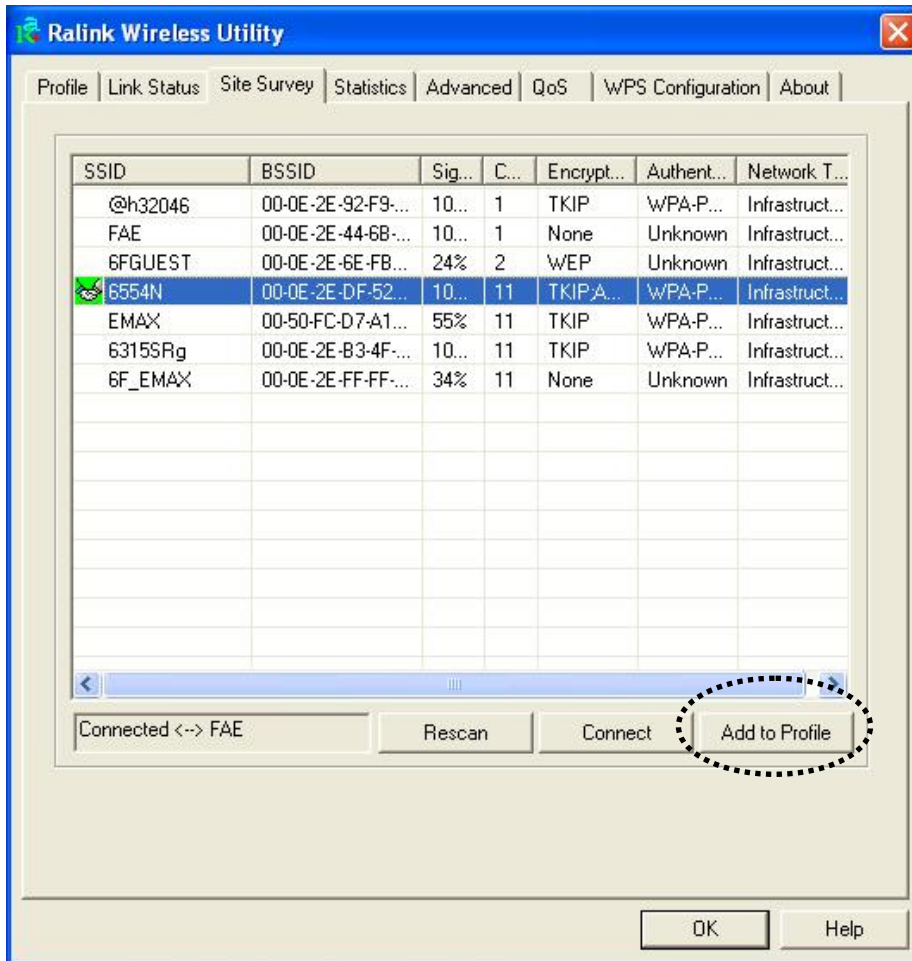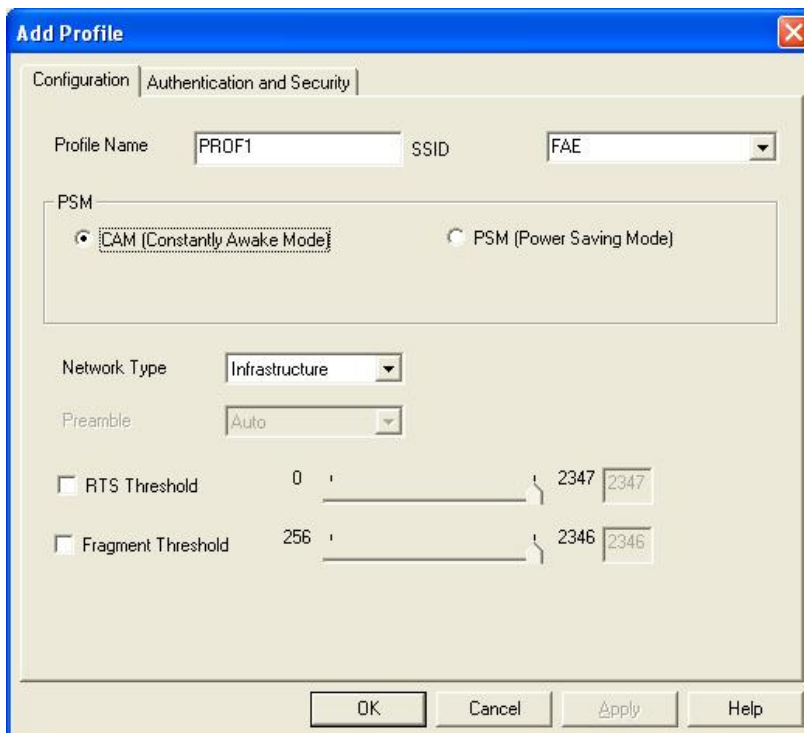|	
Profile Name	*Please give this profile a name, up to 32 alphanumerical characters and symbols are allowed, but space is not allowed.*
SSID	*The SSID of the wireless access point or wireless device you selected will be displayed here. But if the SSID of access point or wireless device is not available, you have to input it here manually.*
PSM: (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 'Authentication and Security' tab, and set the encryption and authentication settings.
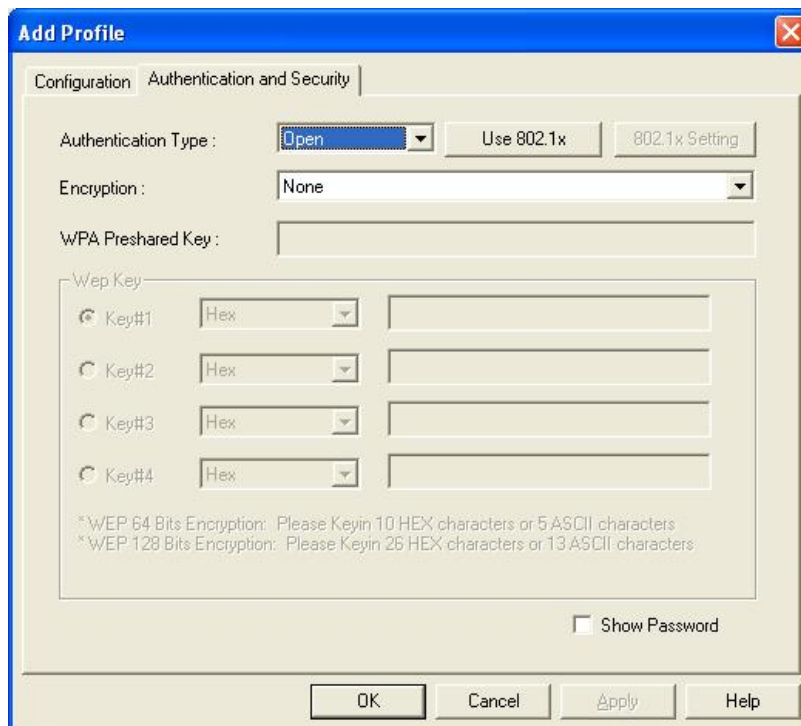
Here are descriptions of every setup items:

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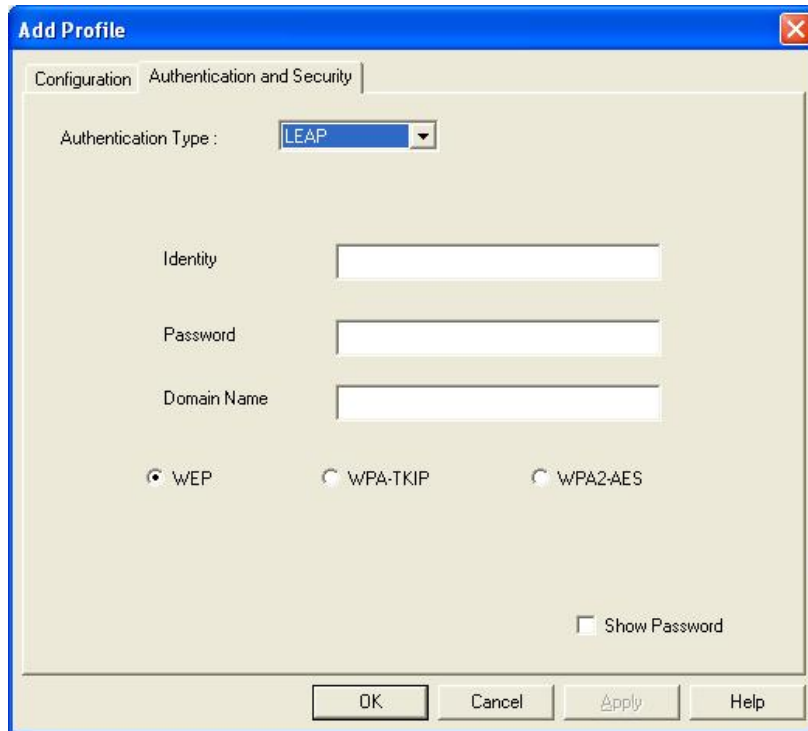
Encryption: *Select the encryption type of the wireless access point or wireless device you wish to connect. If you're adding a profile from an existing access point or wireless device, the value will be selected automatically, and please do not modify it.*

WPA   *Input WPA preshared key here. If encryption is not*
Preshared Key   *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.*

Use 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:
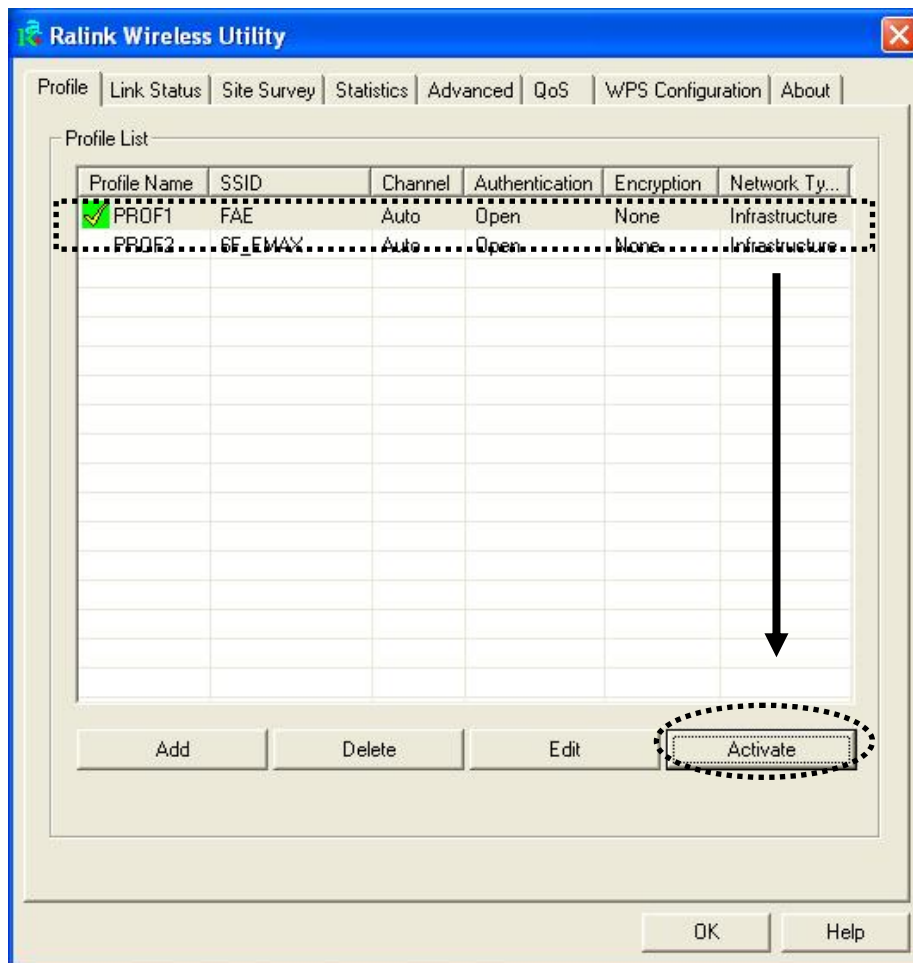
Select the profile you wish to use, and click 'Activate' to use the profile you selected. You can only activate a profile a time, and the profile which is activated currently will have a green check (☑) before its name. If the wireless access point is not reachable, a red check (☑) will be displayed before its name.

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'.

2-3-2 Using 802.1x – Certification

After you click '802.1x Setting', a new window will appear:
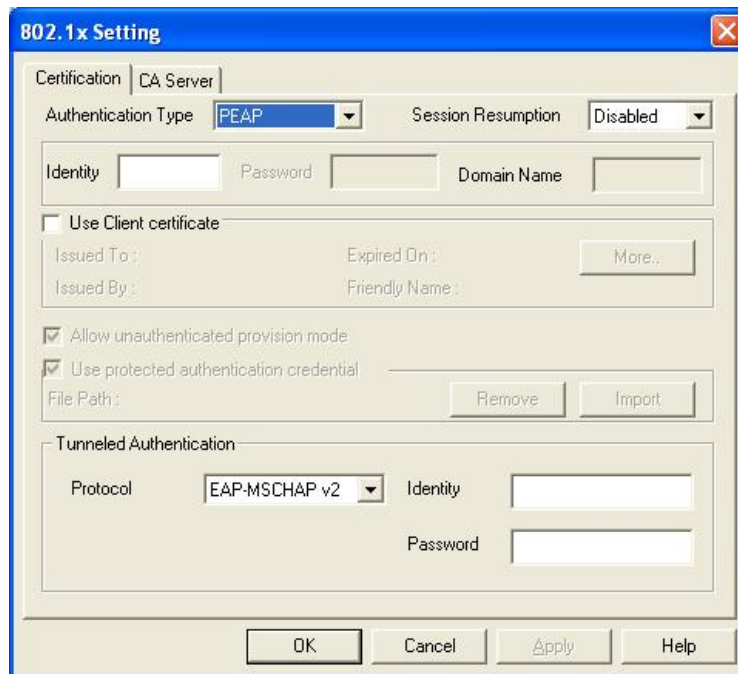
Here are descriptions of every setup items:

Authentication Type	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 if 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'.
Use Client	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.
More..	*After you clicked this button, you'll be prompted to select a certificate on your computer.*
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.*
Protocol	*You can select the protocol of tunneled authentication here. This pulldown 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.*
Identity (of tunneled authentication)	*Please input the identity of tunneled authentication here.*

Password (of tunneled authentication)	*Please input the password of tunneled authentication here.*
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.

2-3-3 Using 802.1x - CA Server

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

Here are descriptions of every setup items:

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 exactly	*Check this box and the wireless configuration utility will check if the server name of CA server 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.

2-4 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.

2-4-1 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'.
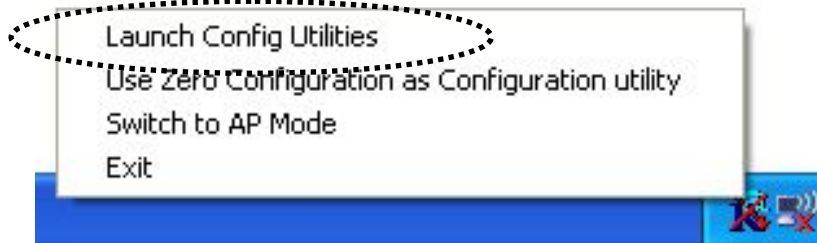
2. Click 'Statistics' tab, and the statistics of wireless connection will be displayed:

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

Click 'OK' to close the window.

2-4-2 Link Status

Please follow the following instructions to check network statistics:
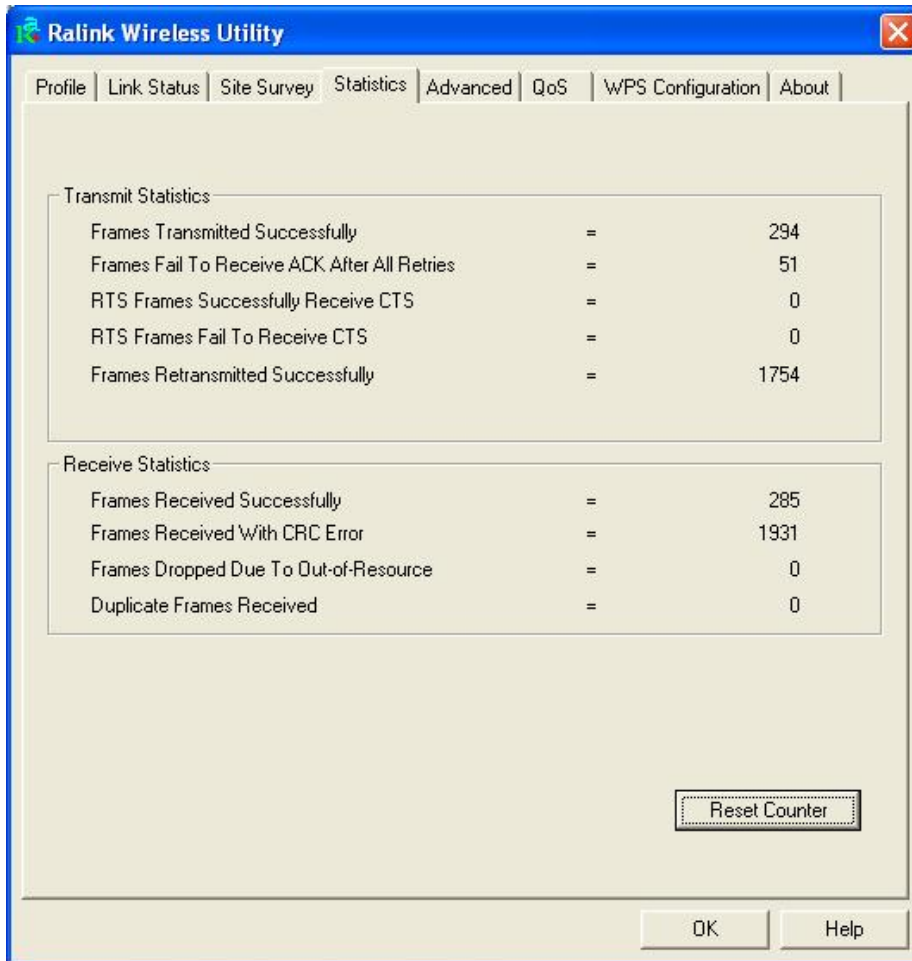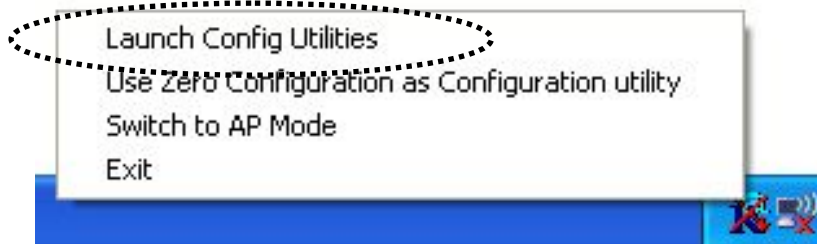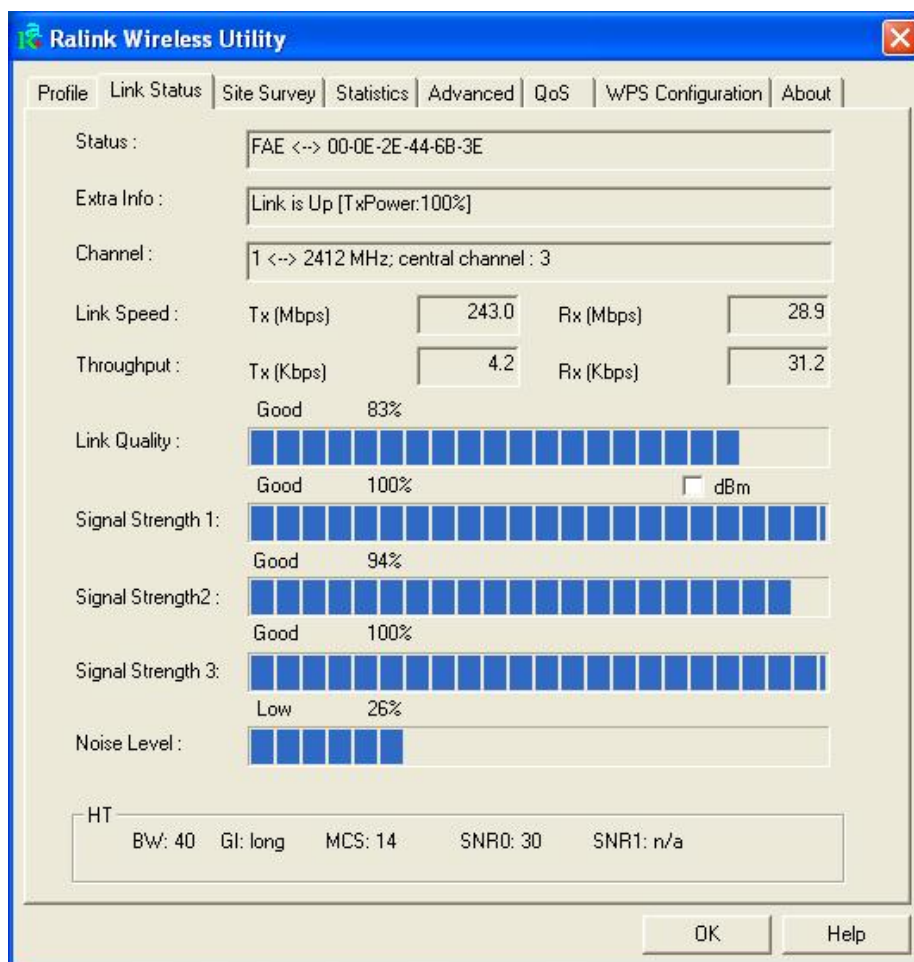
1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utilities'.

2. Click 'Link Status' 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.
dBm	*Check this box and the value of signal strength and noise level will be displayed in dBm level instead of percentage.*

There are several wireless statuses available at the bottom of this window. For their explanations, please see chapter 4-3 'Glossary'.

2-5 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:
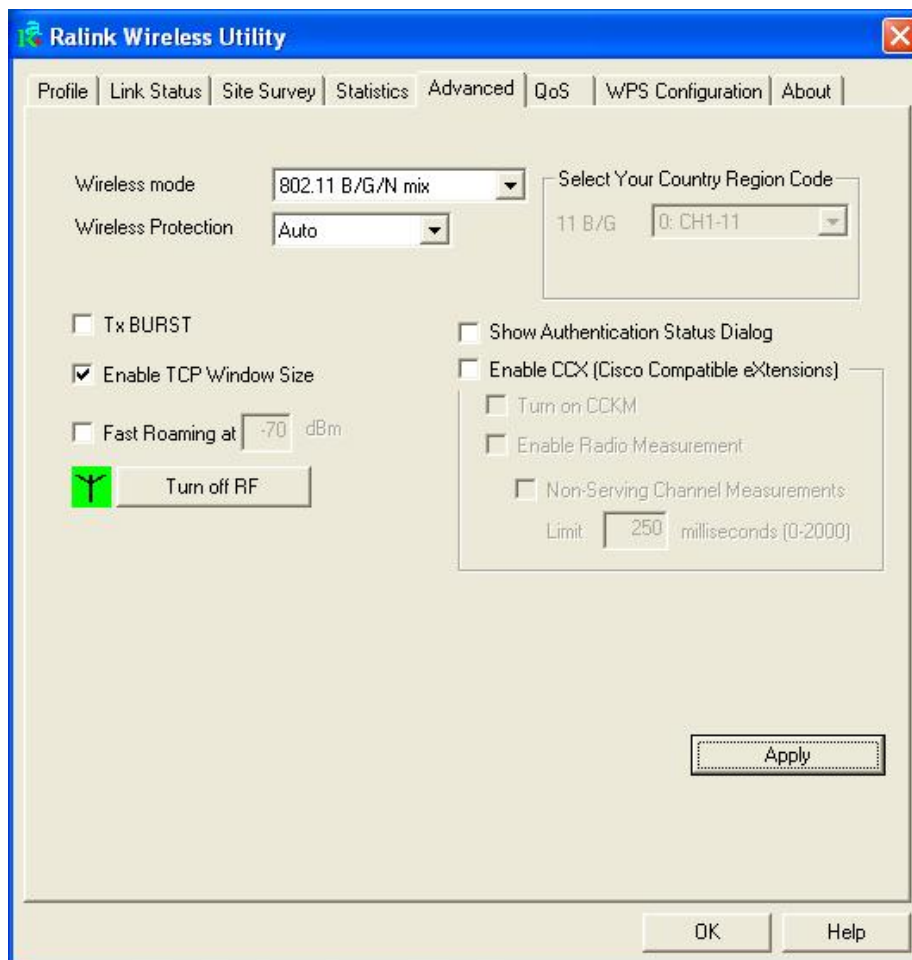
Here are descriptions of every setup items:

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.*
Wireless Protection	*This setting helps your network card to avoid interference with other wireless devices when there are both 802.11b and 802.11g wireless devices in the same place. It's recommended to set this setting to 'Auto', since enabling this setting will slightly reduce the data transfer performance.*
TX Rate	*Normally, the wireless network card will adjust transfer rate automatically according to wireless signal quality. However, you can fix the data transfer rate to a lower fixed rate if you think there's some problem about data transfer, or you're too far from wireless access point. It's recommended to set this setting to 'Auto', unless you really know the meaning of this setting.*
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.
Turn off RF	*Click this button to switch wireless radio off, click it again switch wireless radio on.*
Select Your Country Region Code	*Select the country / region code of the place you're living. Different country / region has different regulations on wireless devices, and it's forbidden to use certain channel (radio frequency) in some countries or regions.*
	The operating frequency channel will be restricted to the country / region user located before importing.
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	*When you're connecting to CCX-compatible*

Measurement	*access point, check this box to enable radio measurement function to improve wireless connectivity.*
Non-Serving Channel Measurements	*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.

2-6 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.
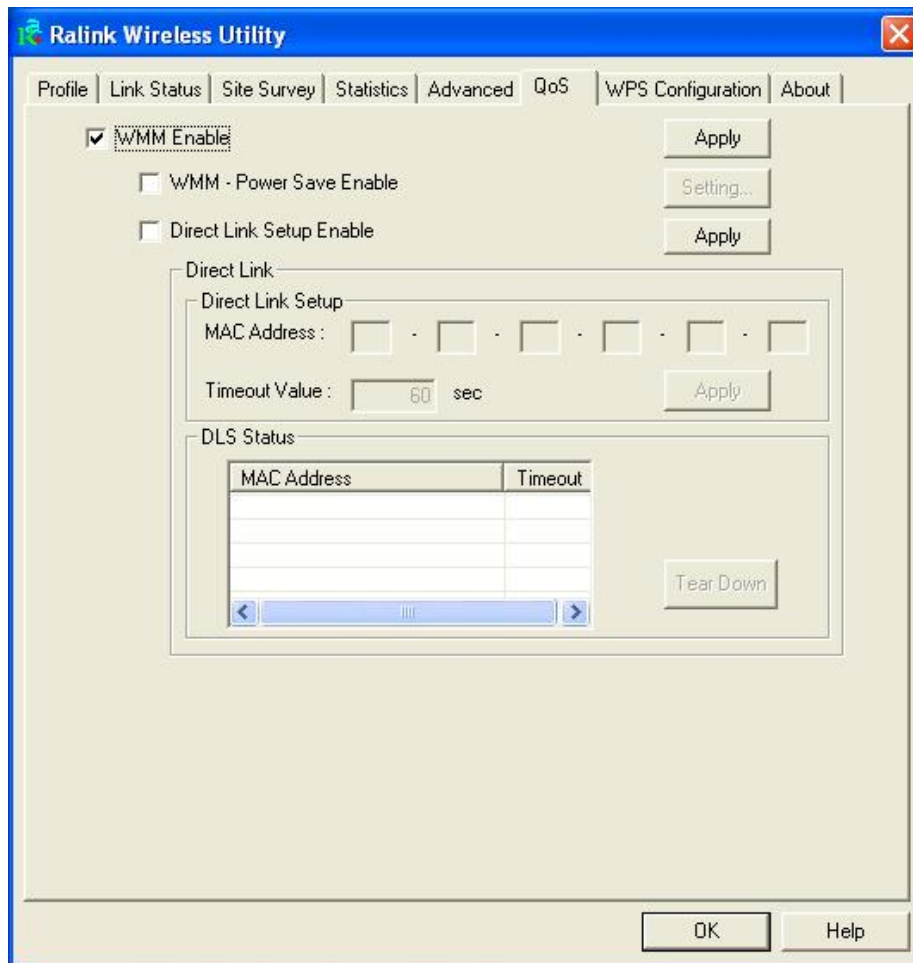
Please follow the following instructions to set advanced wireless settings:

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:

Here are descriptions of every setup items:

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.*
Setting...	*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 'OK' to close configuration utility.

2-7 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:

2-7-1 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:
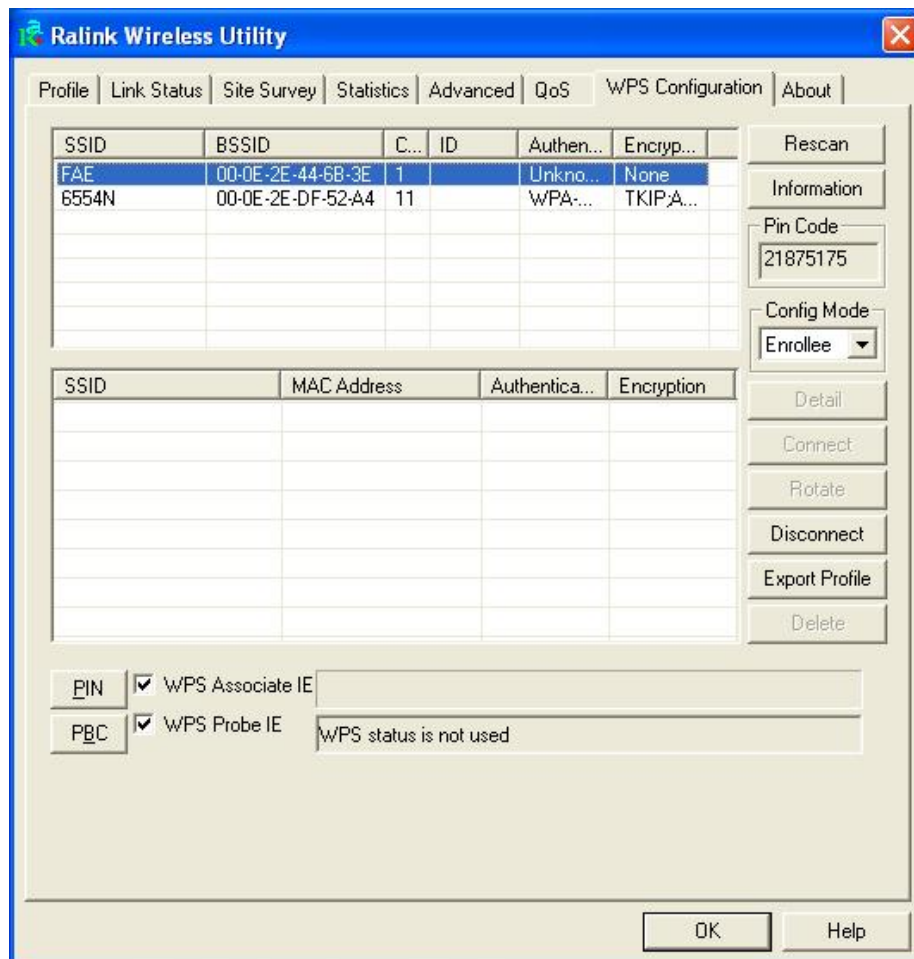
3. Set 'Config Mode' to 'Enrollee', and then push the 'WPS' button on your wireless access point (the button used to activate WPS standby mode may have another name), or use other way to start WPS standby mode as the instruction given by your wireless access point's user manual.

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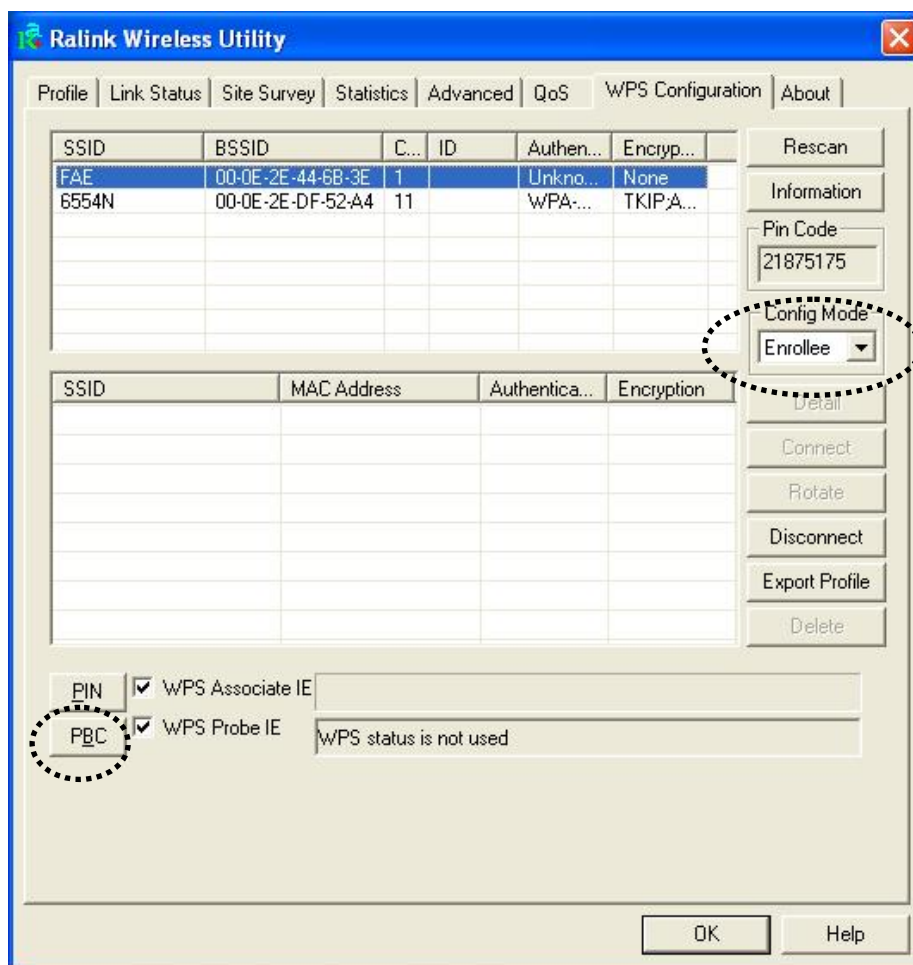
All access points with WPS function enabled will be displayed. Please make sure the access point you wish to connect is displayed. If not, please click 'Rescan' few more times. You can also click 'Information' button to see the detailed information about selected access point.

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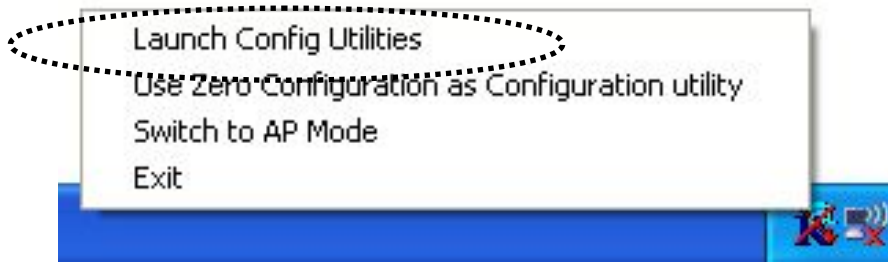
button in wireless configuration utility to start to establish wireless connection by WPS. Please be patient (This may require several seconds to one minute to complete). When you see 'WPS status is connected successfully' message, means the connection between your wireless network card and access point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

2-7-2 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:
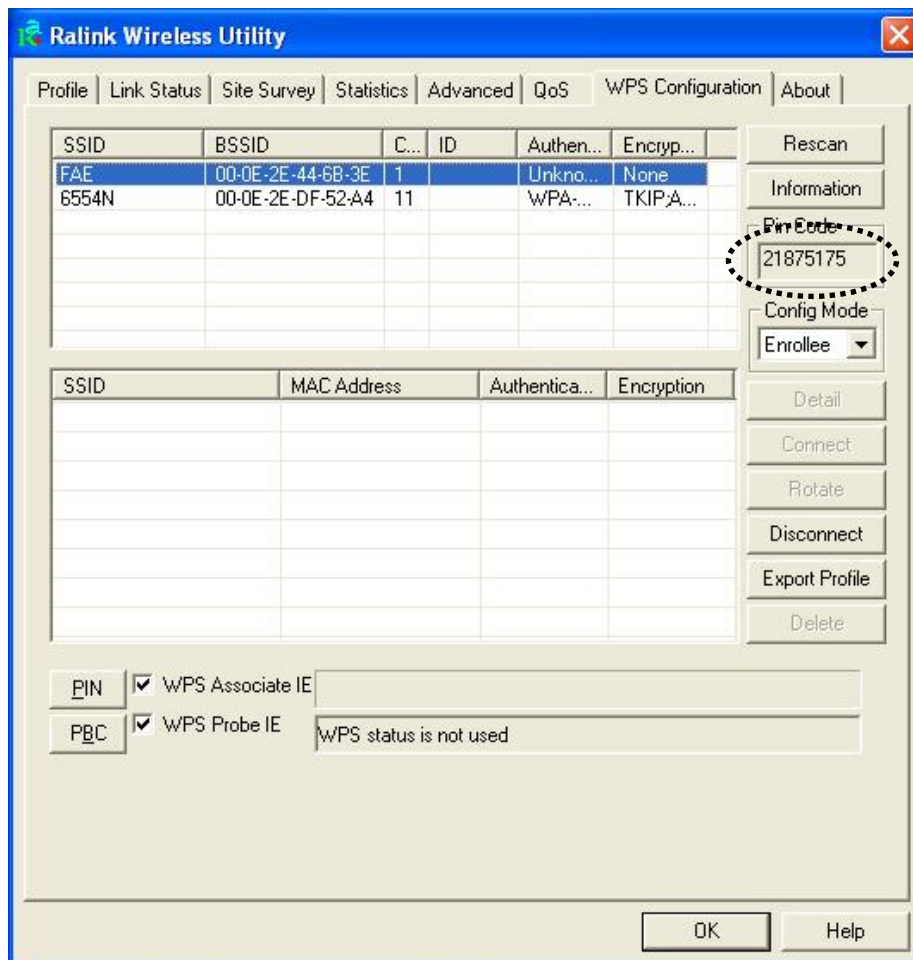

The PIN number of your wireless network card is an eight-digit number

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).

NOTE: The PIN code of every wireless network card is DIFFERENT. Please don't use the sample code shown here.

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:
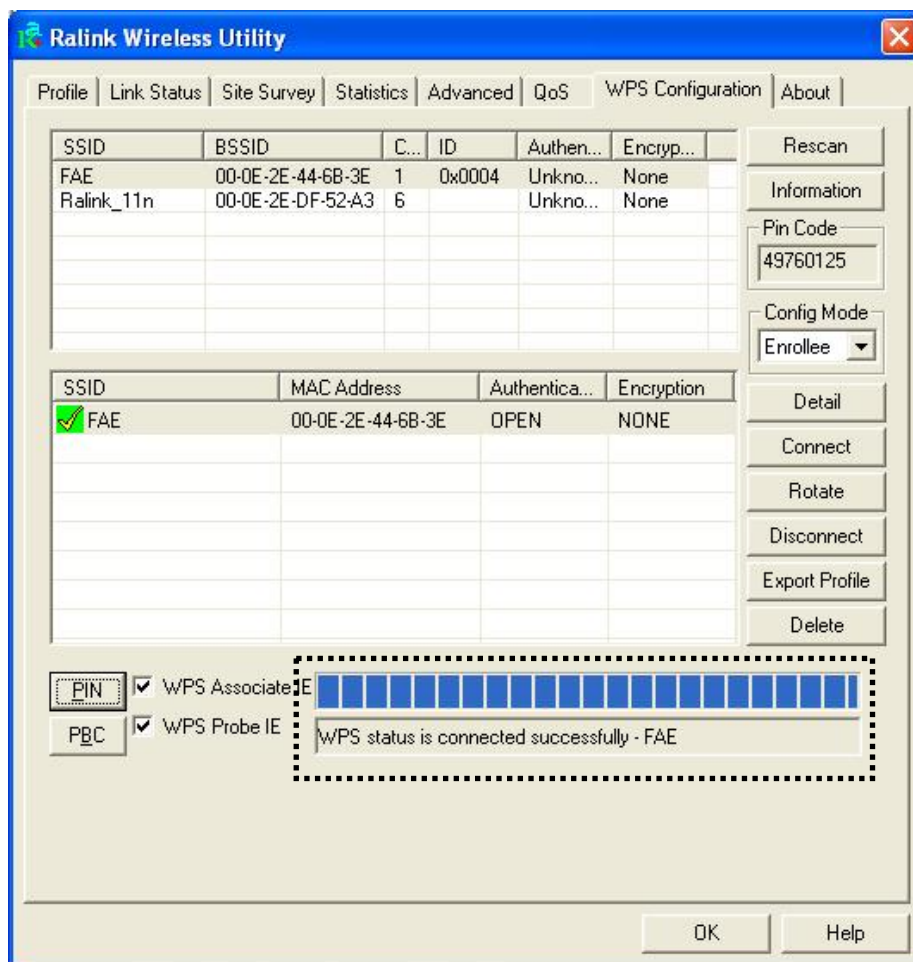

You may have to click 'PIN' for few more times to try again. If you still can not connect to access point by this way, please make sure the PIN code you provided to access point is correct.

2-8 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'.
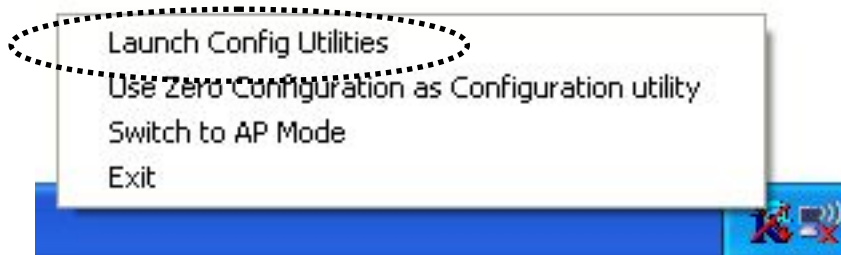
2. Click 'About' tab, and the following settings will appear:
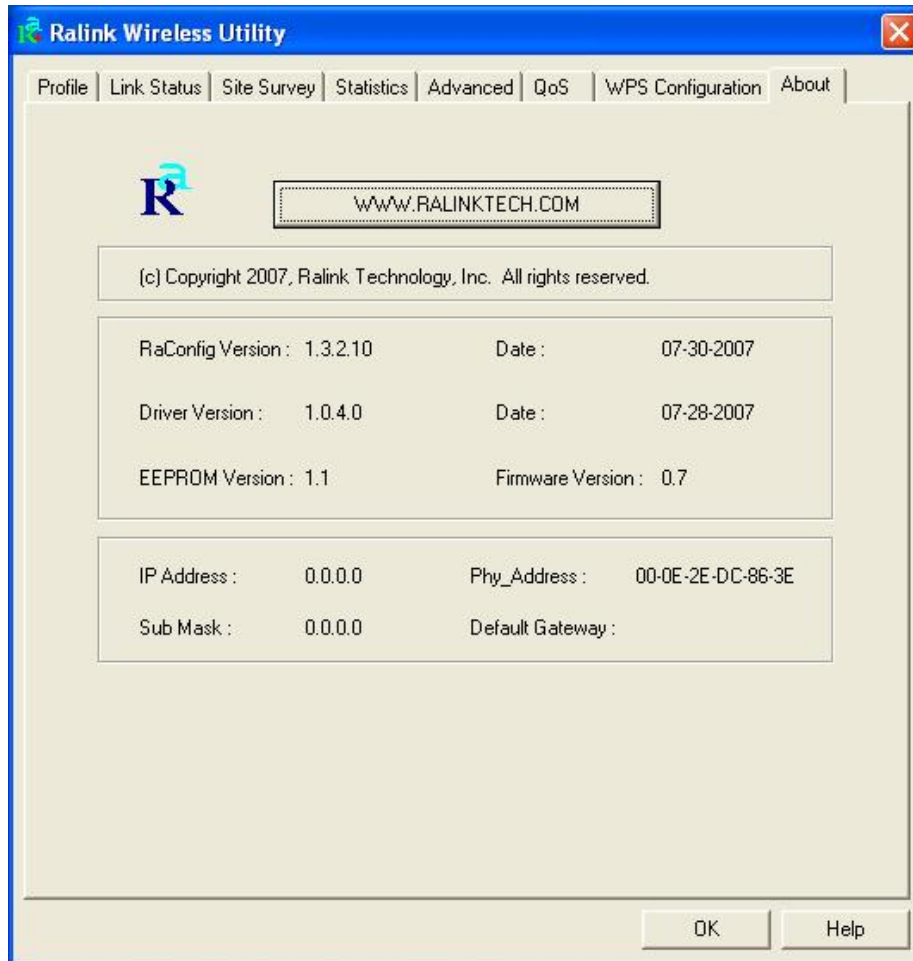
If you need assistance about network problem, you'll need these values.
You can also click 'WWW.RALINKTECH.COM' button to go to the web
site of network card driver manufacturer and get more information about
your wireless network card.

Please click 'OK' to close configuration utility.

CHAPTER III: 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.

3-1 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'.
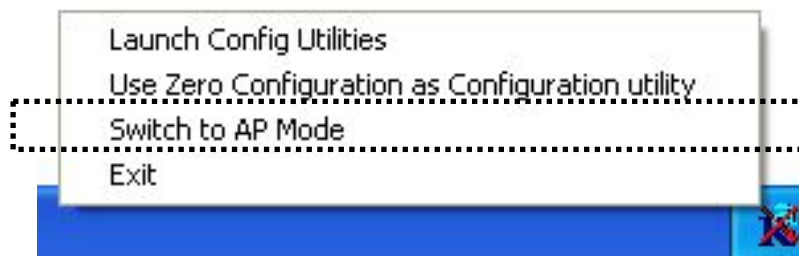

After you select 'Switch to AP Mode', the Ralink utility icon will change:

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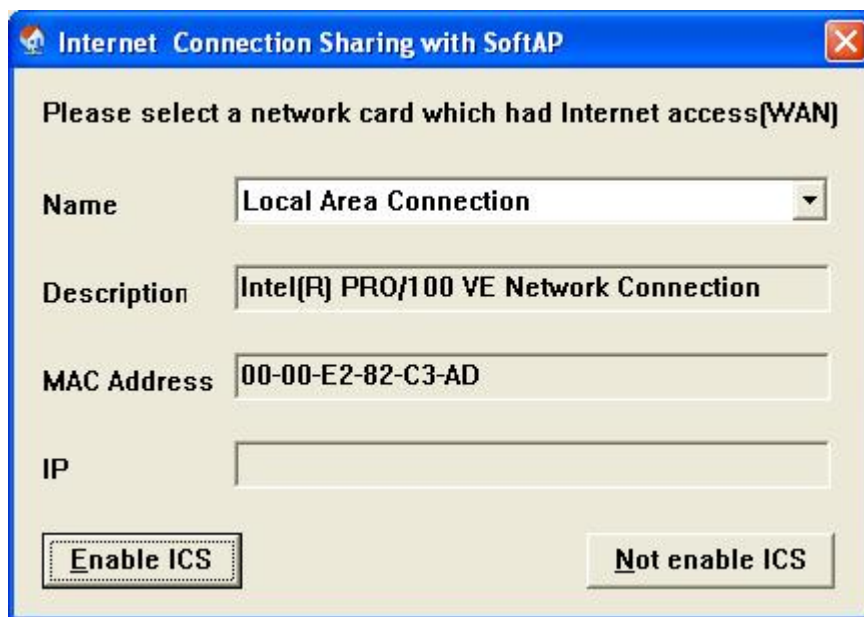
If your computer has another network card which is connected to Internet, please select it from 'Name' dropdown menu, and click 'Enable ICS'; if your computer does not have another network card with Internet connection, please click 'Not enable ICS'.

After you click 'Enable ICS' or 'Not enable ICS', you'll see the basic configuration menu of the AP function:
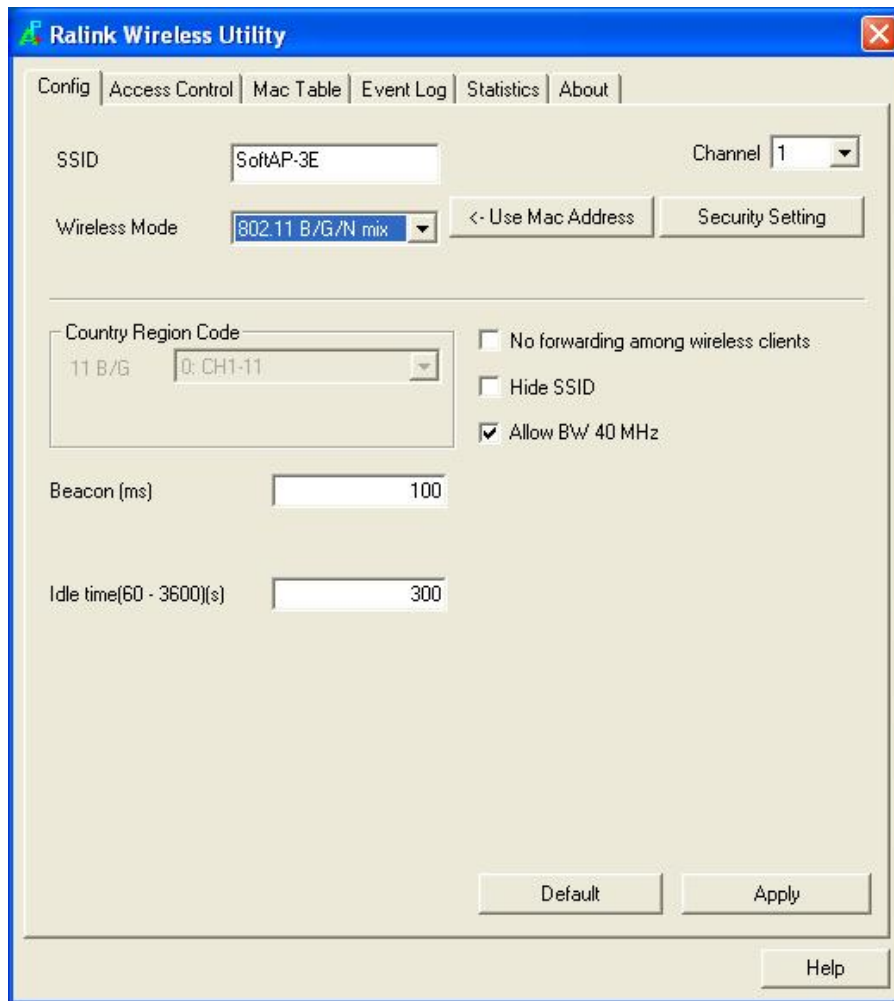
Here are descriptions of every setup items:

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

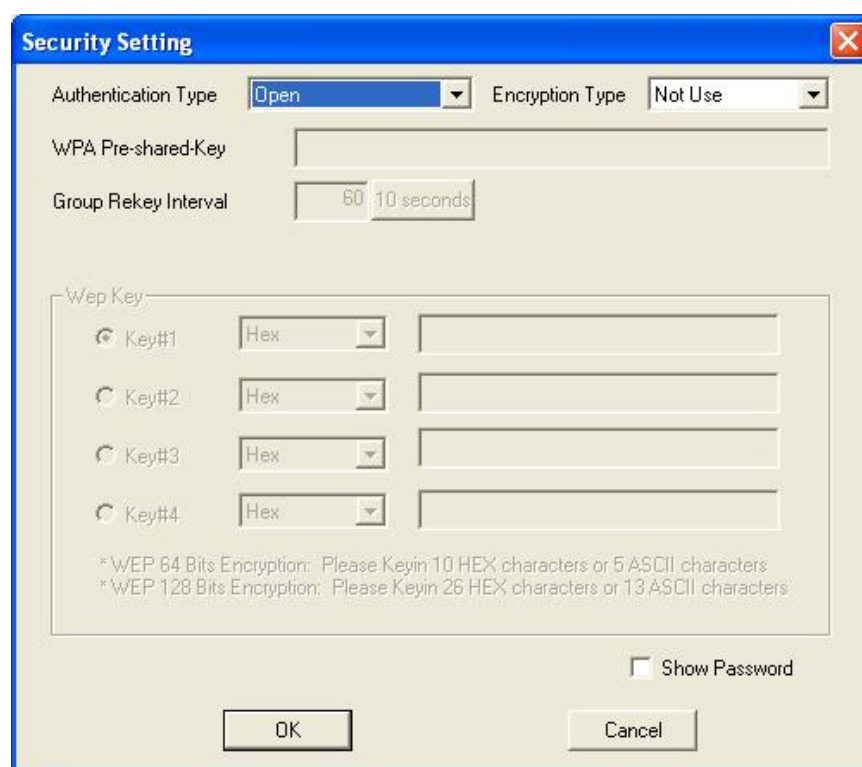|	
	use wireless protection or not. You can also select 'ON' or 'OFF' to force the use of wireless protection or not.
Beacon(ms)	*You can define the time interval that a beacon signal should be send. Default value is 100. Do not modify this value unless you know what will be affected.*
Idle Time	*Select 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.

3-2 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:

Here are descriptions of every setup items:

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.*

3-3 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'
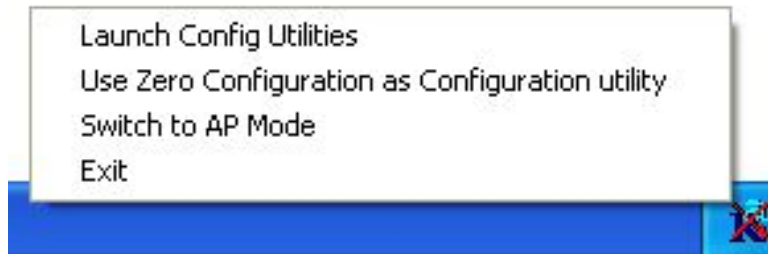
2. Click 'Access Control' tab, and the following messages will appear:
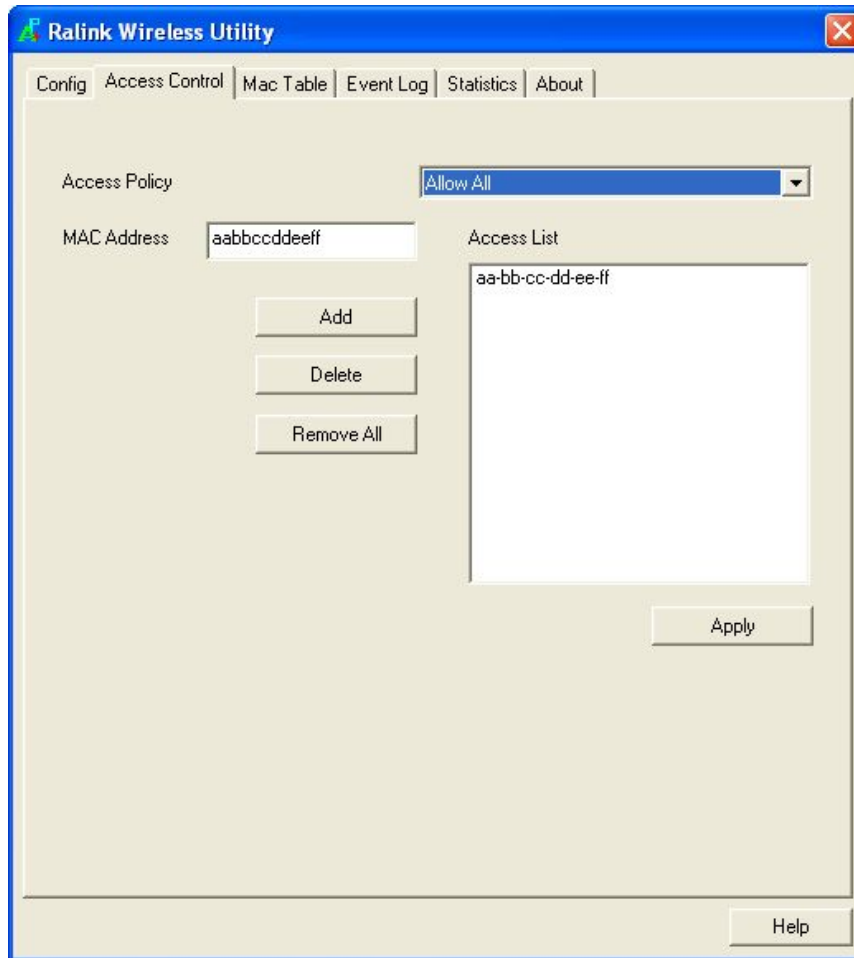
Here are descriptions of every setup items:

|	
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 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.*
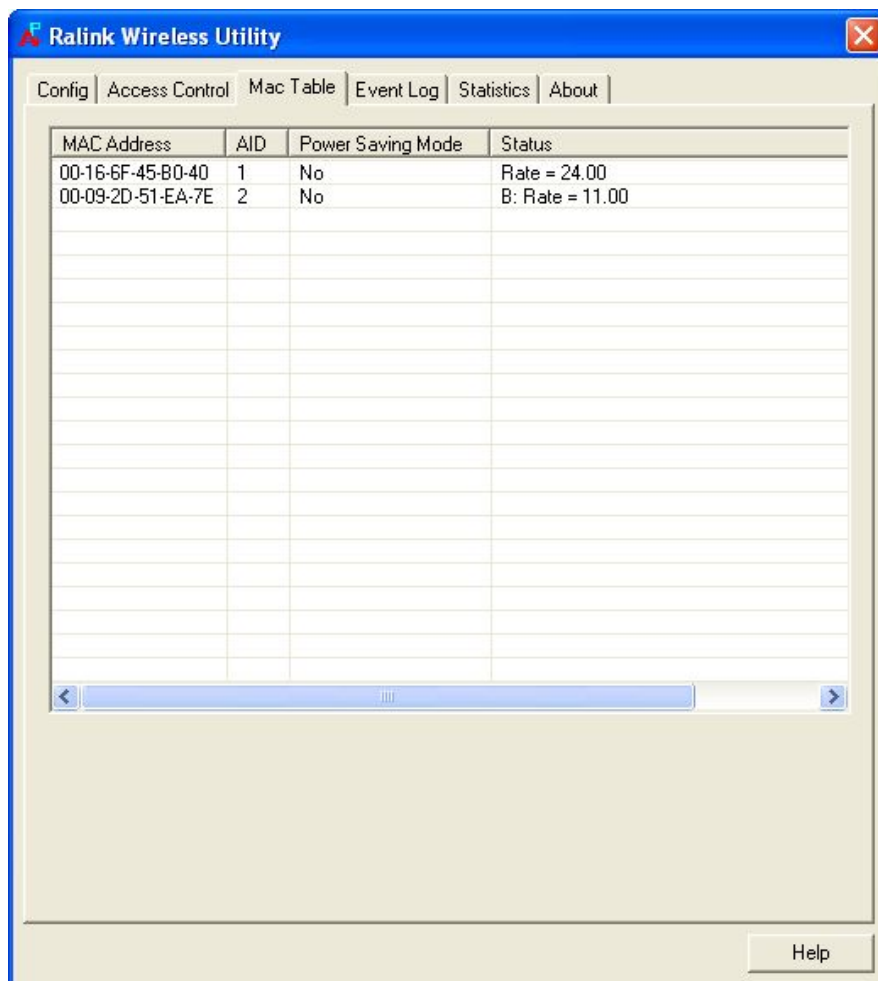
Apply   *Save and apply changes you made.*

3-4 Connection table

If you want to see the list of all wireless clients connected to this access point, please follow the following instructions:

1. Right-Click Ralink configuration utility icon, and select 'Launch Config Utilities'
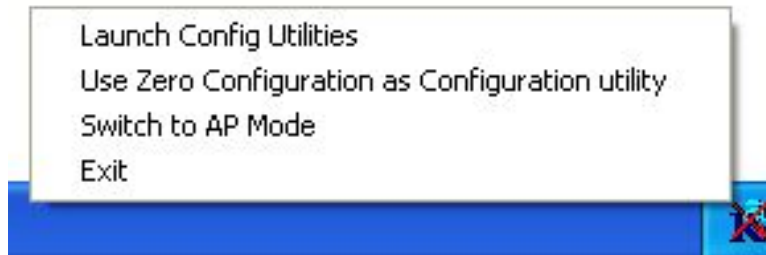
2. Click 'Mac Table' tab, and a list containing all connected wireless clients will appear:

Here are descriptions of every fields:

|	
MAC Address	*Displays the MAC address of this wireless client.*
AID	*The serial number of this wireless connection.*
Power Saving Mode	*Displays the capability of power-saving function of this wireless client.*
Status	*Displays additional information of this wireless Connection, like current wireless operating mode and data transfer rate.*

3-5 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'
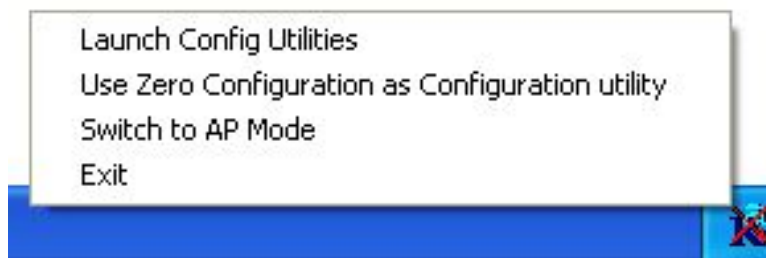
2. Click 'Event Log' tab, and the event log will be displayed:
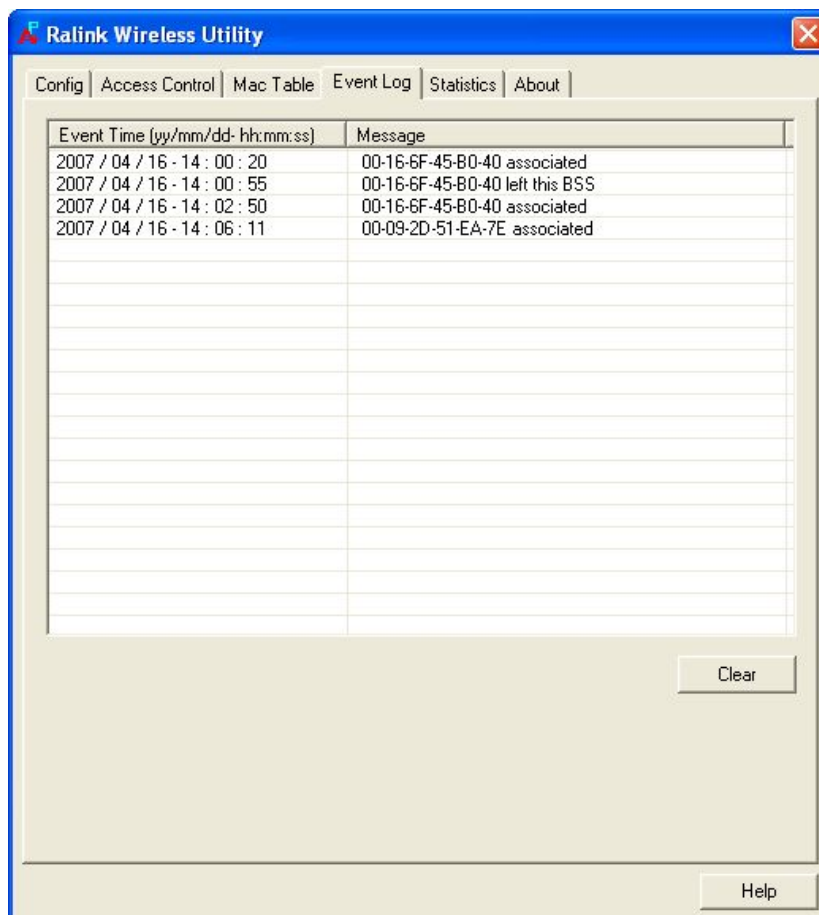
You can click 'Clear' to remove all entries in the log.

3-6 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'

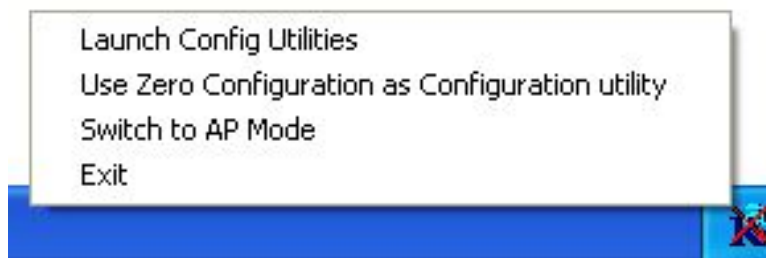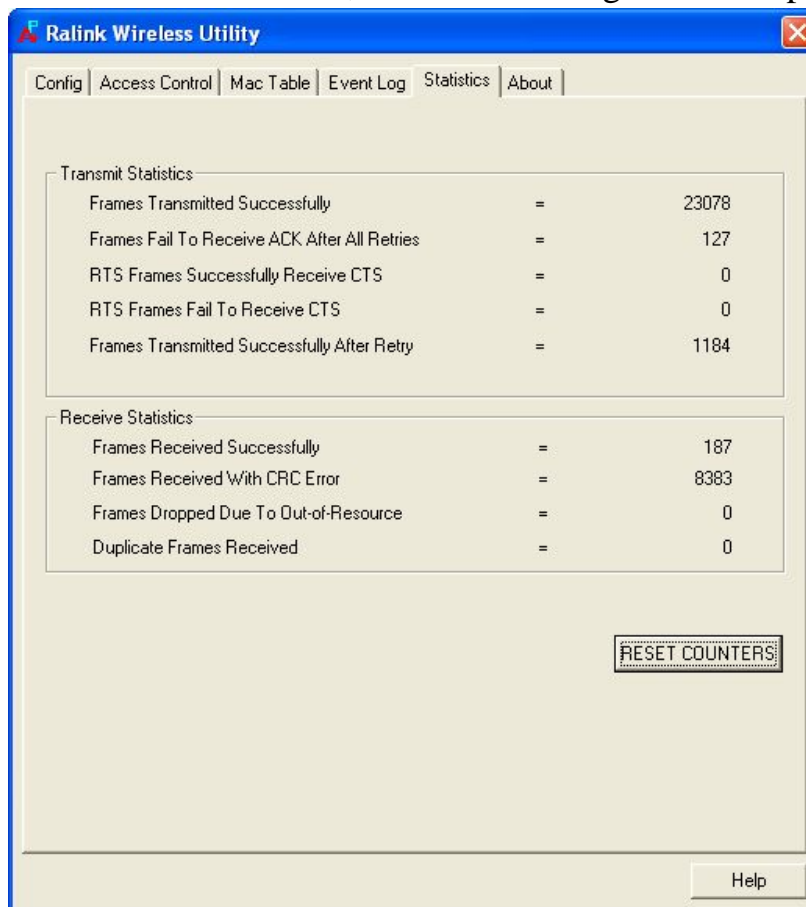2. Click 'Statistics' tab, and the event log will be displayed:

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

3-7 Wireless LAN Installation Guidelines and Authorization for

User

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by Chung Nam Electronics (CNE) may void the user's authority to operate the equipment. CNE is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. CNE and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful.

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please first verify authorization to use these devices prior to operating the equipment.

Chapter 4 Regulatory Information

4.1 FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

4.2 FCC Guidelines for Human Exposure

Warning:

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

4.3 FCC Electronic Emission Notices

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.

4.4 FCC Radio Frequency 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 when the equipment is operated in a commercial environment. 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. Operation of this equipment in a residential area may cause harmful interferences, in which case the user will be required to correct the interference at his own expense.

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

4.5 OEM installation Guide

This device is intended only from OEM integrators under the following conditions:

1) The antenna must be installed such that 20cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna.

IMPORTANT NOTE: in the event that these conditions can not be met (for example Certain laptop configurations or co-location with another transmitter). Then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances. The OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter nodule is authorized only for use in devices where the antenna may be installed such than 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ADSL modems, and similar equipment). The final end product must be labeled in visible area with the following:

"Contains TX FCC ID: Q72WLC123NR"

End Product Manual Information

The user manual for end users must include the following information in a prominent location "IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

IMPORTANT NOTE

FCC RF Radiation Exposure Statement: This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

RF Exposure Info (For mobile configuration)

To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter

This device is certified as modular radio form with the following antenna types. Change to other type requires re-evaluation/ certification

Dipole Antenna 1.8 dBi max

Chapter 5 Technical Specifications

Appendix A: Specifications

Standards	IEEE802.11b, 802.11g, 802.11n Draft 2.0
Operating Frequency	2.4 GHz ~ 2.4835 GHz ISM band 2.4 GHz ~ 2.497 GHz (Japan ISM band)
Channel Bandwidth	20/40MHz Support
Protocols	802.11b: CCK, QPSK, BPSK 802.11g: OFDM 802.11 Draft-N: BPSK, QPSK, 16-QAM, 64-QAM
Security	802.11i – WEP 64/128, WPA & WPA2. Cisco CCX V1.0, V2.0 & V3.0 Compliant
Receive Sensitivity	54Mbps@-70dBm (Typical) Draft-N@-70dBm (Typical)
Operating Voltage	3.3 VDC ± 10%
Bus Interface	Mini-PCI
Antenna Connector Type	3 pieces of SMT ultra-miniature coaxial connectors
Antenna port impedance	50ohm