Chung Nam Electronics (CNE)

IEEE 802.11b/g/n WLAN USB Adapter
(Model #: WLC311NRM)
User Manual

Version 2.0

December 2008

Contents

Chapter 1: Product Information

1.1 Introduction

CNE WLC311NRM is a USB 2.0 pen-size WLAN USB Adapter supporting IEEE 802.11b/g/n at 2.4GHz radio operation, The WLAN USB Adapter provides high-speed wireless connectivity with data rate from 1 Mbps up to 135Mbps theoretically. Additionally, wireless roaming allows the user to move among different access points without losing the connection. The WLAN USB Adapter also provides excellent security features such as WEP 64/128, WPA, WPA2, TKIP, AES, WPS, PBC, PIN encryption security which make the network almost impenetrable.

Featuring high performance transmission rates, simple installation and adaptability as well as strong security, the WLC311NRM WLAN USB Adapter is the perfect solution for small office and home use.

1.2 Features

- Complies with IEEE 802.11b/g, IEEE 802.11n Draft 2.0 standards.

- 1T1R Modes with 135Mbps PHY Rate for Antenna configurations.

- Legacy and High Throughput Modes.

- Dynamic data rate: Maximum data rate up to 135Mbps. Auto fallback switching with 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 and 1Mbps.

- Reverse Direction Grant Data Flow and Frame Aggregation.

- QoS-WMM, WMM-PS.

- Multiple BSSID Support.

- Wireless data encryption with 64/128 encryption for security

- Supporting WPS by external push button or software API.

- Lower Power with Advanced Power Management.

- Drivers supports Windows XP 32/64, 2000, Vista32/64, Linux, Macintosh.

1.3 LED Status

The LEDs in this WLAN USB Adapter indicate Link/Act status. It blinks at green light when sending and receiving data.

Chapter 2: Installation Guide

2.1 Overview

The WLC311NRM WLAN USB Adapter Setup Wizard will guide you through the installation procedure for Windows 2000, XP, Vista and Linux. This Wizard will also guide you installing the Utility and drivers.

In case you plug in the hardware before installing the software, you will be prompted by "Found New Hardware Wizard", please click the **Cancel** button, and run the Setup Wizard program from the installation CD-ROM shipped together with the USB Adapter.

All of following sections are written based on Windows XP.

* **Note:** The comments and conditions for other OS platforms may be different from this chapter.

2.2 Installation procedure

2.2.1 Software installation
Please follow below instructions to install the driver for WLC311NRM WLAN USB Adapter.

1. Insert the Resource CD into the CD/DVD-ROM drive of your computer; then execute **Setup.exe** to install the driver. The system will operate automatically,
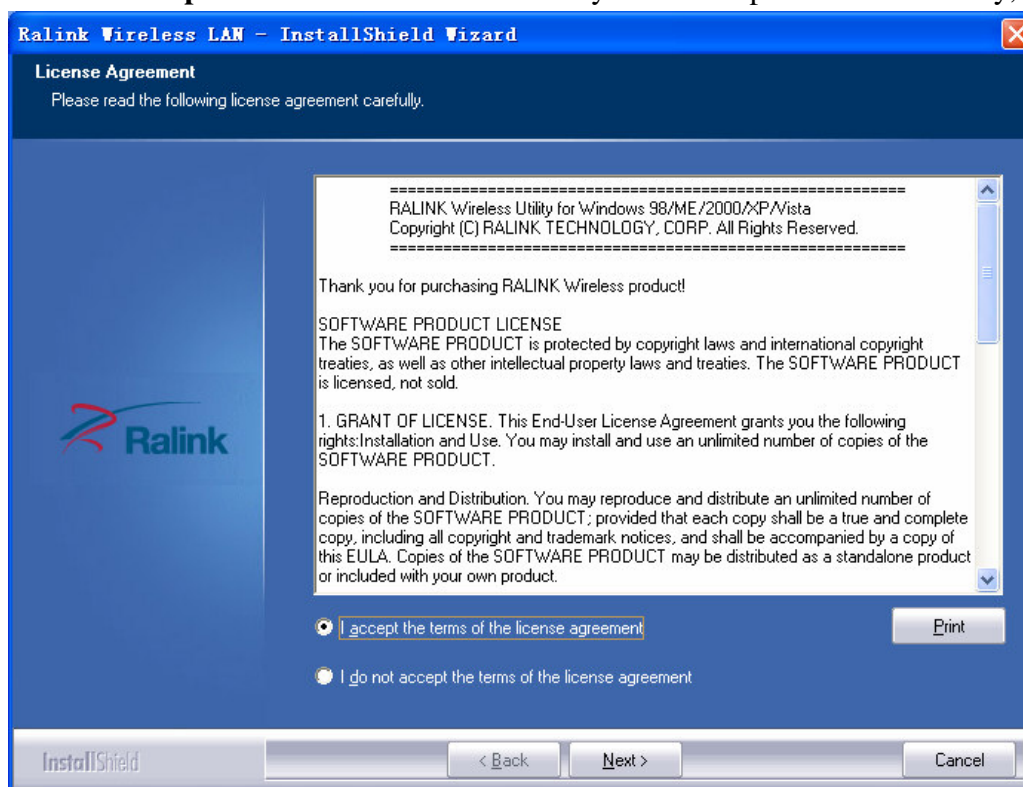

Figure 2-1 License Agreement

and the License Agreement dialog box as shown in *Figure 2-1* will appear on the

screen. Please read all the license agreement thoroughly and select **Yes** in case you accept the terms and conditions of the license agreement, then click **Next >**.

2. The dialog box **Setup Type** shows as *Figure 2-2* will allow you to choose your wanted driver, you can select the best suit your needs. It is recommended to choose the **Install driver and Ralink WLAN Utility**, and click on the button **Next >**.
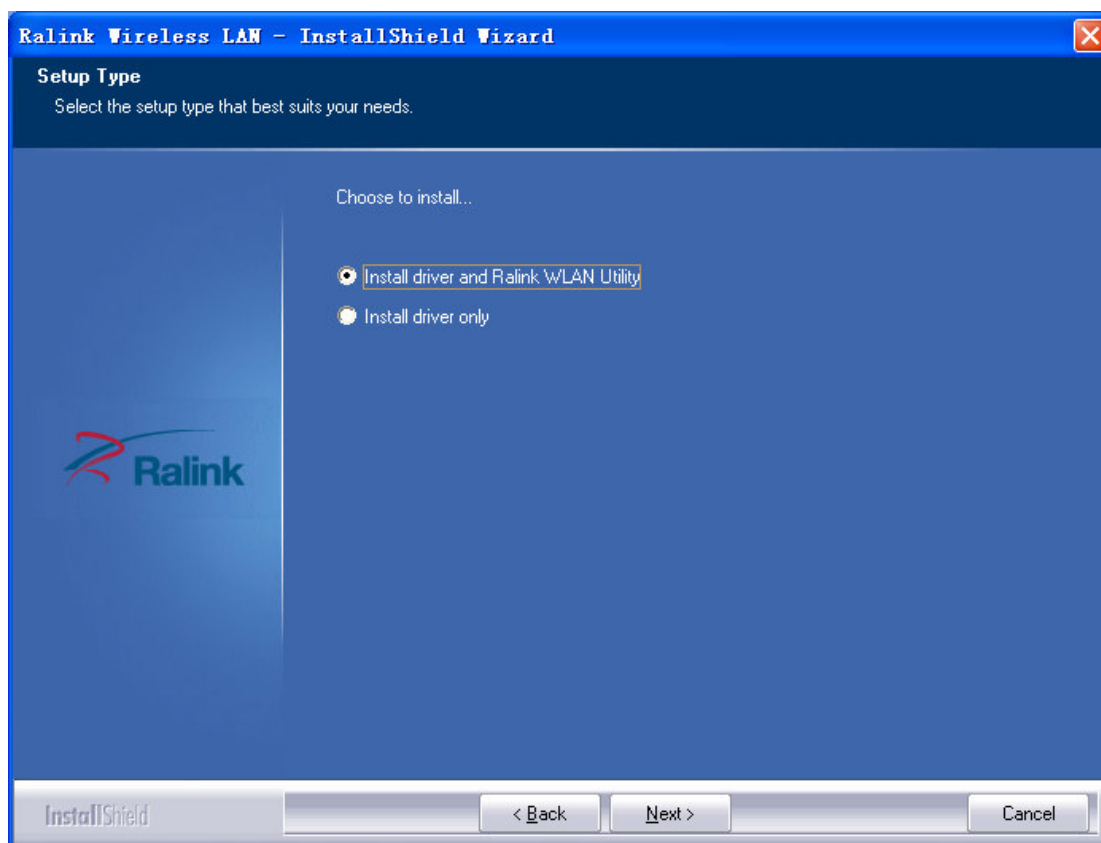
Figure 2-2 Setup Type to choose installed driver

3. The **Setup Type** dialog box as shown in *Figure 2-3* appears on the screen, you can choose either using **Ralink Configuration Tool** or **Microsoft Zero Configuration Tool** to configure your new IEEE 802.11b/g/n USB WLAN USB Adapter. However, it is recommended to select **Ralink Configuration Tool** to configure the USB Adapter as it provides fully access to all functions of the USB Adapter. If you prefer to use the wireless configuration tool provided by Windows XP or Vista, please select **Microsoft Zero Configuration Tool**. Then click **Next** to continue.
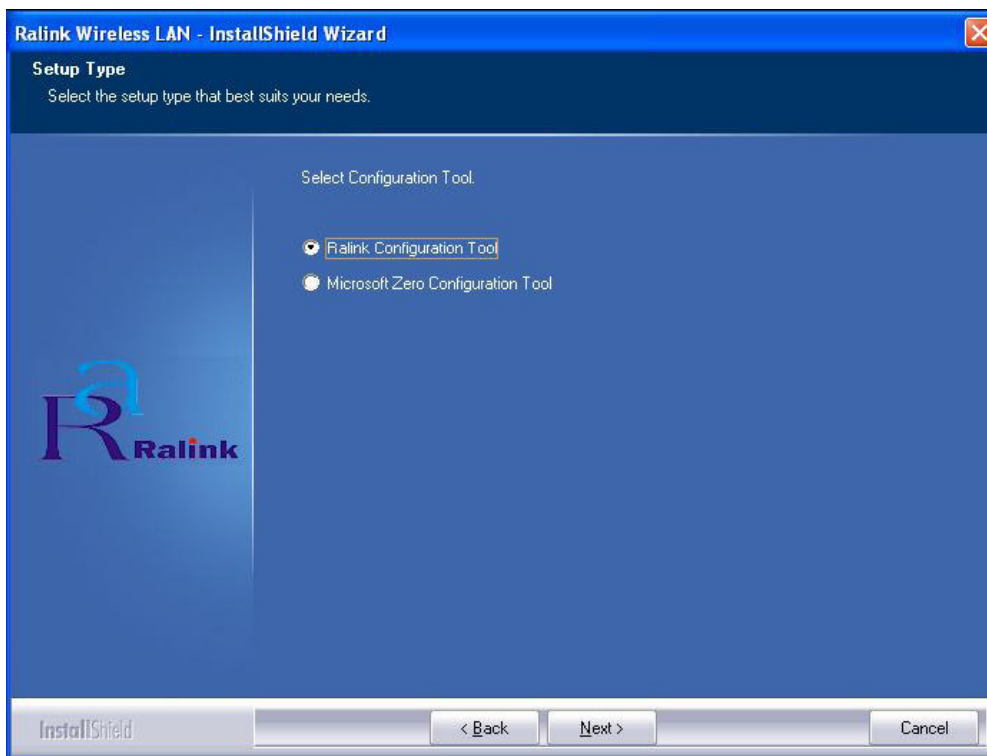
Figure 2-3 Select Configuration Tool in the Setup Type

4. You have selected the setup type that best suit your needs, and you are ready to install the program, please select the button **Install** in the dialog box *Figure 2-4*.
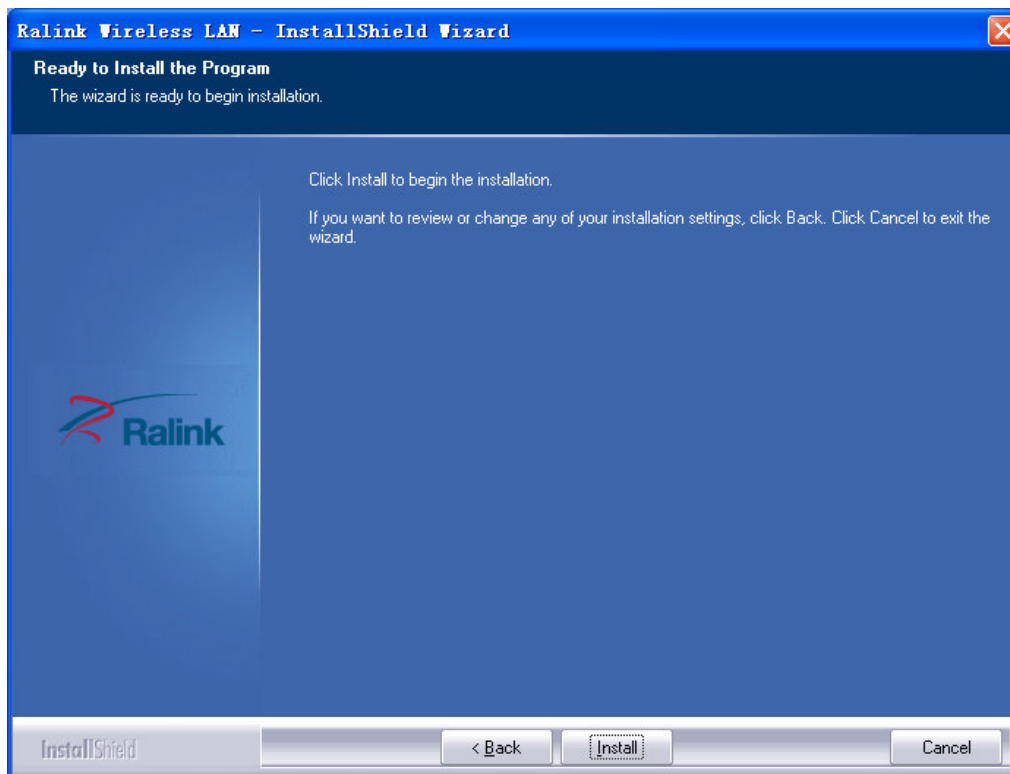
Figure 2-4 Ready to install the program

5. Please wait for a moment and the dialog box of **Setup Status** as *Figure 2-5* will appear on the screen.
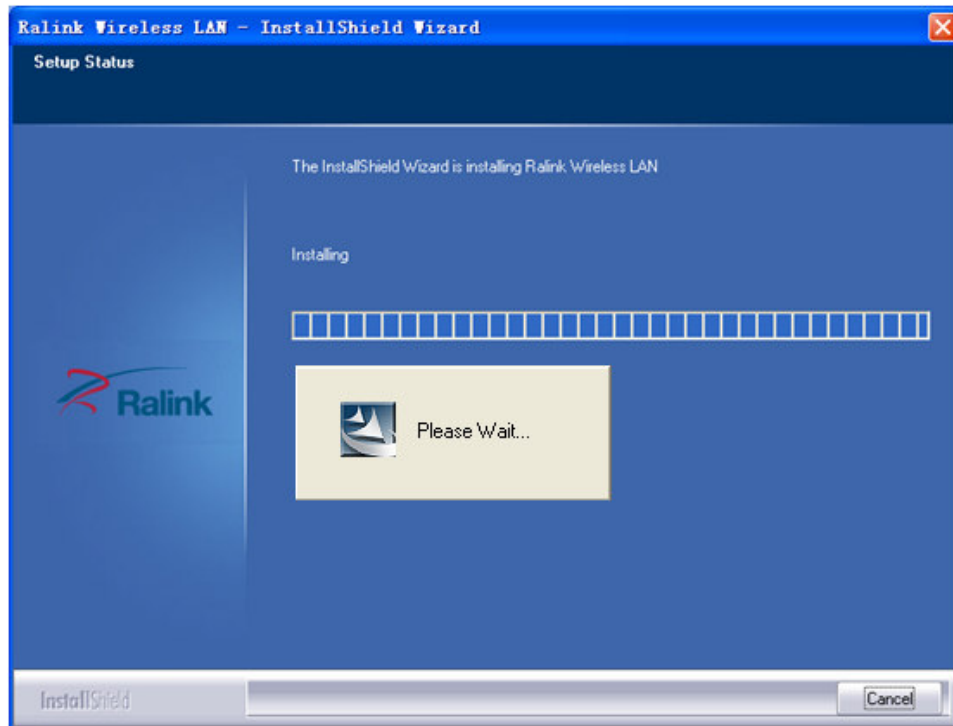
Figure 2-5 Setup Status

6. When the computer finish the driver installation. The screen of *Figure 2-6* will then appear. Click the **Finish** to complete the installation.
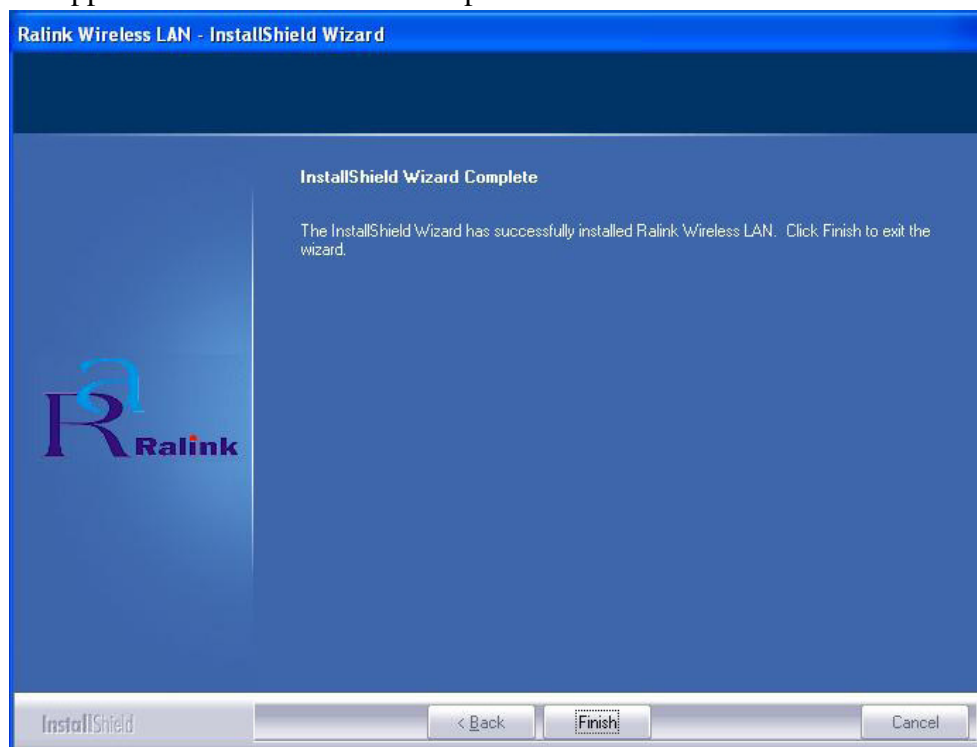
Figure 2-6 Install Shield Wizard Complete

7. A new icon will appear at the lower-right corner of your computer after driver

installation. If you put the mouse cursor on top of the icon, a pop up message box will indicate to you that the WLAN USB Adapter does not exist.

8. Please plug in the WLC311NRM WLAN USB Adapter into your PC for the hardware installation. If you want to understand the detail hardware installation instructions, please refer to next section – Hardware Installation.

2.2.2 Hardware Installation
After successfully installation of the software driver, please plug the WLC311NRM WLAN USB Adapter into your PC for WLAN card hardware installation. The OS will detect the USB Adapter and find the appropriate driver automatically (In case it does not, please follow the setup steps again as despite in Section 2.2.1) and the the icon

will appear in your system icon box.
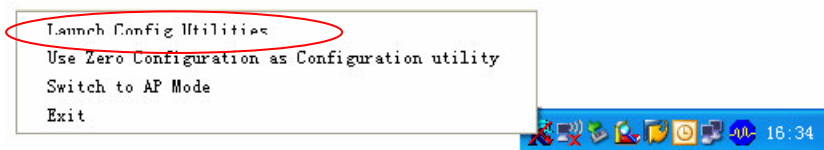
Figure 2-7 select the configuration of the WLAN USB Adapter

When you want to configure your WLAN USB Adapter, please right click the icon

, and a popup menu of *Figure 2-7* will appear. You can click **Launch Config Utilities** to start the configuration. If you want to close configuration utility, please click **Exit**.

＊ **Note:** If you want to stop configuration utility by clicking the **Exit**, you'll not be able to maintain the current wireless link connectivity to the access.

You can start configuration utility again by clicking **Ralink Wireless Utility** icon from **Start -> All Programs -> Ralink Wireless -> Ralink Wireless Utility.**

2.3 Uninstall Software

2.3.1 Uninstall the driver software

If you want to install a new WLAN USB Adapter, you have to uninstall the software driver. Below are the procedures to uninstall the driver:

To remove any old software or this WLAN USB Adapter in Windows XP:

1. On the Windows taskbar, click the **Start** button, select the **programmer -> Ralink Wireless -> Uninstall - RT2870** as *Figure 2-8* to uninstall the software.
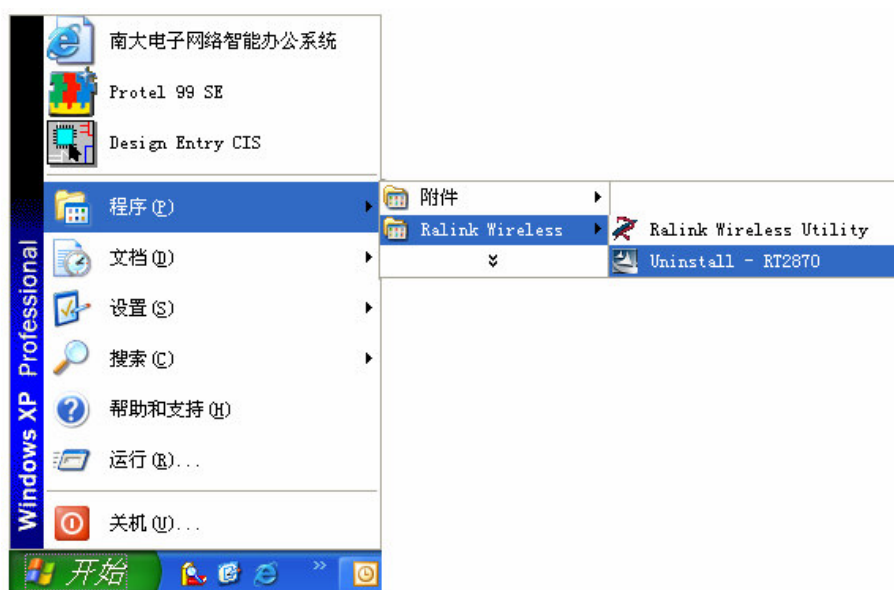
Figure 2-8 uninstall utility

2. ①. On the Windows taskbar, click the **Start button**, point to **Settings**, and then click **Control Panel**.

②. Double-click the **System** icon, click on the **Hardware** tab in the System window.

③. Click on the **Device Manager** button, double-click **Network Adapters**, and then right-click **802.11 USB Wireless LAN Card**.

④. Click **Uninstall**..., shown in above *Figure 2-9*, the system will uninstall the driver software of the WLAN USB Adapter from you PC.

2.3.2 Uninstall the utility software from your PC

1. On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**

2. Double-click the **Add/Remove Programs** icon, find the WLC311NRM program from the installed program list, highlight it and click the **Remove** button.

3. Following the Install Shield Wizard will uninstall the utility software from your PC.
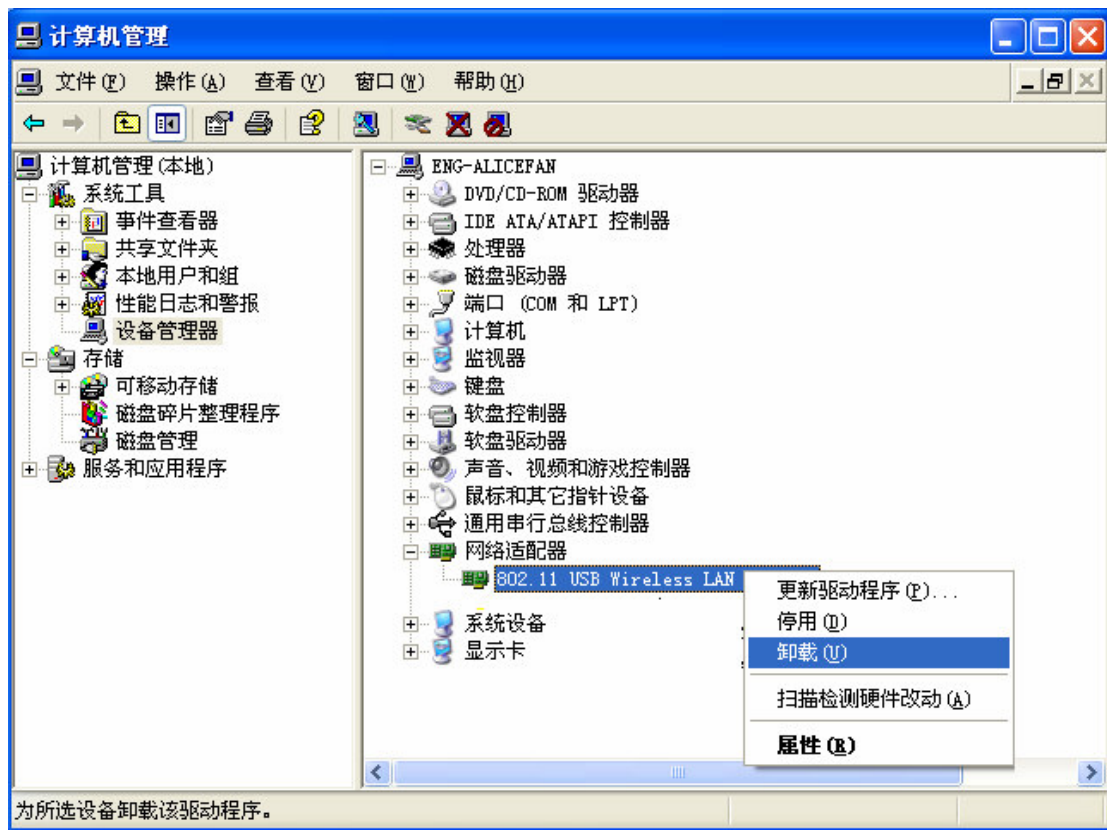
Figure 2-9 uninstall driver

Chapter 3: Connect to Wireless Access Point

This section shows you how to configure the WLC311NRM WLAN USB Adapter in order to getting connection to a wireless access point. There are two kinds of ways that you can carry out this task:

- Using **Ralink Configuration Utility** to connect the wireless access point.

- Using Windows built-in **Windows Zero Configuration Utility** to connect the wireless access point.

3.1 Using Ralink Configuration Utility
Below instructions show you how connect to the wireless access point using Ralink Configuration Utility:
1. Right-click the Ralink configuration utility icon located at low-right corner of your PC, click **Launch Config Utilities**, *Figure 2-7* will appear.

2. To add a new connection profile, you can either

- **Create a new profile** or

- **Modify a profile from an existing wireless access point or wireless device**.

Figure3-1 Profile setting

a. To create a new profile, please click the tab **Profile** as *Figure 3-1*, and select the button **Add** and then **Edit** to create and edit new profile:

● **Profile Name** - Up to 32 alphanumerical characters and symbols, space is not allowed in this field.

● **SSID** - The SSID of the wireless access point or wireless device you selected will be displayed here. In case the SSID of access point or wireless device is not available, you are requested to input the SSID manually.

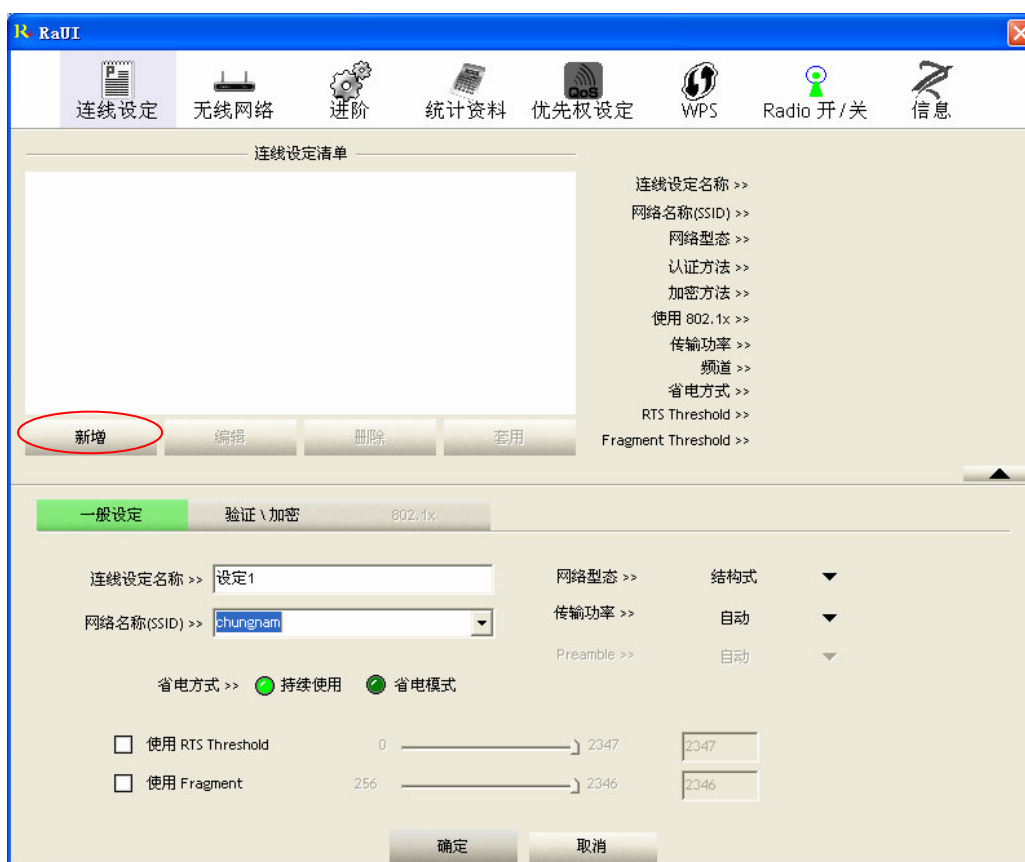● **PSM** - Please select CAM (constantly Awake Mode) in case you want to keep the wireless radio activity even if there is no data transfer.   Or you can select the PSM (Power Saving Mode) while the radio activity will be switched off when there is no data transfer.   It's recommended to choose 'PSM' if you're using this WLAN card with notebook computer in order to save the battery power.

● **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

● **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** - 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
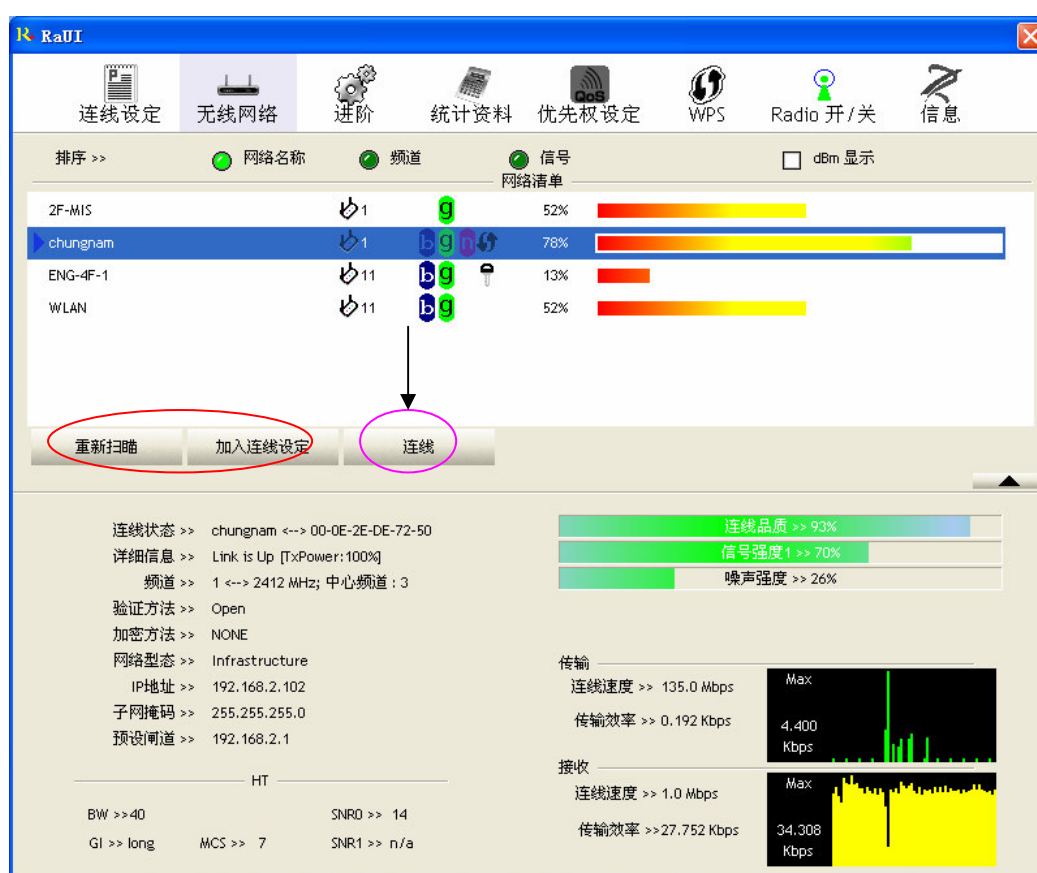
Figure 3-2 the status of Congratulations

b. You can also add a connection to the wireless access point or wireless by clicking the tab **Network**, and select the button **Rescan** as *Figure 3-2* to find the wireless access point with the SSID (the name of wireless access point) that we can be used, and please select the best which you wanted to get connection, and click the button **Add to profile** and **Connect** to setting which you selected SSID and connect it.

● **SSID** - Service Set IDentifier is the identity of wireless access point.　You can think SSID is the name of access point.

● **Channel** - Shows the channel number that access point or wireless device being used.

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

3. You can also to set the encryption and authentication settings when you click the tab **Auth.\ Encry** as *Figure 3-3*.

Figure 3-3 setting for Auth.\ Encry

● *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 click the button **Show Password** 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, 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

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

4. If the wireless access point uses encryption, please setting in the dialog box as *Figure 3-3,* 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**.

5. Open the tab **Advanced** as *Figure 3-4*, you can set some advanced setting in here.
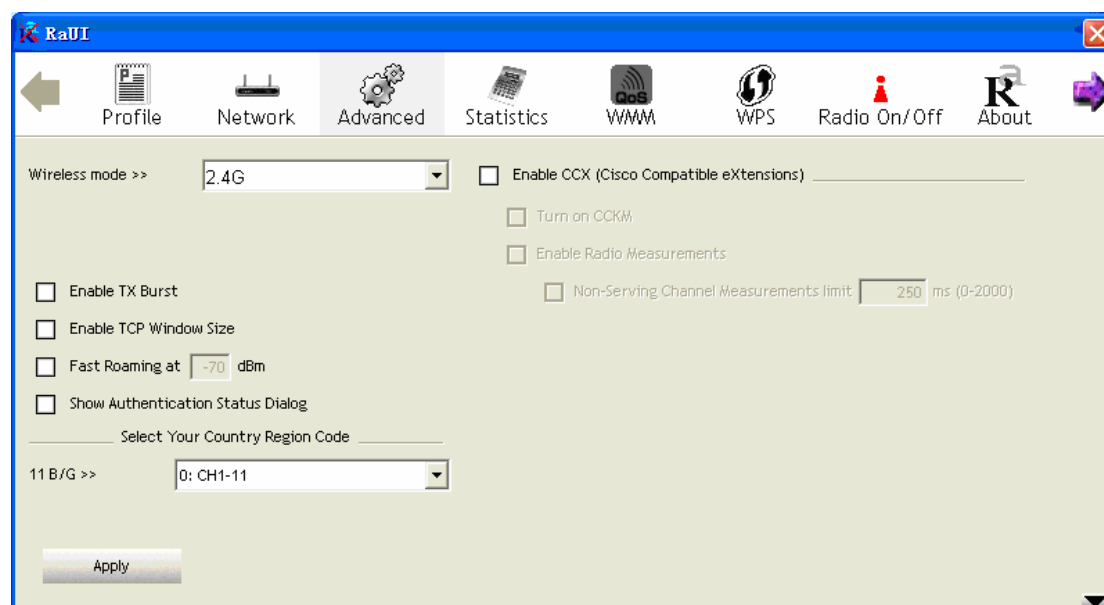
Figure 3-4 The setting for Advanced

● **Wireless mode** - Select wireless operation mode, available options are 2.4G.

● **Enable 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.

● **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 Measurements -** 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 the time used for said measurement to a certain time. Default value is 250.

6. Open the tab **Statistic** as the *Figure 3-5 Statistics of transmit and receive*, you can click **Reset Counter** to reset the statistics of all items back to 0. Click **OK** to close the window.

● **Transmit** – To appear the Statistic of the frames transmitted successfully, frames retransmitted successfully, frames fail to receive ACK after all retries RTS frames successfully receive CTS and RTS frames fail to receive CTS.

● **Receive** – To display the statistic of frames received successfully, frames received with CRC error, frames dropped due to out-of-resource and duplicate frames received.

● **Reset Counter** – Reset the statistics of all items.
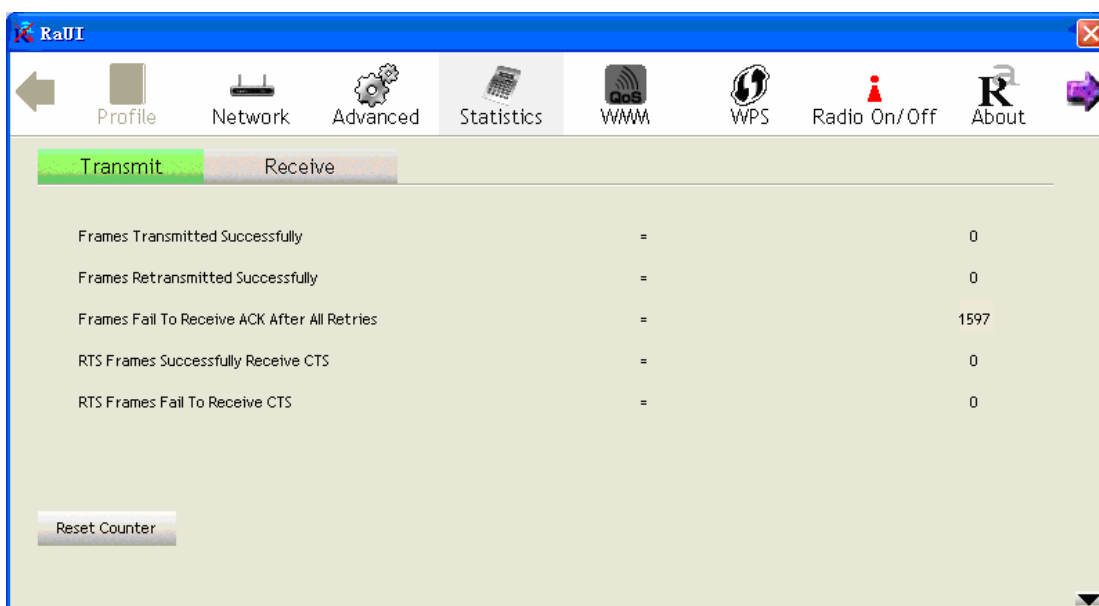
Figure 3-5 Statistics of transmit and receive

7. The functions of **WMM**, **WPS** and **Radio On/Off** are:
WMM -> Display the WMM setup status
WPS -> WPS functional and parameter setting parameter
Radio On/Off -> Button to turn ON/OFF the WLAN USB Adapter.

8. Open the tab **About** as the *Figure 3-6*, the tab provides you the information about version numbers of configuration utility, firmware, and other important information about your wireless network card.

Figure 3-6 The information of configuration utility

3.2 Using Windows Zero Configuration

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

1. Right-click Ralink configuration utility icon as the *Figure 3-8* and select **Use Zero Configuration as Configuration utility**.

Figure3-7 select WZC to configure your wireless network

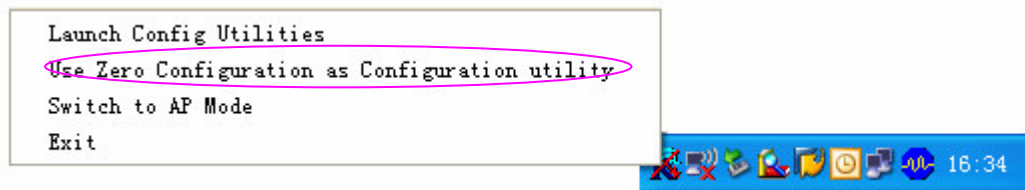2. Click the button **Start** (should be located at the bottom-left corner of windows desktop), select **Start -> Control Panel -> Network and Internet Connections** -> **network Connection**

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

Figure 3-8 Setting for wireless Network Connection

4. 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**.
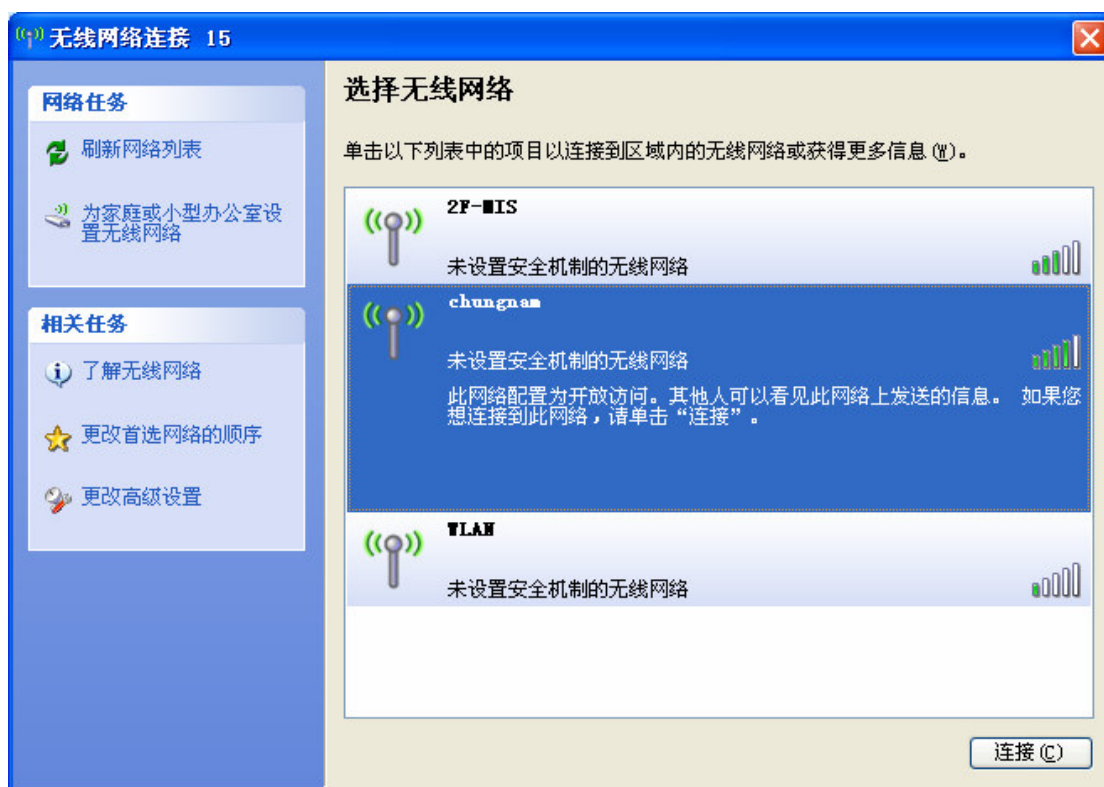
Figure3-9 Choose a wireless network to connect

5. 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.

Figure 3-10 setting for security key or passphrase

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

Chapter 4: Regulatory information

4.1 FCC Information to User

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.

4.2 FCC Guidelines for Human Exposure

FCC RF exposure statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements please follow operation instructions as document in this manual.

This device has been tested for compliance with FCC RF Exposure (SAR) limits in the typical laptop computer configuration and this device can be used in desktop or laptop computers with USB slots. Other applications like handheld PDAs (personal digital assistants) or similar device has not been verified and may not compliance with related RF exposure rule and such use should be prohibited. This device with its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.

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.

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.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Chapter 5: Technical Specifications

Appendix A: Specifications

Standards	IEEE802.11b, 802.11g and , 802.11n Draft

Operating Frequency	USA (FCC):
	       2.412GHz ~ 2.462GHz ISM band (channel 1 ~ 11)
	Europe (CE):
	       2.412GHz ~ 2.472GHz ISM band (channel 1 ~ 13)

Channel Bandwidth	20/40MHz
Protocols	802.11b: CCK, QPSK, BPSK 802.11g: OFDM Draft-11n: BPSK, QPSK, 16-QAM, 64-QAM
Antenna	PCB Antenna
Security	WPA/WP2, 64/128/152-bit WEP, WPS
Transmit Output Power	11b: 16±1.5dBm @ 11Mbps 11g: 14±1.5dBm @ 54Mbps 11n: 14±2dBm
Receive Sensitivity	11b: -82dBm @ 11Mbps (Typical) 11g: -68dBm @ 54Mpbs (Typical) 11n: -68dBm (Typical)
Operating Voltage	5.0V DC ± 5%
Power On/Off	External On/Off switch support (for PCBA only)
Bus Interface	A-type USB 2.0 Connector or 4 pin Jumper
Antenna Port Impedance	50ohm

Appendix B: Glossary

* **802.11b -** The 802.11b standard specifies a wireless product networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

* **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

* **Ad-hoc Network -** An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

* **DSSS** (**D**irect-**S**equence **S**pread **S**pectrum) **-** DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

* **FHSS** (**F**requency **H**opping **S**pread **S**pectrum) **-** FHSS continuously changes (hops) the
carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.

* **Infrastructure Network -** An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

* **Spread Spectrum -** Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications 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).

* **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless LAN card for an embedded system. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

* **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

* **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

* **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

* **WPA** (**W**i-Fi **P**rotected **A**ccess) **-** A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

THE END