Micronet
Making Communication Easier

User's Manual

11n Wireless LAN USB Adapter

Model No.: SP907NL

http://www.micronet.info

Table of Contents

Chapter 1 Introduction

Micronet SP907NL, 11N Wireless LAN USB Adapter, delivers next generation high speed at a more economical and affordable price tag. It is easily implemented for medium-sized business to allow immediate access to high speed wireless experience. It is compliant with IEEE 802.11n and backward compatible with IEEE 802.11b/g. The USB adapter supports MIMO (Multi-In, Multi-Out) technology, which uses 1T1R (1 transceiver, 1 receiver) to enhance data rate and wireless coverage. It is the part of the complete package of the new 11n high speed wireless solution. Ideal installation is for both desktop computer and notebook with USB 2.0/1.1 port.

1.1   Package Contents

Prior to the installation of the device, please verify the following items are in the package:

- SP907NL 11n WLAN USB Adapter
- Quick Installation Guide
- Manual CD

Note: Contact your dealer immediately if any of the above items are missing, damaged, or if the unit does not work.

1.2   Key Features

- High-efficiency antenna expands the scope of your wireless network.
- High-speed data transfer rate of up to 150Mbps.
- QoS function: control the bandwidth required for different applications.
- Compatible with 802.11b/g/n wireless networks.
- Supports major encryption methods like WEP, WPA, and WPA2 encryption.

1

- WPS configuration for easier connection between adapter and AP/router. Enable connection via pushing a button or entering an 8-digit code.
- Support the commonly available interface USB 2.0 to allow convenient installation.

1.3   Safety Information

In order to keep the safety of users, please read through the following safety instructions:

- This USB Adapter is designed for indoor use only.
- Do not put this device at or near hot or humid places. Also, do not leave this device in the car in summer.
- The USB Adapter is small enough to put in a child's mouth, ear, or nose, and it could cause serious or fatal injury.
- There's no user-serviceable part for the device. If users found the device is not working properly, please contact the authorized dealer of purchase. Do not disassemble the device, otherwise warranty will be void.
- If the device falls into water, do not use it again before sending to the dealer of purchase for inspection.
- If users smell something strange, or even see some smoke coming out from the network card, remove the power supply or switch the electrical power off immediately, and call authorized for help.

## 1.4   System Requirements

- An empty USB 2.0 port (USB 1.1 will degrade the performance dramatically).
- Windows 2000, 2003, XP, or Vista operating system.
- CD-ROM drive.
- At least 100MB of available disk space.

1.5   Specifications

Standards	IEEE802.11b/ 802.11g / 802.11n
Interface	USB 2.0/1.1
Frequency Band	2.4000 ~ 2.4835GHz
Data Rate	• 11b: 1/2/5.5/11Mbps • 11g: 6/9/12/24/36/48/54Mbps • 11n (20MHz): MCS0-7 (up to 72Mbps) • 11n (40MHz): MCS0-7 (up to 150Mbps)
Output Power	• 11n: 14dBm±1.5dBm • 11g: 14dBm±1.5dBm • 11b: 17dBm±1.5dBm
Security	• WEP 64/128-bit • WPA & WPA2 • Cisco CCX Support
LED Indicators	Link /Activity
Antenna	Internal Antenna
MIMO Technology	1T1R MIMO Technology
Humidity	10~95% (Non-Condensing)
Temperature	32~104°F (0 ~ 40°C)
Operating System	Windows 2000/XP/2003/Vista
Emission	FCC, CE

3

Chapter 2   Tour of Product

2.1   USB Adapter
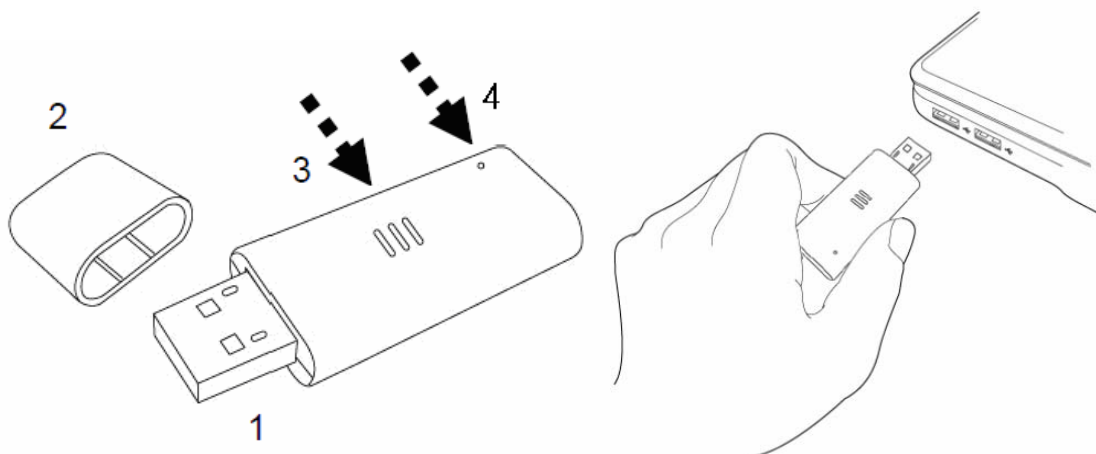
1. **USB Connector:** insert this side of the device into an available USB slot.
2. **Connector Cab:** for protecting device when not in use.
3. **WPS button:** located on the bottom side of the device for activating WPS pairing mode.
4. **Link/Activity LED:** indicate device is in use or traffic activity is evident.

2.1.1 LED Indication

| LED	Status	Operation
Link/Activity	On	Successful connection to AP or Router
	Flashing	Transmitting data to AP or Router
	Off	No link to AP or Router/ WLAN function is disabled

4

Chapter 3 Configuration

3.1 Drivers Installation

Step 1. Gently insert the USB adapter into an available USB slot. The following message will appear, please press **<Cancel>**.

Step 2. Insert driver CD into the CD/DVD ROM drive of the computer, and execute 'Setup.exe' program in 'Utility' folder. Read through the License Agreement and select 'I accept the terms of the license agreement' then press **<Next>** to proceed.

5
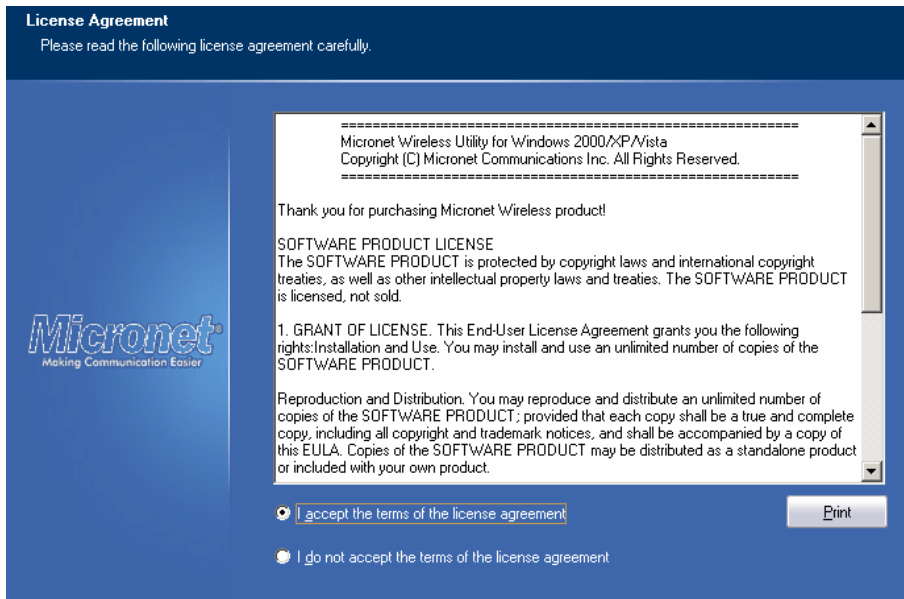
Step 3. It is recommended to select 'Install driver and Ralink WALN Utility' for first-time installation. Otherwise select second option to update existing drivers.
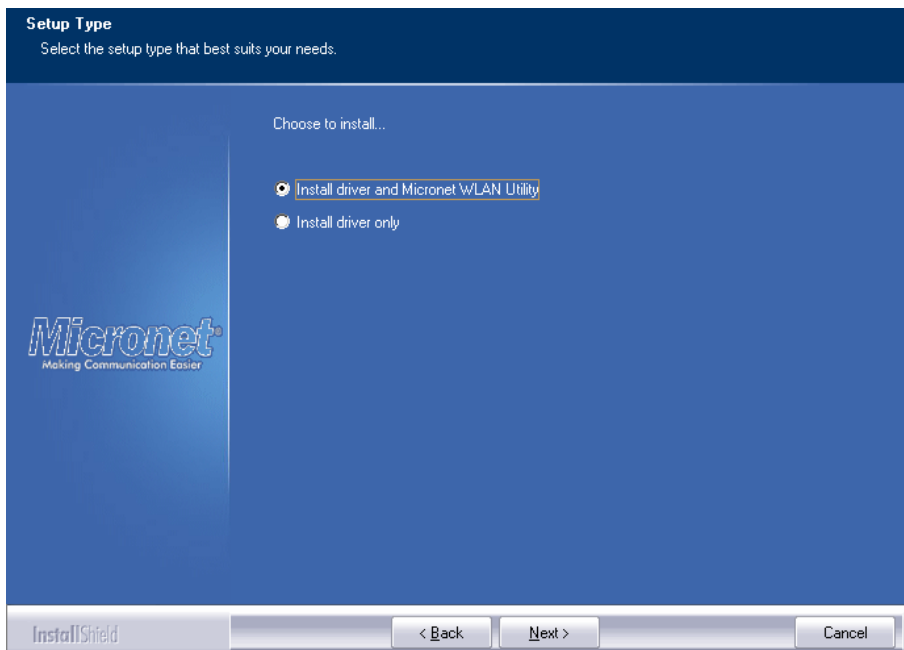
Step 4. The following windows will appear, please press on 'Install' to start the process.
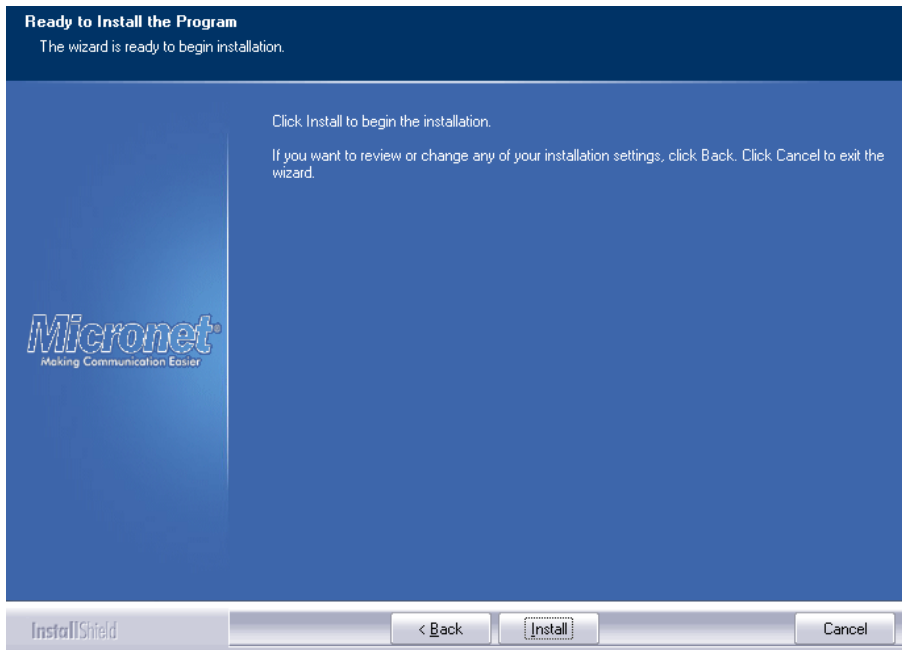
Step 5. Click **<Finish>** to complete the driver installation process.
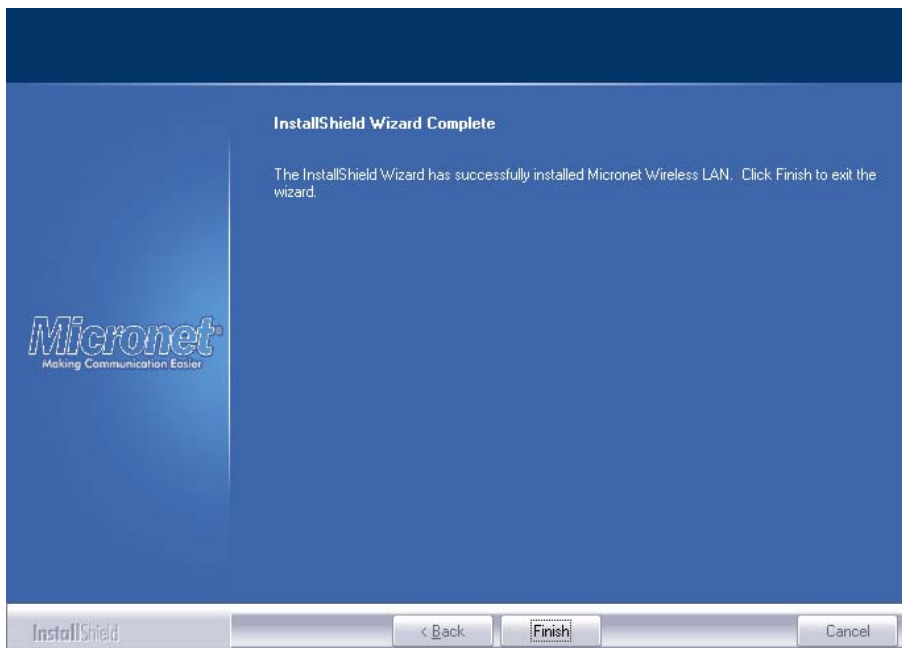
3.2　Operating Configuration Utility

After installation is complete, wireless configuration utility will be shown as an icon at the lower-right corner of the windows desktop. Click on the icon using right mouse key and select **<Launch Config Utilities>.**

Step 1. Configuration utility will scan for available wireless access points automatically. Please select an access point to connect, and click **<Connect>**. If the AP you wish to connect is not in the list, please press **<Rescan>** to renew the interface.
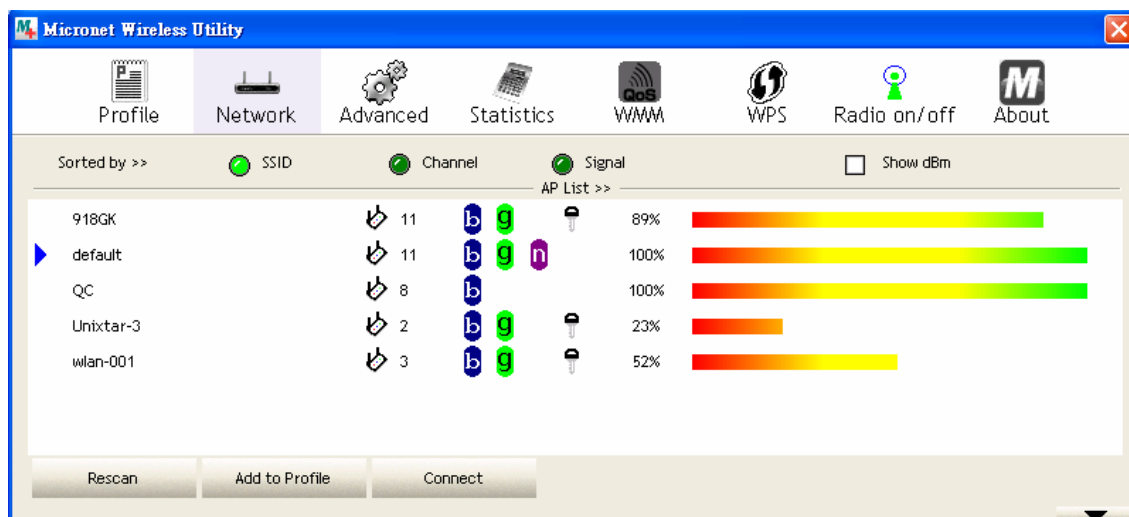
Some function includes more information, and can not be fitted in setup area. In this case, you can click 'More / less' button to expand the setup utility window, to display more information:

8
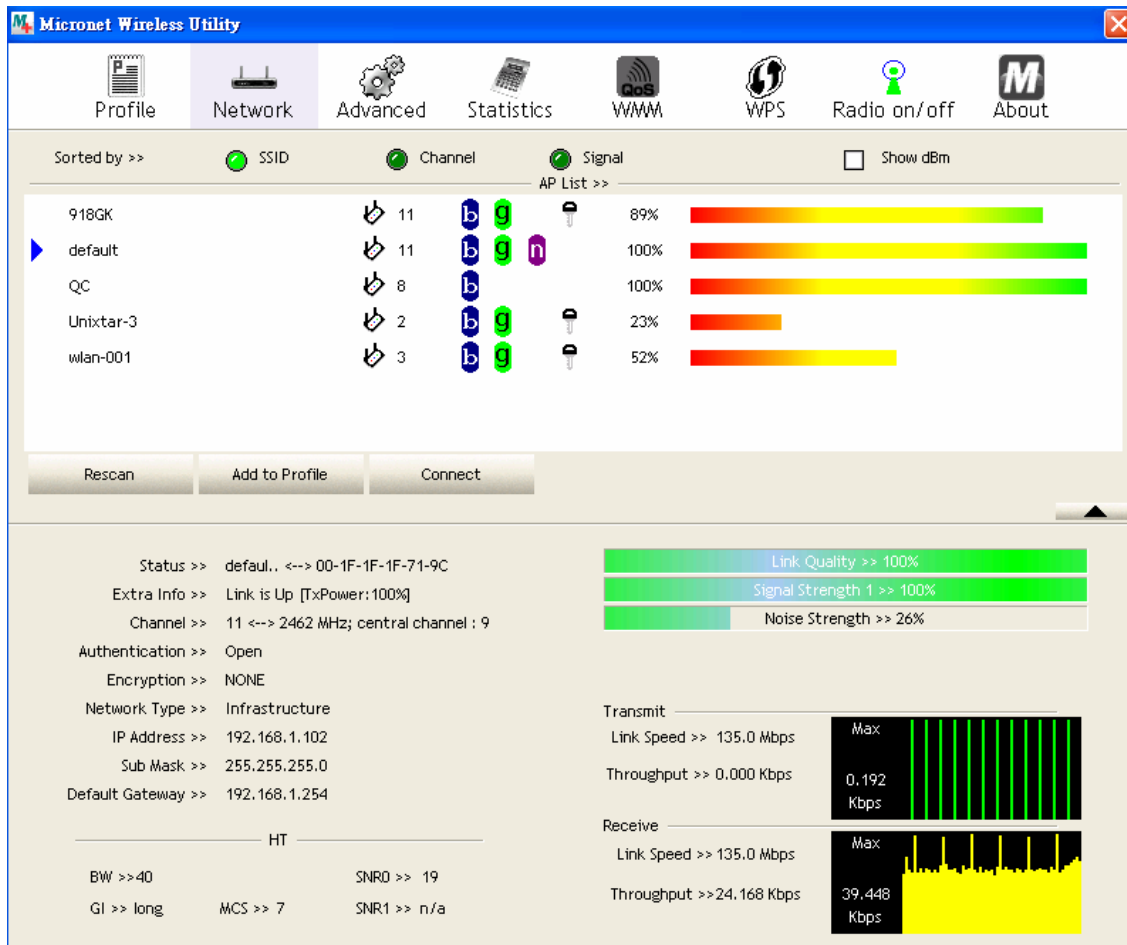
3.2.1 Scan for Other Wireless Devices

There are two kinds of wireless connection mode: Infrastructure and Ad-Hoc. Infrastructure mode is used by wireless access points, which is able to establish wireless connection for you and other wireless/wired network clients. Ad-Hoc mode is also know as 'point-to-point' mode, and in this mode, wireless devices such as computer or PDA will not be capable to establish wireless connection with more than one wireless device, and is suitable for establishing a one-to-one wireless connection between two wireless devices. Before connecting to any wireless access point or device by infrastructure or Ad-Hoc mode, there are two issues to be aware of:

- Wireless device's 'SSID' (Service Set Identifier). Users can scan for the SSID of other wireless devices nearby, but if the SSID of the wireless device is hidden, it is necessary to know exact SSID before establishing the connection.

9

- If the wireless device uses encryption, the user must know its encryption key in order to connect.

Please launch utility and it will scan for wireless access points near by:

Parameter	Description
SSID	The SSID of the wireless access point or wireless device selected by user will be displayed here. When the SSID of access point or wireless device is not available, users have to input it here manually.
▶	If symbol appears in front of the name of wireless device, it means the user has established connection with that wireless device.
ᵇ3	It shows the connection type and channel number of this wireless device. : Wireless device is an access point. : Wireless device is a computer (Ad-Hoc mode for point-to-point connection).
b g n	The wireless standard supported by this access point is displayed here. : WPS icon will appear when the access point supports WPS. : If the access point uses encryption, a key icon will appear. When the access point supports WPS and WPS will appear. User may not see the key icon, even through the access point uses encryption.

10

If users cannot see the access point, please click 'Rescan' button to scan for access point again, until the one preferred is displayed on the interface. Users may have to click 'Rescan' for more than two times before the access point wish to connect appears. If user still cannot see the access point after clicking 'Rescan' for more than five times, please move the computer closer to the wireless access point.

If users wish to see detailed information for a specific access point, please double-click on it, and detailed information will be provided.

Parameter	Description
General	Displays basic information about this access point, such as SSID, MAC Address, authentication / encryption type, channel etc.
WPS	If this access point supports WPS (Wi-Fi Protected Setup), related information will be displayed here.
CCX	If this access point supports CCX (Cisco Compatible eXtension), related information will be displayed here.
802.11n	If this access point complies with 802.11n draft, related information will be displayed here.
Sorted by >>	Users can decide how to sort all listed access point by 'SSID', 'Channel', or 'Signal' (signal strength).
Show dBm	Check this box to show the signal strength of access point, instead of percentage.
Rescan	Click this button to rescan access points. Users can click this button for several times, if the access point users wish to use does not show in the list.
Add to Profile	Users can store a specific access point to profile, so access point can be directly connected next time, without inputting authentication key again. To add an access point to profile, users have to select an access point from the list first, then click 'Add to Profile' button. Detailed instructions will be given below.
Connect	Connect to a selected access point. Users have to select an access point from the list first and then click 'Connect' to connect to the selected access point.

3.2.2 Connect to Access Point

If the wireless access point users wish to connect is found, it can establish connection by clicking on 'Connect' button. Instructions will be given as follow:
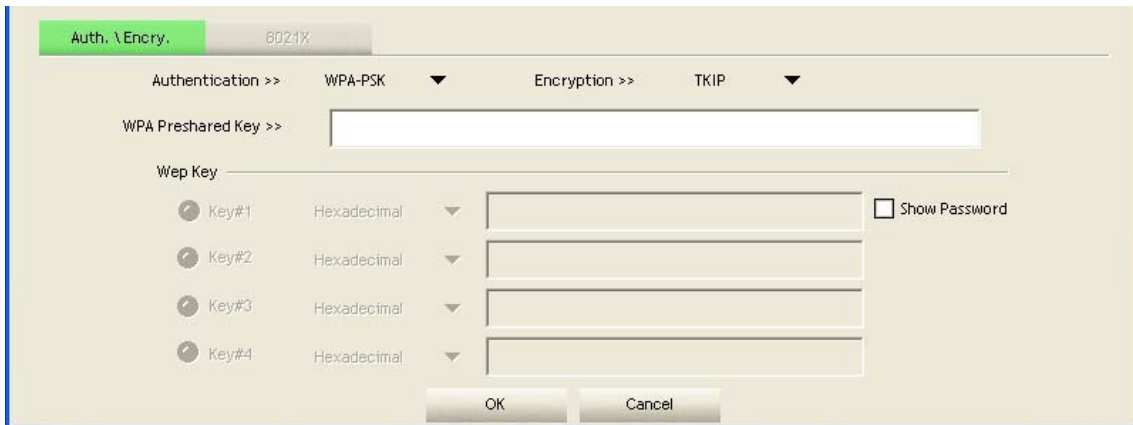
Step 1. Click the wireless access point or network device to connect, it will be highlighted, then click on 'Connect'.
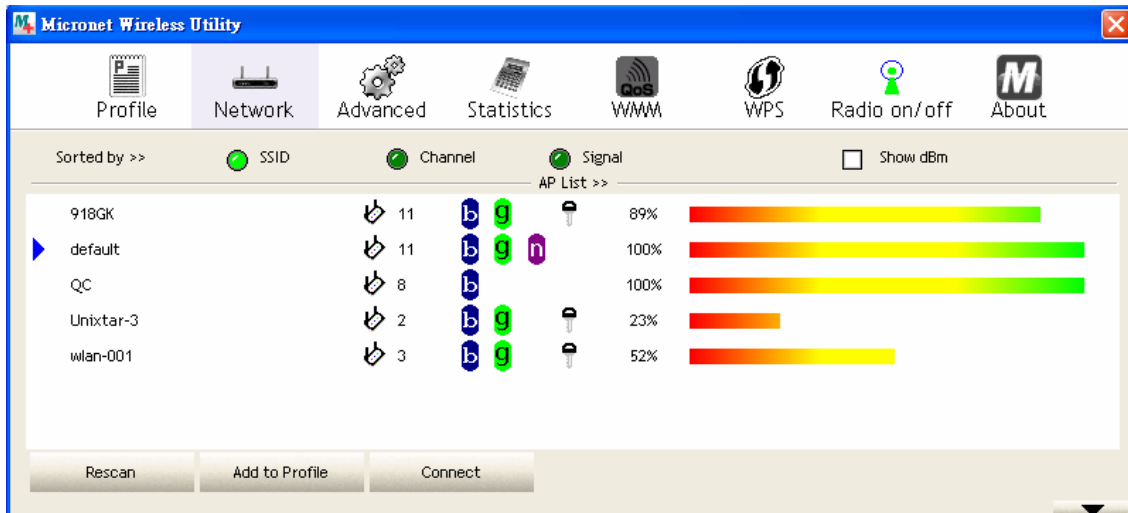
If the access point selected does not use encryption, it will connect to this device within one minute. If the access point selected uses encryption, please proceed to step 3.

Step 2. If the wireless access point does not have SSID, user will be prompted to input it in the field provided. Please ask the owner of wireless access point for the exact SSID to enter, and then click 'OK' when ready. If the SSID provided is wrong, user will be prevented to access the wireless device.

Step 3. If the wireless access point uses encryption, user will be prompted to input its WEP key or WPA preshared key.

12

Step 4. Please ask the owner of the wireless access point for the security information, and input the correct key here and then click on 'OK'. By checking 'Show Password' box, the encryption key inputted here will be displayed. Authentication type will be selected by the access point automatically, please do not change it.

However, if the user connecting to an access point uses 802.1x authentication, they will be required to check '802.1x' box and input related information.

Step 5. If the wireless access point is successfully connected, you'll see an icon appears in front of the name of wireless device.

13
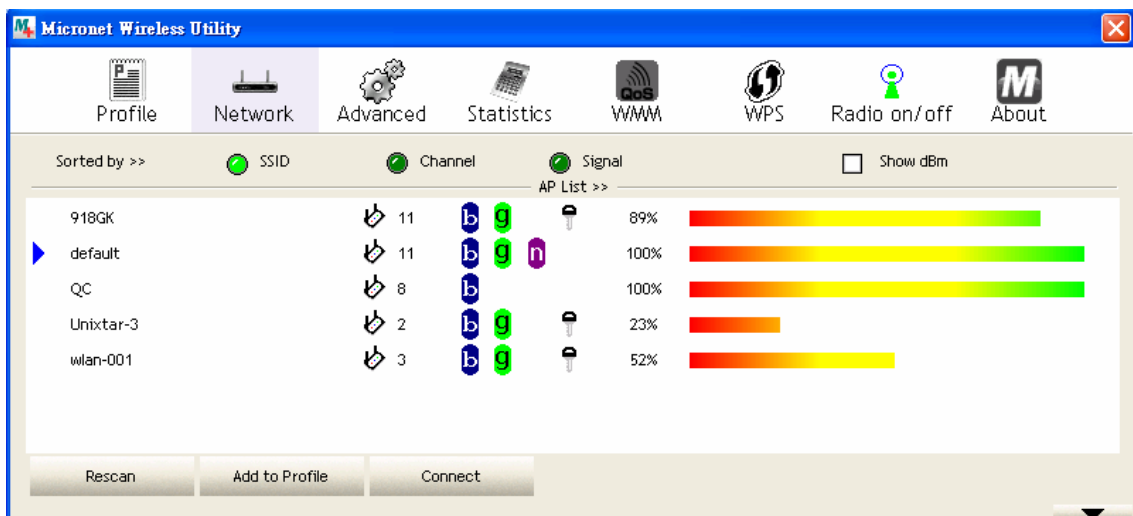
3.2.3 Add Access Point to Profile

If users connect to some specific wireless access point frequently, they can add their information to the profile. Just like the telephone directory, the profile saves all information of access points, and user can recall them anytime. User can add an access point in the 'Network' tab to profile, or input all information of an access point manually.

To add an access point in the 'Network' tab to profile, please select an access point first (make it highlighted), then click 'Add to Profile' button. To input the information of access point manually, please go to 'Profile' menu and click 'Add' button.

14

Parameter	Description
Profile Name	User can give this profile a name. Every profile needs a unique name.
SSID	Please input the SSID of this access point. If user selected an access point from the list, and SSID is not hidden, it will be filled automatically. However, user can modify the SSID if necessary.
Network Type	Please select the network type: Ad hoc or Infrastructure. If user is connecting to an access point, please select 'Infrastructure'. For point-to-point wireless connection (i.e. connecting to another computer using Ad Hoc mode), please select Ad hoc. If user selected an access point from the list above, please keep this field unchanged.
Tx Power	User can select the wireless output power here. If user is not too far from access point (good signal reception), it can select a lower output power to save energy. For a distant access point, user can select a higher output power. It's suggested to select 'Auto' to let setup utility decide the best output power.
Preamble	Select the preamble for Ad hoc mode here. Available options are 'Auto' and 'Long'. It's suggested to select 'Auto' to let setup utility decide the preamble.
Channel	User can select the radio channel number for AdHoc mode.
Power Save Mode	Please select CAM (constantly awake mode, keep wireless radio activity even when not transferring data), or PSM (Power saving mode, switches radio off when not transferring data). It's recommended to choose 'PSM' if user is using this network card with notebook computer to help the battery last longer.
RTS Threshold	Check this box to set the RTS threshold. User can drag the slider to set the threshold value, or input the value in the box located at right. It's recommended to keep this value untouched unless the users know the effect of changing this value.
Fragment Threshold	Check this box to set the packet fragment threshold. User can drag the slider to set the threshold value, or input the value in the box located at right. It's recommended to keep this value untouched unless users know the effect of changing this value.

15

Parameter	Description
Authentication	Select the authentication type of the wireless access point or wireless device in this field. When users are adding a profile from an existing access point or wireless device, authentication type will be selected automatically.
Encryption	Select the encryption type of the wireless access point or wireless device in this field. When users are adding a profile from an existing access point or wireless device, the encryption type will be selected automatically.
WPA Preshared Key	User can select key type (Hexadecimal or ASCII) and input WEP key in this field. If encryption is not enabled, or users select 'WPA' as encryption type, this field will be disabled and grayed out. User can set up to 4 WEP keys here. There are two types of WEP: Hexadecimal and ASCII. For Hexadecimal key, user can input number 0-9 and alphabet a-f (Eg. 001122aabbcc). For ASCII key, user can input number 0-9 and alphabet a-z (Eg. mywepkey12345). The length of WEP key depends on the type of WEP key selected. User can input 10 or 26 hexadecimal characters and 5 or 13 ASCII characters as WEP key.
Show Password	Check this box and all passphrases or security keys inputted will be displayed instead of replacing it with asterisk.
Use 802.1x	If the access point requires 802.1x authentication, please click on 'Use 802.1x' box, then click '802.1X' tab to set parameters.

To set 802.1x authentication for the access point, please click '802.1X' tab:

16

Parameter	Description
EAP Method	Select '802.1x EAP method' from dropdown menu. Please ask the administrator of the access point for the correct EAP method.
Tunnel Authentication	Select 802.1x tunnel authentication type from dropdown menu. Please ask the administrator of the access point for correct tunnel authentication method. This pull down menu is only available when authentication type is 'PEAP', 'TLS / Smart Card', or 'TTLS'. When users use 'EAP-FAST' as authentication type, the protocol setting is always 'Generic Token Card' and cannot be changed. Users also need to select 'Soft Token' or 'Static Password' as password in 'ID \ Password' setting.
ID \ Password Tab	Input 802.1x username/password and other information if it is required. Click 'Show Password' to show the password typed.
Client Certification Tab	Use this tab to select a local certificate from dropdown menu. If the access point requires a specific client certificate, the certificate must be installed on the client computer.
Server Certification Tab	Use this tab to use server-based certification. Please select a CA (Certificate Authority) from dropdown menu. If intermediate certificates are allowed, please select 'Allow intermediate certificates'. Also, if users need to specify CA server's name, they can specify it in 'Server name' field. User can select 'Server name must match' so the CA server's name must be the same with the value set in 'Server name' field. If only the domain name part of full server name needs to be the same value set in 'Server name' field, select 'Domain name must end in specified name'.

After you complete all information related to the access point, click 'OK' to save the profile, or click 'cancel' to stop the process.

3.2.4 Using Windows Zero Configuration

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

Step 1. Right-click on configuration utility icon and select **<Use Zero Configuration as Configuration utility>**.

Launch Config Utilities
Use Zero Configuration as Configuration utility
Exit
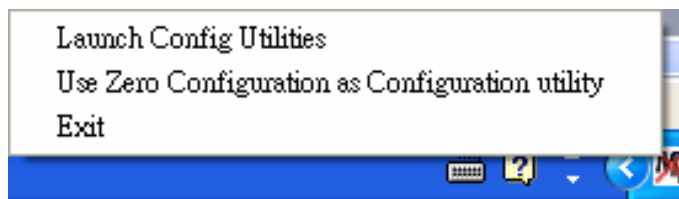
Step 2. Click **<Start>** button and **<Control Panel>**, then select **<Network and Internet Connections>**.

18
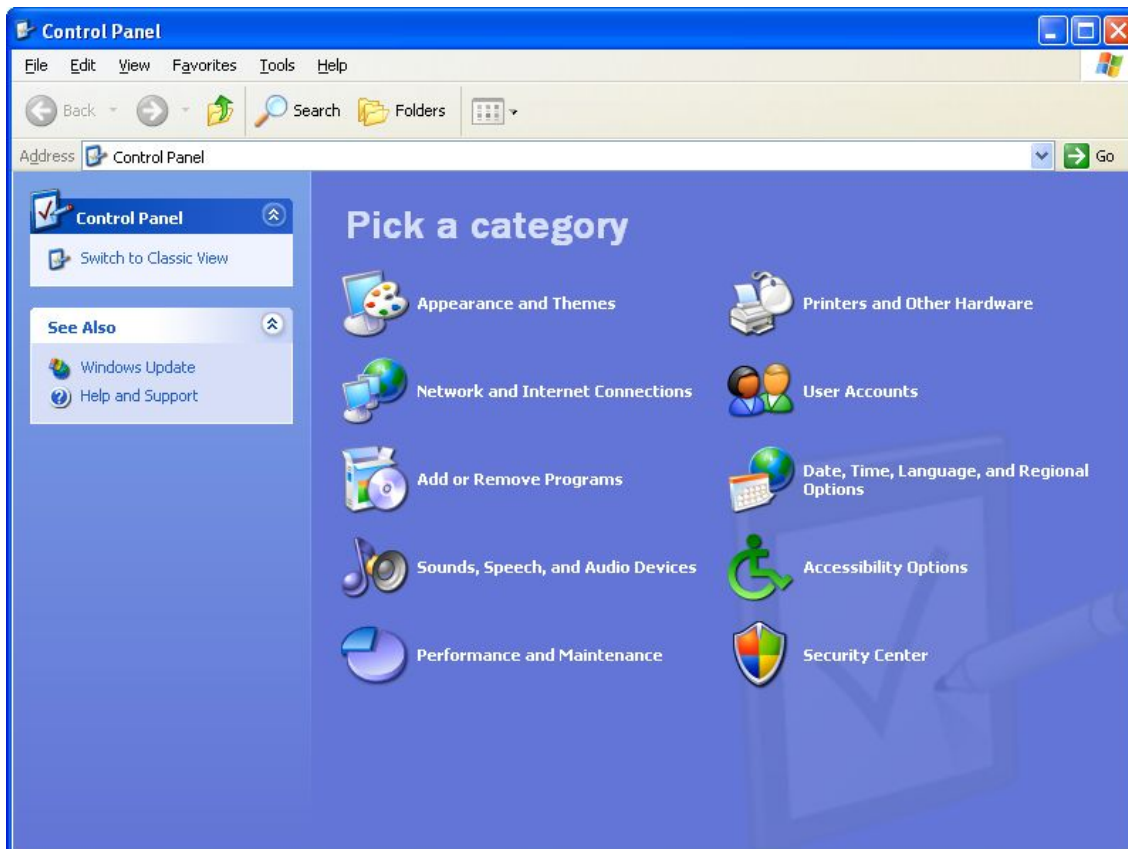
Step 3. Click **<Network Connections>**.
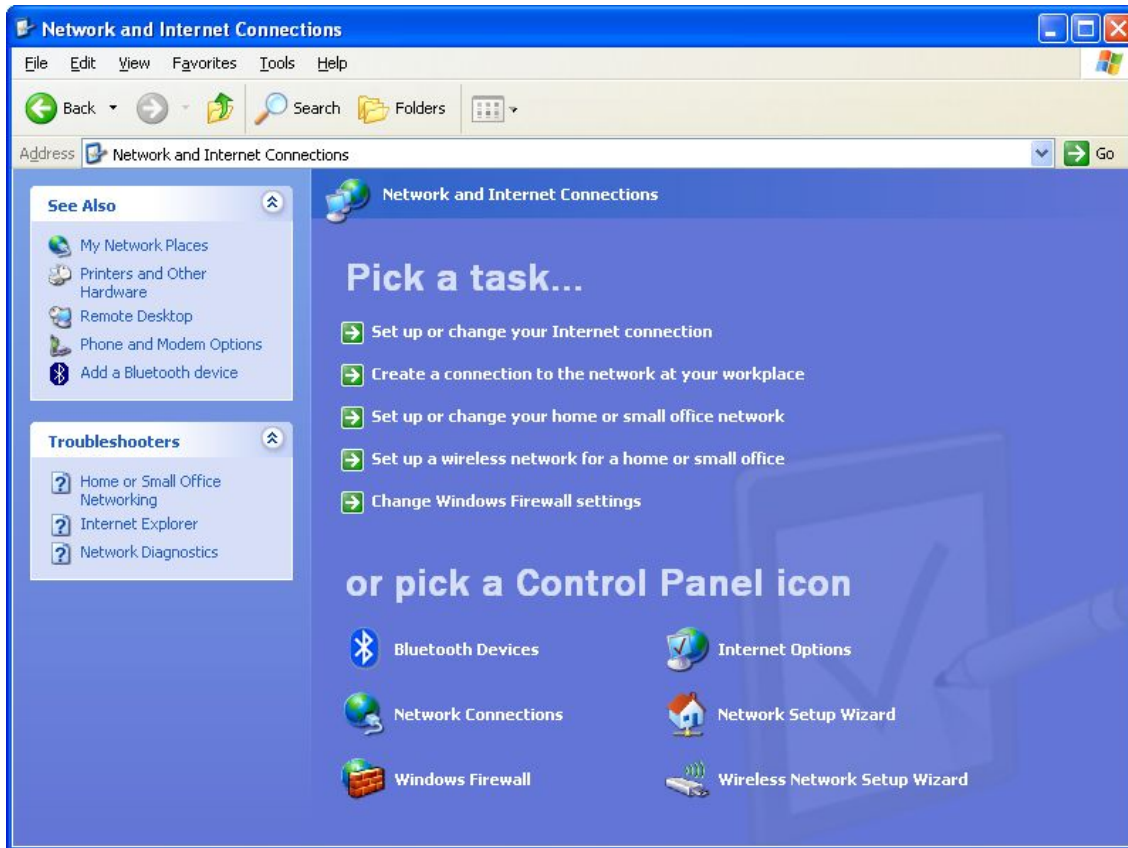
Step 4. Right-click 'Wireless Network Connection' (it may have a number as suffix if you have more than one wireless network card, please make sure you right-click the '802.11n Wireless LAN Card), then select 'View Available Wireless Networks'.

Step 5. All wireless access points within proximity will be displayed here. If the preferred access point is not displayed, please try to move the computer closer

19

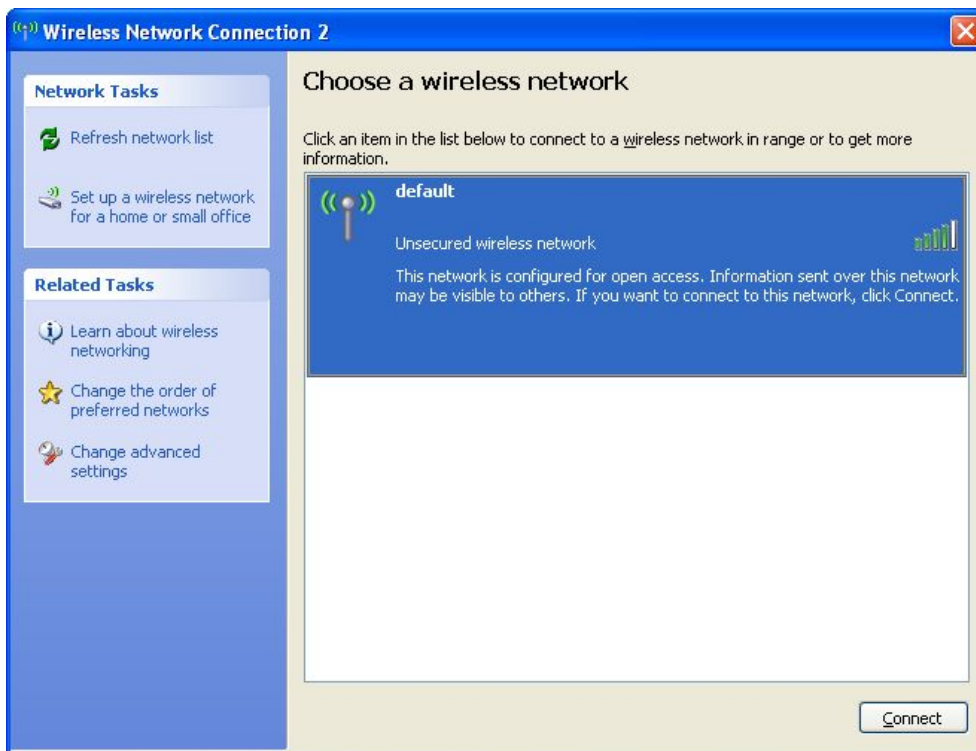to the access point. Otherwise, users can press refresh button to rescan access points. Select the access point if it's shown, then click **<Connect>**.

Step 6. If the wireless access point uses encryption, users will have to input the correct WEP passphrase or WPA pre-shared key. Ensure both the AP and PC is set with the same WEP passphrase/WPA pre-shared key. Otherwise the wireless connection will fail to establish.
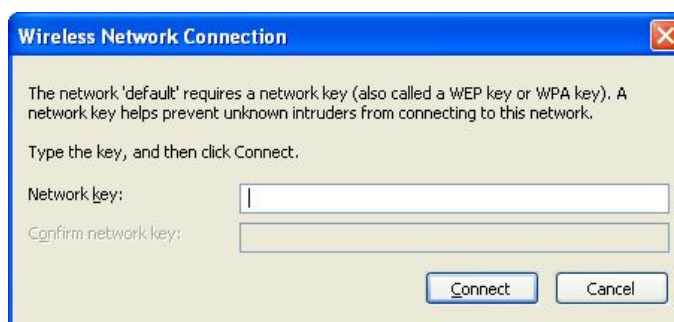
If the access point selected does not use encryption, users will not be prompted for security key or passphrase.

Step 7. If users can see this message, the connection between the computer and wireless access point is successfully established.

20
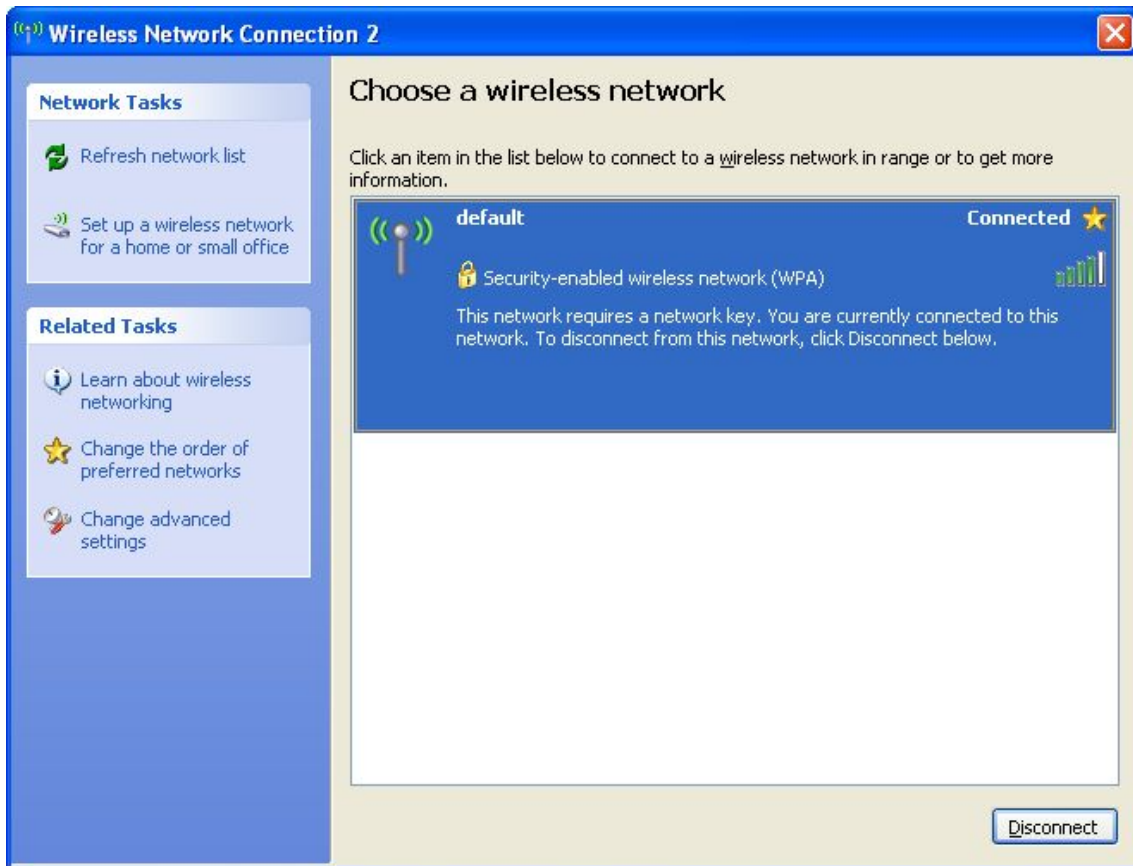
3.2.5 Profile Management

If users need to connect to different wireless access points at different time, they can store the connection parameters (encryption, passphrase, security etc, etc.) as a profile for every access point. Click the 'Profile' menu and all profiles will be listed in 'Profile List'. Users can select a profile from the list and all information about selected profile will be listed.

21
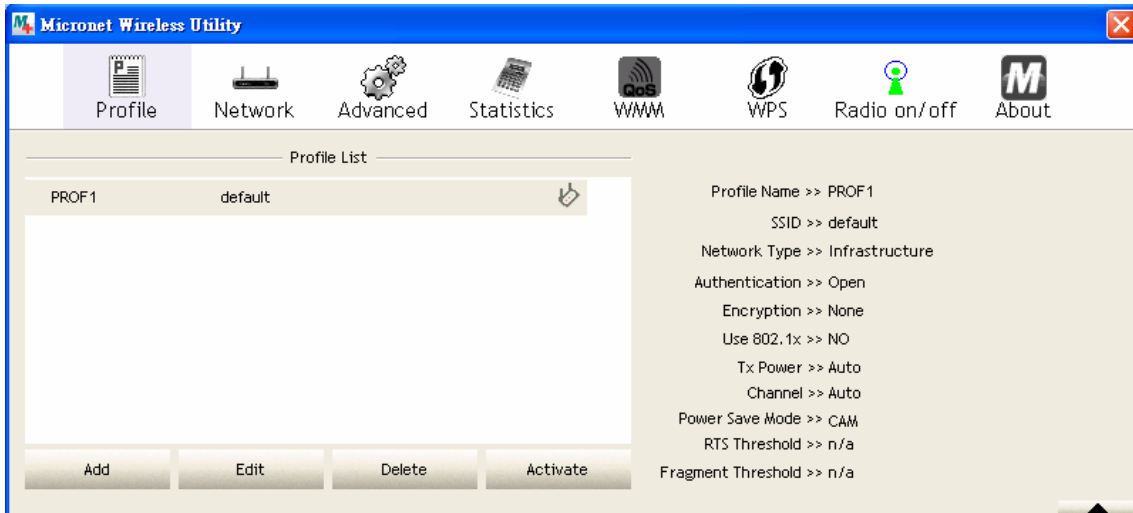
Add a Profile

If users want to create new profile, click 'Profile' menu, then press 'Add' button. The interface will prompt the user to input detailed information of access point.
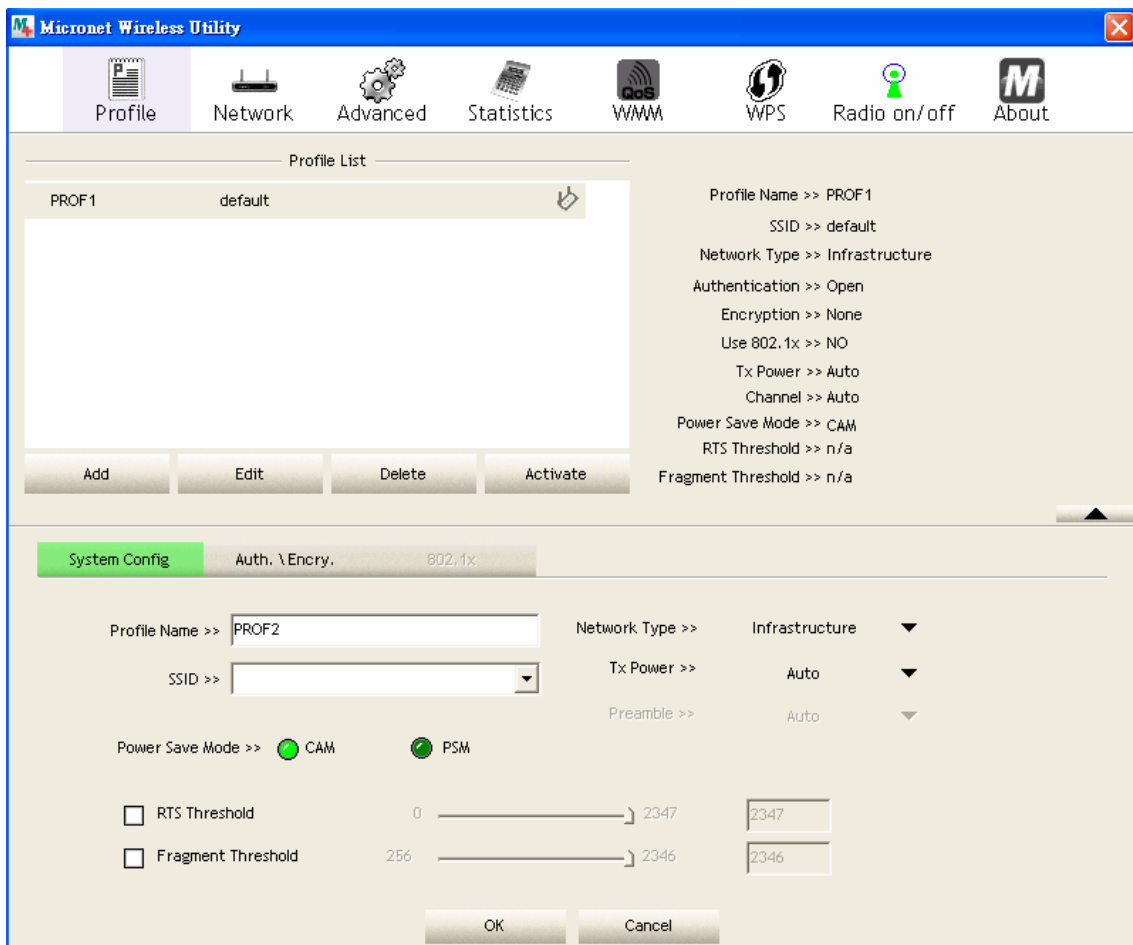
Edit a Profile

If users have added a profile before, and they wish to change the content of the profile, they can use this function. Please select a profile from the list, and then click on 'Edit' button. The interface will provide contents of selected profile for editing. Click on 'OK' to save changes, or click 'Cancel' to discard changes.
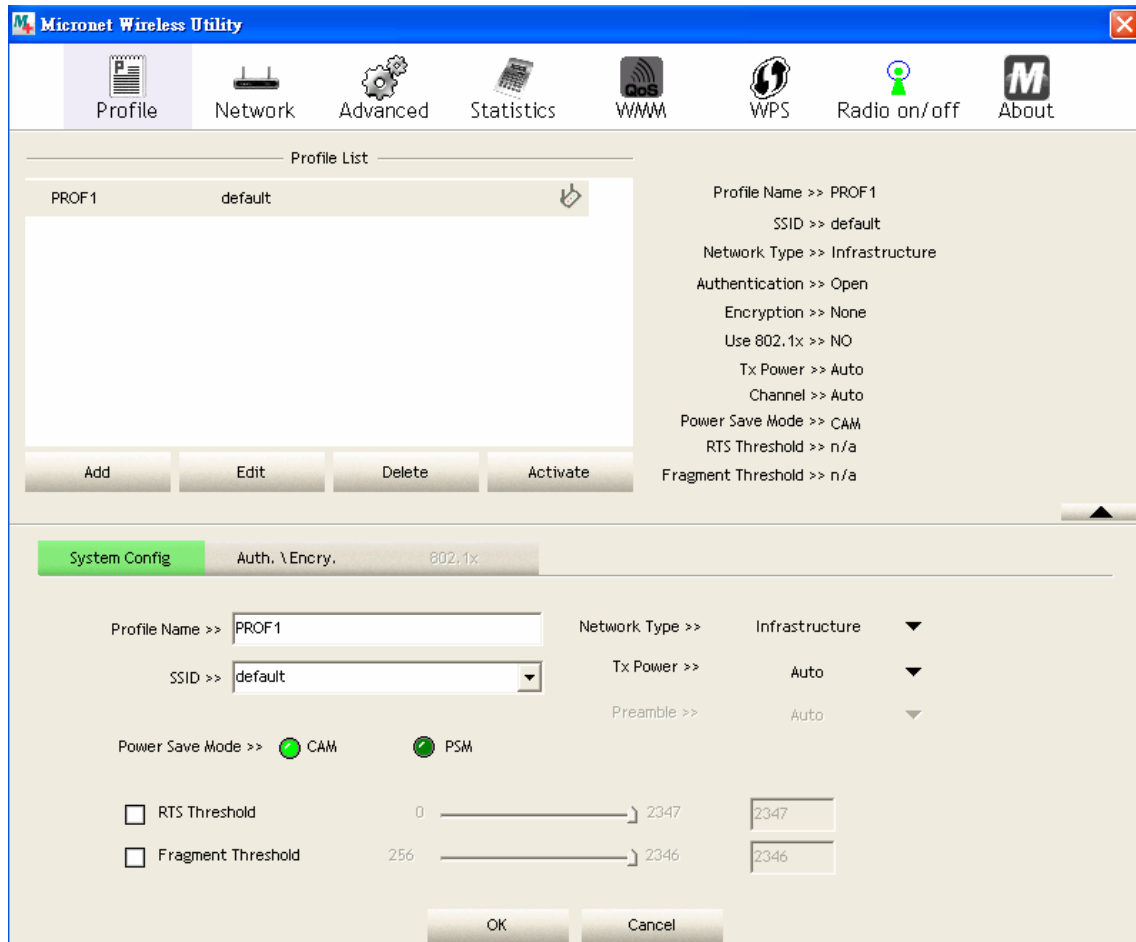
Delete an Existing Profile

If users no longer need a profile, they can delete it via this function. Select the profile to delete from the list, and click 'Delete' button to remove the entry.
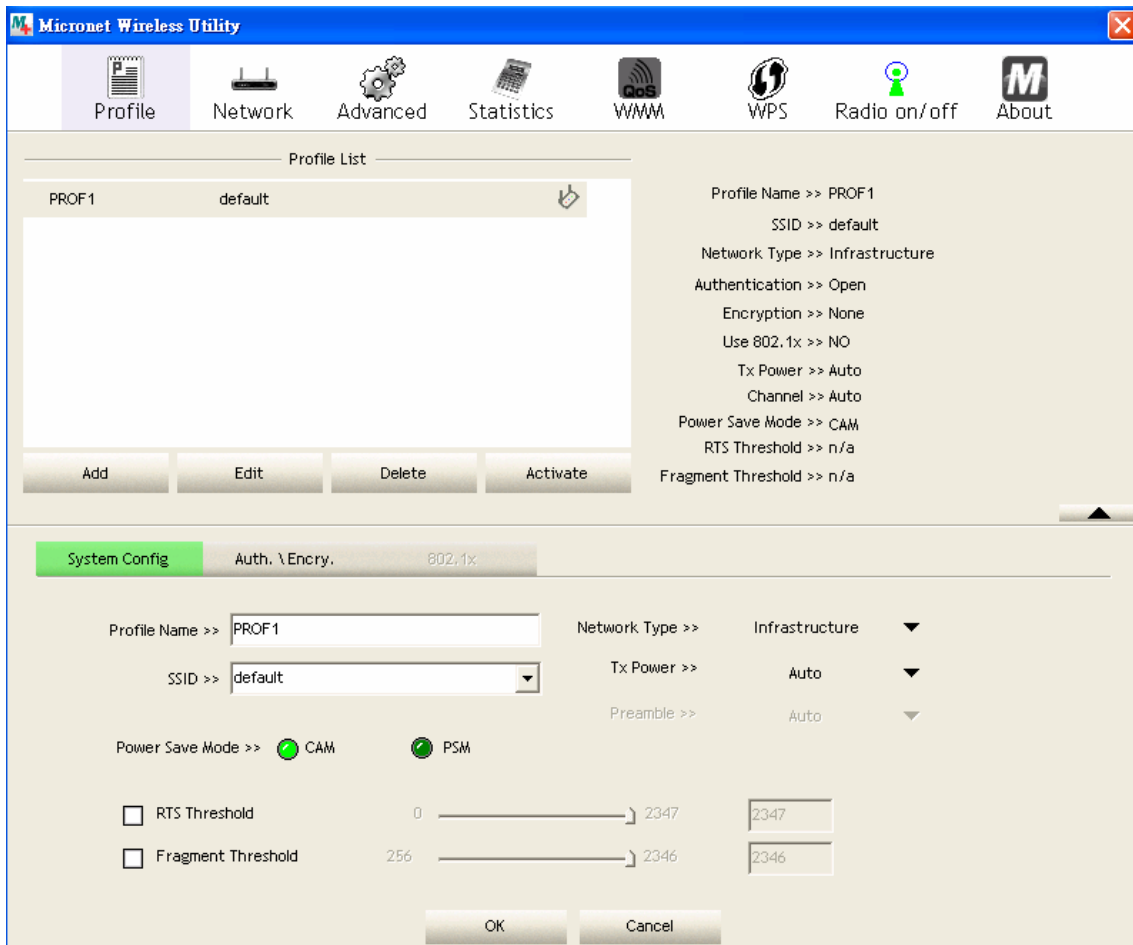
Activate a Profile

When users want to connect to a specific wireless device in the profile list, they can select it and click 'Activate' button to establish connection.
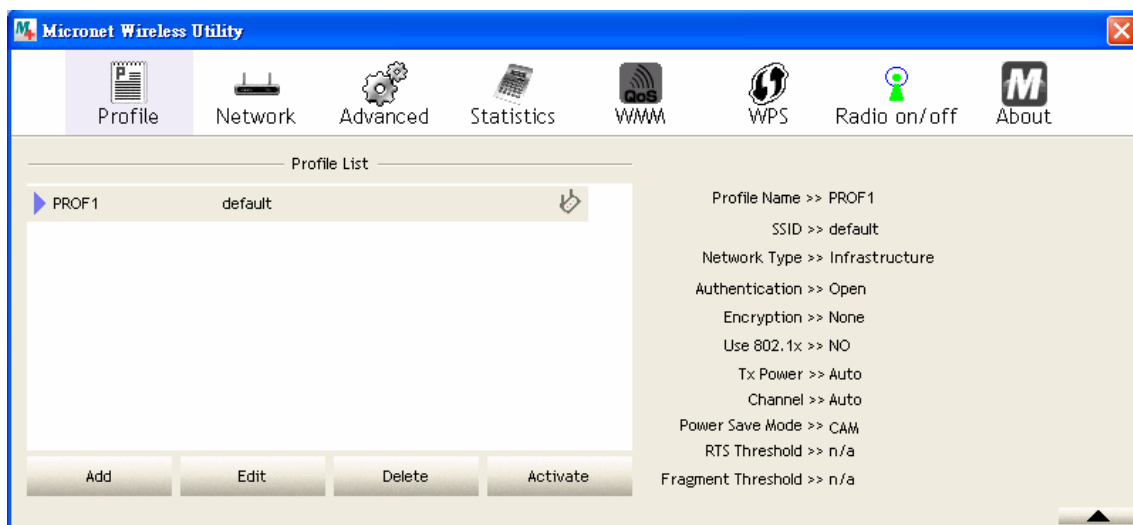
When a profile is selected and click on 'Activate' button, an ▶ icon will be displayed in front of the profile to show that the connection has failed. When the connection is successfully established, an ▶ icon will be displayed.

3.2.6 Advanced Settings

This wireless network card provides several advanced settings for experienced wireless users. Users can change these settings to increase data transfer performance or change operation mode. Please follow the following instructions to set advanced wireless settings.
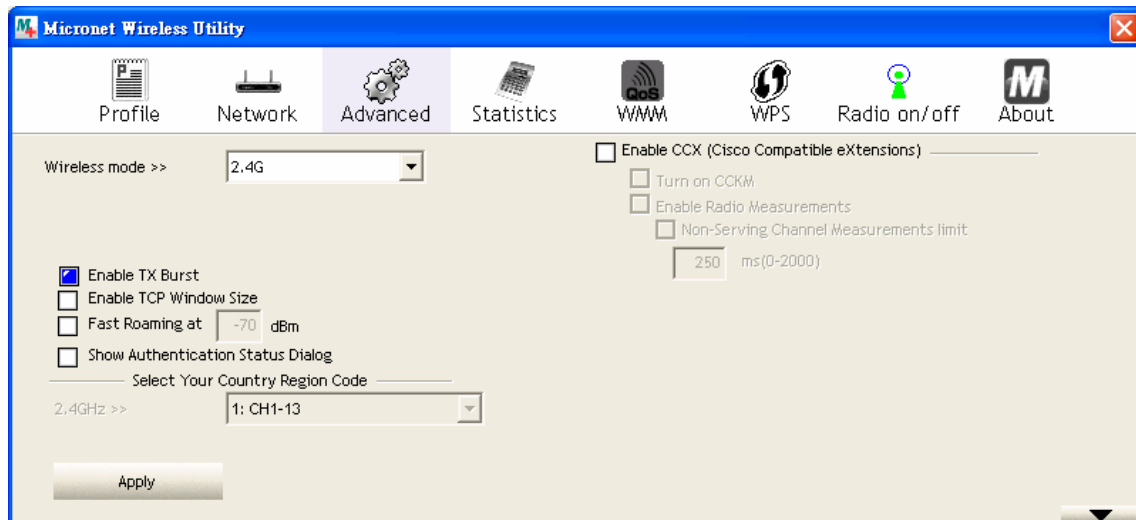
| Parameter	Description
Wireless mode	Display the wireless operation mode of the network card.
Enable Tx Burst	Check this box to accelerate the data transmit rate. It may not work with all wireless access point and wireless devices.
Enable TCP Window Size	Check this box and the configuration utility will adjust TCP window size automatically to get better performance.
Fast Roaming	Check this box to control the threshold for switching between the wireless network card and another access point with better signal quality. Only adjust value when the users need to roam between multiple access points.
Show Authentication Status Dialog	When the computer is being authenticated by wireless authentication server, a dialog window with the process of authentication will appear.

	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 the users need to connect to CCX-compatible wireless devices. When CCX is enabled, the following setup items will become available:
Enable CCX	➢ 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 connecting to CCX-compatible access point, check this box to enable radio measurement function to improve wireless connectivity. ➢ Non-Serving Channel Measurements Limit: When connecting to CCX-compatible access point, check this box to enable measurement on unused radio channels to improve wireless connectivity.

*Click **<Apply>** to save the changes.*

3.2.7 View Network Statistics

The configuration utility provides information about network statistics and link status. If users want to know how the wireless network card is working, use these functions to get detailed information.
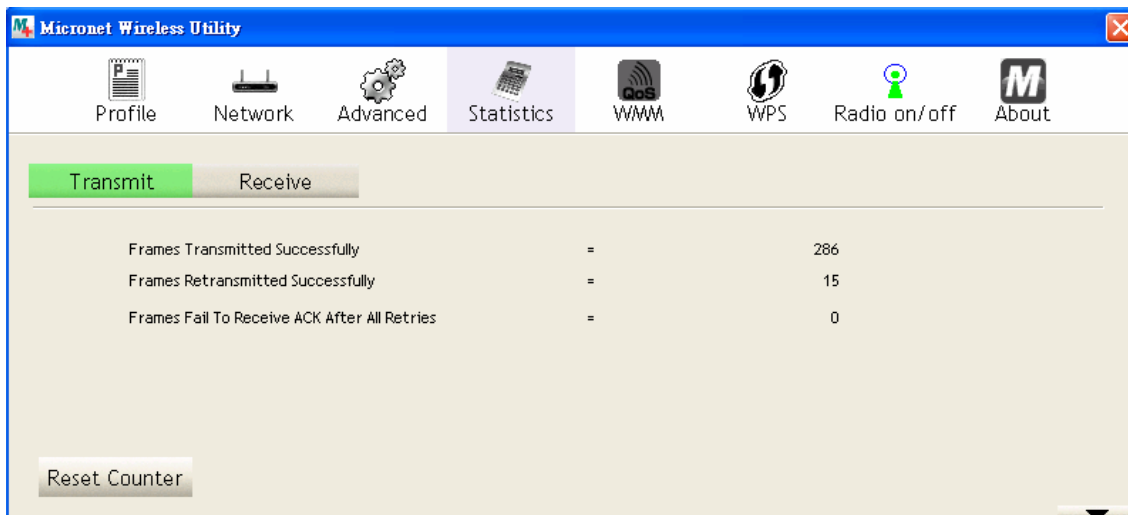
All connection-related statistics is displayed here. Users can click 'Transmit' or 'Receive' tab, to view the statistics of transmitted or received packets. It can also click 'Reset Counter' button, to reset the statistics of all items back to 0.

3.2.8 WMM Setting

This wireless network card provides WMM (Wi-Fi Multimedia) function, which can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When the users enable the WMM function of this network card, they can define the priority of different kinds of data to give higher priority to applications which require instant response.

Parameter	Description
WMM Enable	Check this box to enable WMM function. Please click 'Apply' button on the right of this check box so corresponding settings in this window will be activated or deactivated respectively.
WMM – Power Save Enable	Check this box to enable WMM power saving mode to save energy, and allow the computer's battery to last longer. Users also have to select WMM power save modes: ➢ AC_BE: Best Performance ➢ AC_BK: Worst Performance ➢ AC_VI: Video data has priority ➢ AC_VO: Voice data has priority
Direct Link Setup Enable	If users have another WMM-enabled wireless device, they can enter its MAC address in this field, and then click 'Apply' button. This network card will establish a direct link to the wireless device specified. The users also have to specify the timeout value of this directly-linked wireless device. Valid values are from 1 to 65535 (seconds), and input '0' for infinity.

27

3.2.9 WPS Configuration

Wi-Fi Protected Setup (WPS) is the latest wireless network technology, which makes wireless network setup become very simple. The user doesn't have to configure the wireless access point and setup data encryption when devices support WPS.

This wireless network card is compatible with WPS. To use this function, the wireless access point must also support WPS function. Please follow the following instructions to establish secure connection between WPS-enabled devices.
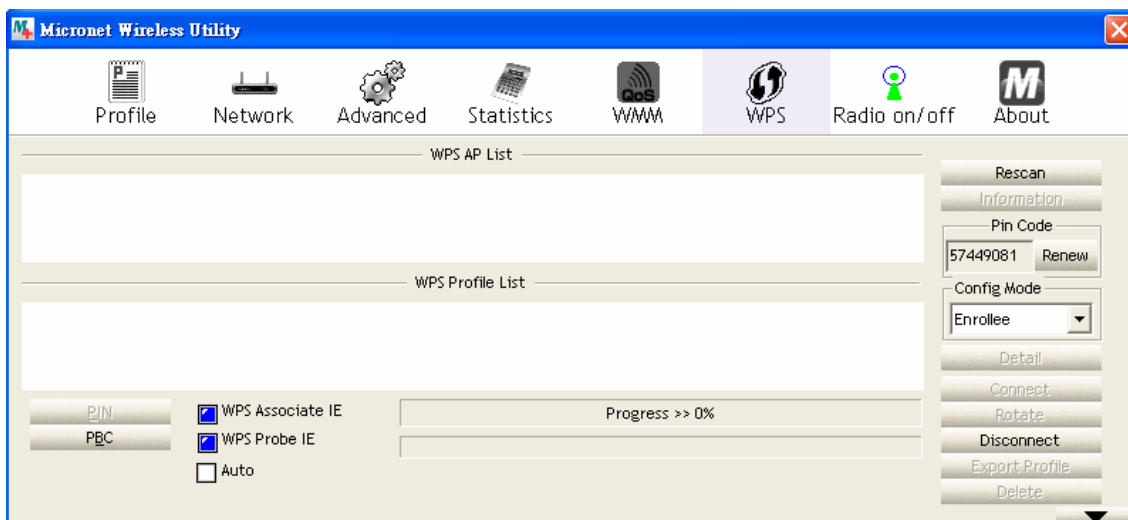
WPS Setup - PBC (Push-Button Configuration)

Step 1. Set 'Config Mode' to 'Enrollee', and then push the 'WPS' button on the wireless access point (the button used to activate WPS standby mode may have another name), or use other way to start WPS PBC standby mode as the instruction given by the wireless access point's user manual. User can also set 'Config Mode' to 'Registrar'. In this mode, the wireless network card will wait for other WPS-enabled access points to send WPS pairing requests. Please refer to the instruction given by the wireless access point's user manual to understand how to send WPS requests.

Step 2. Before users start to establish the wireless connection by using WPS, click 'Rescan' button to search for WPS-enabled access points and make sure the WPS function of the access point is activated.

28
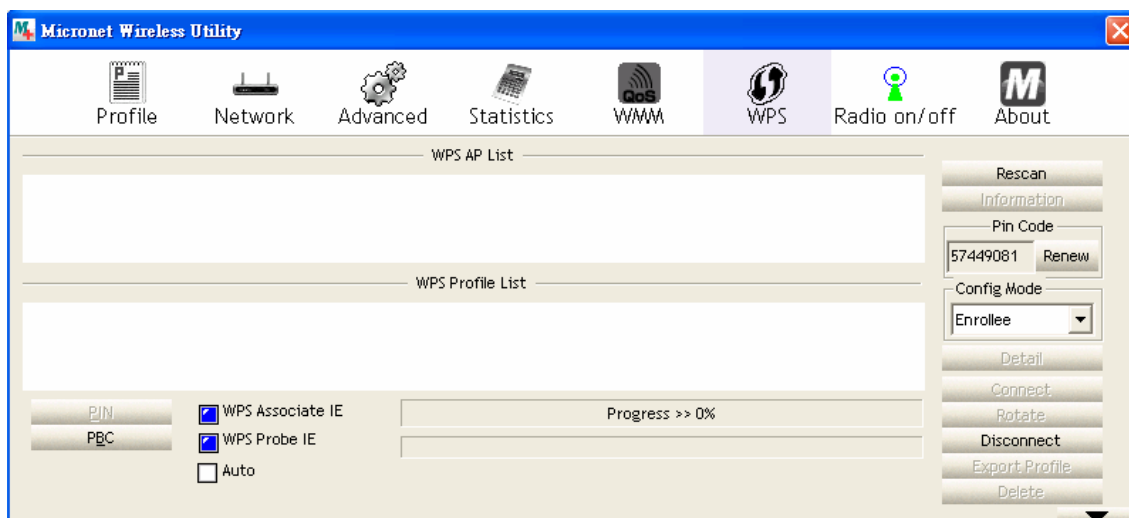
All access points with WPS function enabled will be displayed here. Please make sure the access point users wish to connect is displayed. If not, please click 'Rescan' few more times. The user can also click 'Information' button to see the detailed information about selected access point.

Step 3. 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 as this may require several seconds to one minute to complete. When users see 'WPS status is connected successfully' message, means the connection between this wireless network card and access point is successful.

Users can click 'Detail' button to see further information of connected access point. If users wish to save this connection as a profile, they can click 'Export Profile' button, and this connection will be saved. Users can find this connection in 'Profile' tab in a later time.

Sometime WPS may fail (In the following picture, WPS pairing is failed because no WPS-enabled access point is found):
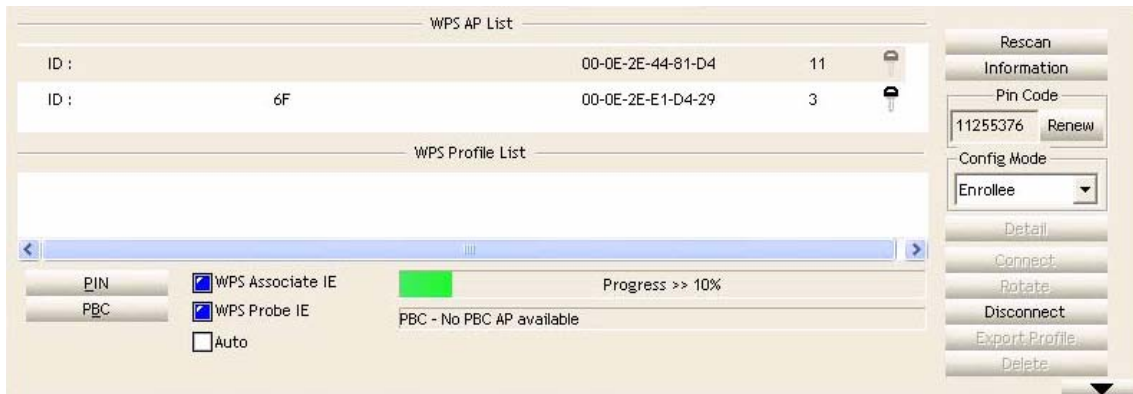
Users can click 'PBC' button few more times to try again. When an access point is connected, users can click 'Disconnect' to disconnect your wireless network card from a connected access point. Users can also click 'Rotate' button, and next access point on the list will be selected to establish connection.

WPS Setup – PIN

The PIN code of the wireless network card is an eight-digit number located at the upper-right position of configuration utility. Remember the code and input the number to the wireless access point as the WPS PIN code.
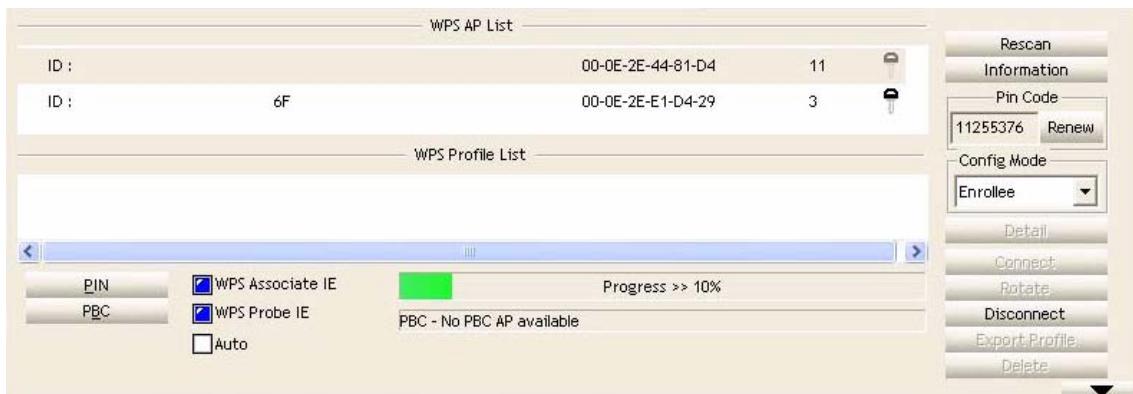
Step 1. Click on 'PIN' button now, and wait for few seconds to one minute. If a wireless access point with correct PIN code is found, it will be connected to that device.

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

30
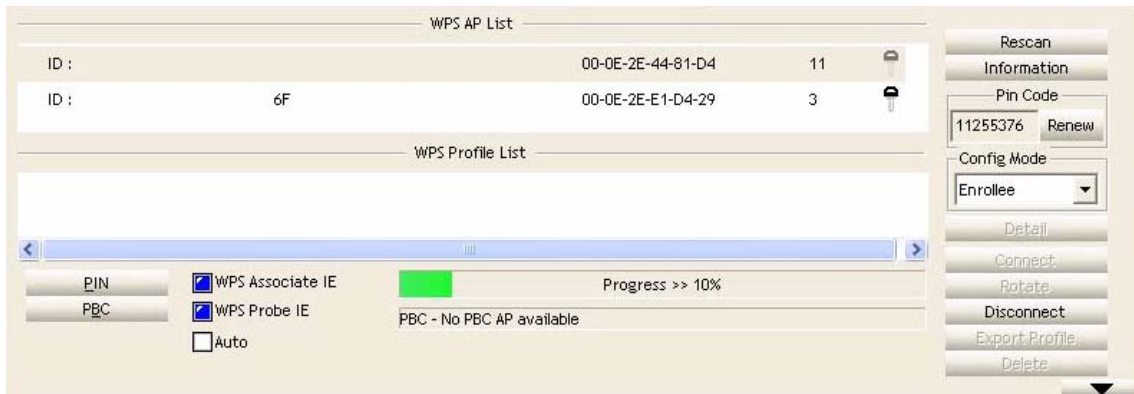
Parameter	Description
WPS associate IE	Check this box to send the association request with WPS IE during WPS setup.
WPS probe IE	Check this box to send the WPS probe request with WPS IE during WPS setup.
Auto	When in PIN mode, wireless access point to be connected will be selected automatically if this box is checked.

3.2.10   Radio On/Off

Users can switch the wireless radio transceiver on and off via the utility interface, therefore it is not necessary to physically remove the network card from the PC/laptop.

Step 1. To switch wireless radio on/off, please click on 'Radio On/Off' button.

31
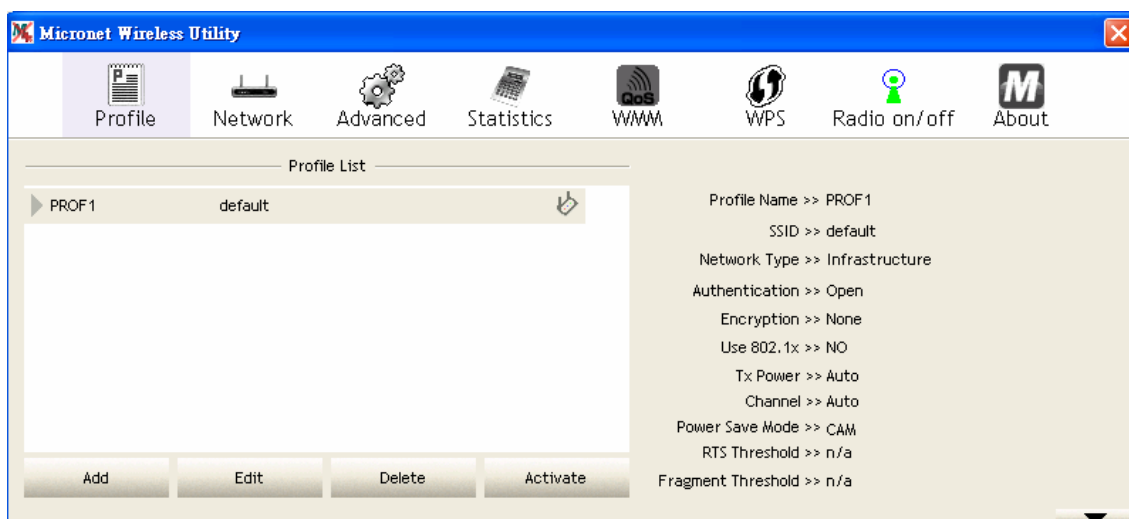
3.2.11 About

The 'About' tab provides the information about version number of the configuration utility, driver, and other important information about the wireless network card.
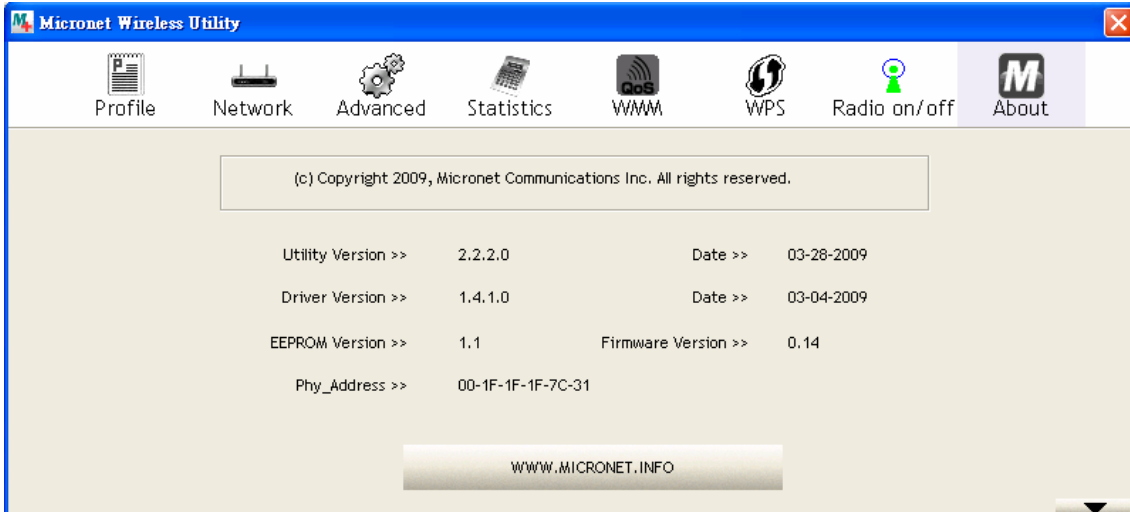
Chapter 4 Soft-AP Function

Besides becoming a wireless client of other wireless access points, this
wireless card can also act as a wireless service provider. Users can switch this
wireless card's operating mode to 'AP' to simulate the function of a real
wireless access point by software and even sharing the internet connection.
Please follow the instructions in following chapters to use the AP function of the
wireless card.

4.1   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 users want to switch to AP mode,
please right-click on utility icon, and select 'Switch to AP Mode'.
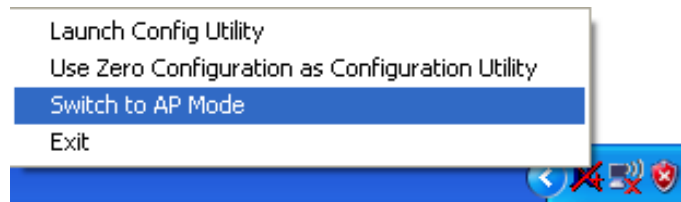
If users want to switch the wireless card back to station mode (become a client
of other wireless access points), click 'Switch to Station Mode'.
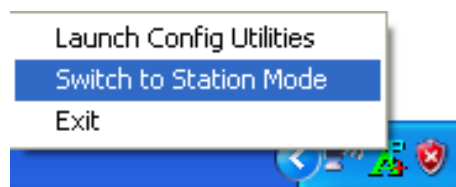
A configuration window will appear after switching the operation mode to 'AP',
which asks users to assign an existing network card with internet connection.

33
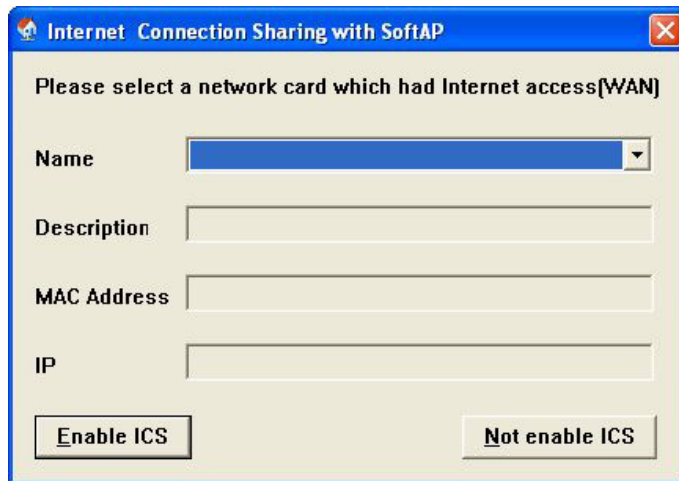
If the computer has another network card which is connected to Internet, please select it from 'Name' dropdown menu, and click 'Enable ICS'. If your computer does not have another network card with Internet connection, please click 'Not enable ICS'.

After clicking on 'Enable ICS' or 'Not enable ICS', the user will see the basic configuration menu of the AP function.
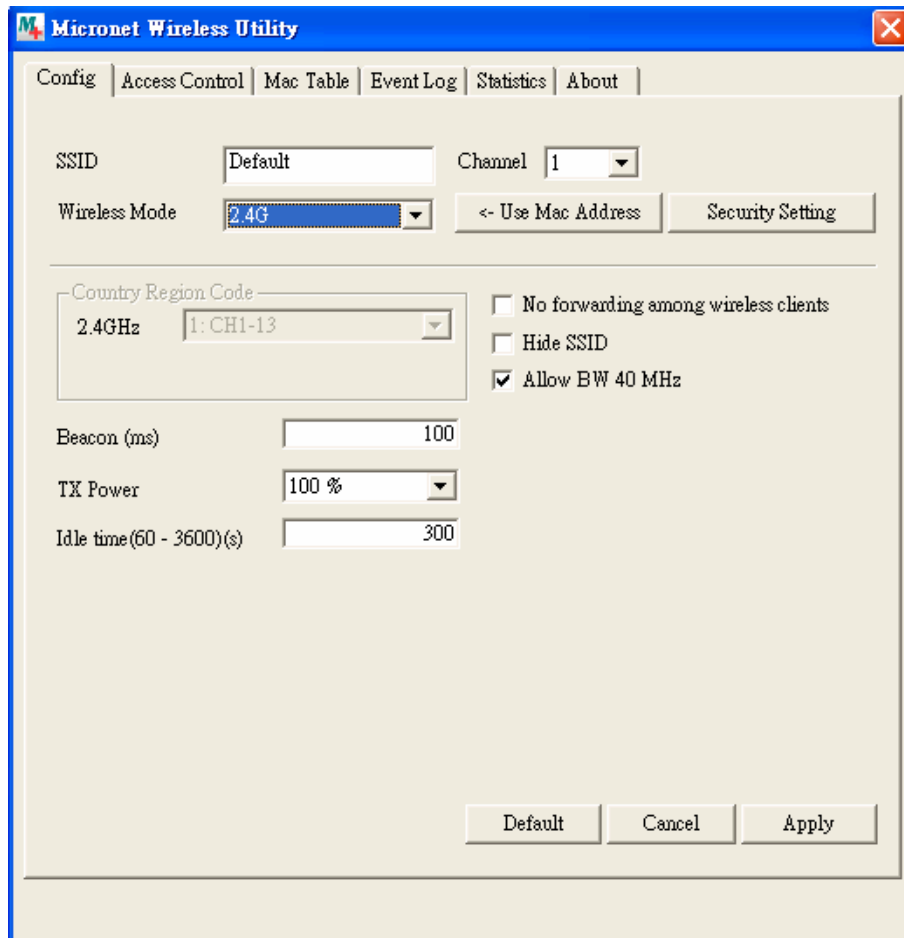
Parameter	Description
SSID	Please input the SSID (the name used to identify this wireless access point) in this field. Up to 32 numerical characters can be accepted here excepting space.
Channel	Please select the wireless channel to use for the environment. The number of channels available here will vary depending on the setting of 'Country Region Code'.
Wireless Mode	Select the operation mode of the access point in this field.
Use Mac Address	Click this button to use the MAC address of the wireless card as SSID. A prefix 'AP' will be added automatically.
Security Setting	Set the security options (wireless data encryption). Please refer to next section on 'Security Settings' for details.

35

Country Region Code	Please select the country code of the country or region. Available options are 0-7, which will affect the available wireless channels: 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) Please note that only change the country code if the country is different. For example, when operating this product in US, only channels 1~11 can be operated. Selection of other channels is not permitted under FCC regulations.
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 the computer. This option is useful to enhance security level.
Allow BW 40 MHz	Check this box to allow BW 40MHz capability.
Tx BURST	Check this box to accelerate the data transmit rate. It may not work with all wireless access point and wireless devices.
Beacon(ms)	Users can define the time interval that a beacon signal should be send. Default value is 100.
TX Power	Users can select the wireless output power in this field. Please select a proper output power setting according to the actual needs. Users may not need 100% of output power if other wireless clients are nearby.
Idle Time	Select the idle time for the wireless access point. Default value is 300. Do not modify this value unless you know what will be affected.

*Click **<Apply>** to save the changes.*

4.2   Security Setting

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 the users wish to open the computer (and its internet connection) to the public. When users click on 'Security Setting' in the utility, the following window will appear:

36
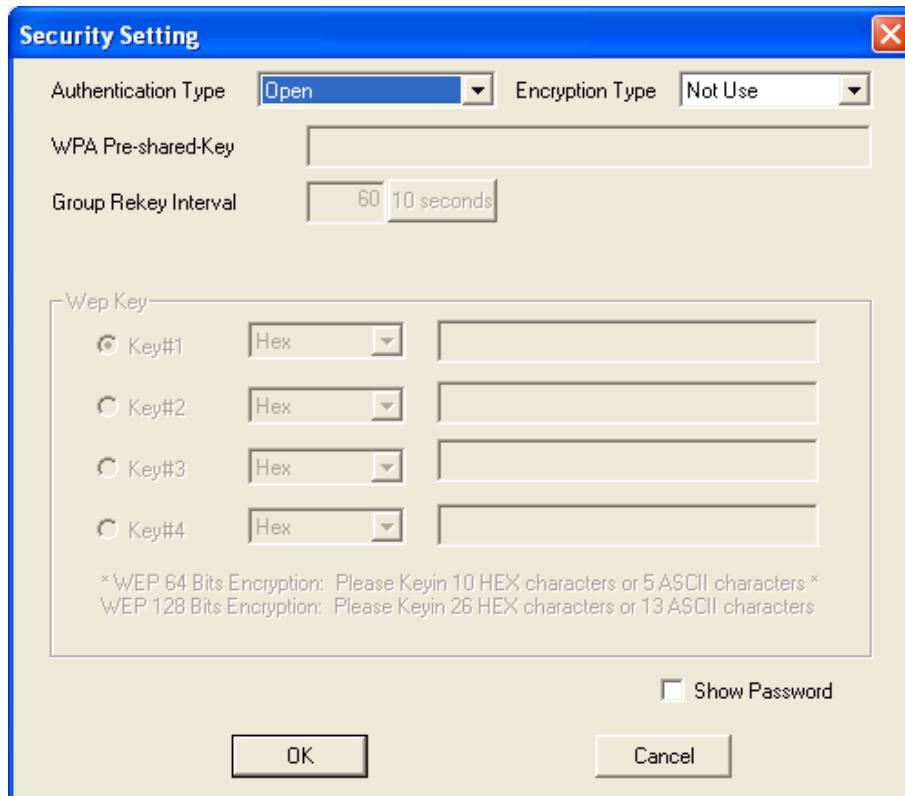
Parameter	Description
Authentication Type	Please select a wireless authentication type to use. Available options are 'Open', 'Shared', WPA-PSK', 'WPA2-PSK', and 'WPA-PSK / WPA2-PSK'. If users want to disable wireless data encryption, please select 'Open'.
Encryption Type	Please select an encryption mode. The available options in this setting item will vary depending on the authentication type selected. If users select 'Not Use', data will not be encrypted and people with some networking knowledge will be able to read the data transferred with proper tool.
WPA Pre-shared Key	Please input the WPA pre-shared key in this field. Only clients with the same pre-shared key inputted here will be able to connect to the computer. This setting is only available when WPA encryption is selected.
Group Rekey Interval	Users can specify the time interval to re-issue the key to wireless clients. Users 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 specified in 'Group Rekey Interval' field).

37

WEP Key	Please input the WEP encryption key in this field when 'WEP' is selected. 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 selected.

If users want to use WEP 64 bits encryption, please input 10 characters for HEX and 5 characters for ASCII. If users want to use WEP 128bits encryption, please input 26 characters for HEX and 13 characters for ASCII. 128 bits encryption is safer than 64 bits, but the data transfer speed will be slightly reduced. |
| **Show Password** | Check this box and the WPA pre-shared key or WEP key inputted will be display and not replaced by asterisk (*). |

*When you finish with setting and want to save changes, click **<Ok>** button, or click **<Cancel>** button to discard all changes made.*

4.3   Access Control

If users are not going to open the computer and wireless resources to the public, they can use MAC address filtering function to enforce the access control policy. So only the MAC address included by the ACL can connect to the device.

Parameter	Description
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.

*Click **<Apply>** to save the changes.*

4.4   MAC Table

If users want to see the list of all wireless clients connected to this access point, please select 'Mac Table' tab from the utility.

Parameter	Description
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.

4.5   Event Log

This software access point will log all wireless-related activities as a log. Click 'Event Log' tab, and the interface below will be displayed.

4.6   Statistics

If users want to know detailed information about how the software access point works, click 'Statistics' tab, and the below interface will be displayed.

40

4.7　About

The 'About' tab provides the information about version number of the configuration utility, driver, and other important information about the wireless access point.

Micronet Wireless Utility

Config | Access Control | Mac Table | Event Log | Statistics | About

WWW.MICRONET.INFO

(c) Copyright 2009,Micronet Communications Inc. All rights reserved.

Utility Version :	2.1.2.0	Date :	03-27-2009
Driver Version :	1.4.1.0	Date :	03-04-2009
EEPROM Version :	1.1	Firmware Version :	0.14

IP Address :	192.168.123.1	Phy_Address :	00-1F-1F-1F-7C-31
Sub Mask :	255.255.255.0	Default Gateway :	

42

Chapter 5   Troubleshooting

If users encounter any problem when using this wireless network card, consult this section for possible solutions. Before calling the dealer of purchase for help, please check this troubleshooting table, the solution towards the problem could be very simple.

Scenario	Solution
I can't find any wireless access point / wireless device in 'Site Survey' function.	1. Click **\<Rescan\>** for few more times and see if it 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 that wishes to establish a direct wireless link. 4. Please adjust the position of the network card and click 'Rescan' button for few more times.
Nothing happens when I click 'Launch config utilities'.	1. Please make sure the wireless network card is firmly inserted into the computer's USB slot. If the configuration utility's icon is black, the network card is not detected by the computer. 2. Reboot the computer and try again. 3. Remove the driver and re-install. 4. Contact the dealer of purchase for help.
I cannot establish connection with a certain wireless access point.	1. Click **\<Connect\>** for few more times. 2. If the SSID of access point is hidden, users have to input correct SSID of the access point. Please contact the owner of access point to ask for correct SSID. 3. Users 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 only allows network cards with specific MAC address to establish connection. Please go to 'About' tab and write the value of 'Phy_Addess' down, then present this value to the owner of access point so he / she can add the MAC address of the network card to his / her access point's list.
The network is slow / having problem when transferring large files	1. Move closer to the place where access point is located. 2. Enable 'Wireless Protection' in 'Advanced' tab. 3. Disable 'Tx Burst' in 'Advanced' tab. 4. Enable 'WMM' if users need to use multimedia / telephony related applications. 5. Disable 'WMM – Power Save Enable'. 6. There could be too much people using the same radio channel. Ask the owner of the access point to change the channel number.

Chapter 6   Glossary

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides 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 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. protection mechanism called RTS/CTS that govern 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 who has 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 with their own Wireless LAN Card connecting 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 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.

45

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, 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? 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.

46

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 saves. 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.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com