



**Wireless PCI Card  
IEEE 802.11n 300Mbps**



**USER MANUAL**

[www.hamletcom.com](http://www.hamletcom.com)

Dear Customer,  
thanks for choosing an Hamlet product. Please carefully follow the instructions for its use and maintenance and, once this item has run its life span, we kindly ask You to dispose of it in an environmentally friendly way, by putting it in the separate bins for electrical/electronic waste, or to bring it back to your retailer who will collect it for free.

We inform You this product is manufactured with materials and components in compliance with ROHS directives: 2002/95/CE; with RAEE Directives: 2003/96/CE, Italian Legislative Decree 2005/151 and below EEC Directives:

EN 62311: 2008

EN 300 328 (2006-10)

EN 301 489-1 (2008-04)

EN 301 489-17 (2008-04)

EN 55022: 2006+A1: 2007, Class B

EN 61000-4-2: 1995+A1: 1998+A2:2001

EN 61000-4-3: 2006+A1: 2008

### **CE Mark Warning**

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.



### **Trademarks**

All trademarks and company names mentioned in this manual are used for description purpose only and remain property of their respective owners.

### **Changes**

The material in this document is for information only and subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Hamlet assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. Hamlet reserves the right to make changes or revisions in the product design or the product manual without reservation and without obligation to notify any person of such revisions and changes.

# Table of contents

<b>1. INTRODUCTION.....</b>	<b>4</b>
1.1 FEATURES & BENEFITS.....	5
1.2 PACKAGE CONTENTS.....	5
1.3 PCI CARD DESCRIPTION.....	5
1.4 SYSTEM REQUIREMENTS .....	5
<b>2. PCI CARD ADAPTER FOR WINDOWS 2000/XP/VISTA.....</b>	<b>6</b>
2.1 BEFORE YOU BEGIN .....	6
2.2 INSTALLING THE DRIVERS .....	6
2.3 PROFILES.....	8
2.4 AUTHENTICATION AND SECURITY .....	10
2.5 NETWORK.....	12
2.6 SITE SURVEY.....	13
2.7 STATISTICS .....	14
2.8 WPS .....	14
2.9 ABOUT .....	15
2.10 UNINSTALL THE DRIVERS & CLIENT UTILITY.....	15
<b>3. PCI CARD ADAPTER FOR WINDOWS 2000/XP .....</b>	<b>16</b>
3.1 BEFORE YOU BEGIN .....	16
3.2 INSTALLING THE DRIVERS .....	16
3.3 PROFILES.....	17
3.4 AUTHENTICATION AND SECURITY .....	20
3.5 NETWORK.....	27
3.6 ADVANCED CONFIGURATION .....	29
3.7 STATISTICS .....	29
3.8 WMM (WIRELESS MULTIMEDIA) .....	30
3.9 WPS .....	31
3.10 ABOUT .....	32
3.11 RADIO.....	32
3.12 UNINSTALL THE DRIVERS & CLIENT UTILITY.....	33
<b>4. APPENDIX A – GLOSSARY .....</b>	<b>34</b>
<b>5. APPENDIX B – SPECIFICATIONS.....</b>	<b>44</b>
<b>6. APPENDIX C – FCC INTERFERENCE STATEMENT .....</b>	<b>45</b>

# 1. Introduction

The high-speed wireless PCI CARD is the most convenient way to let you put a desktop/notebook computer almost anywhere without the hassle of running network cables. Now you don't need to suffer from drilling holes and exposed cables. Once you are connected, you can do anything, just like the wired network. This PCI CARD operates seamlessly in 2.4GHz frequency spectrum supporting the 802.11b, 802.11g, and 802.11n wireless standards. It's the best way to add wireless capability to your existing wired network or simply surf the web.

To protect your wireless connectivity, the high-speed wireless PCI CARD can encrypt all wireless transmissions through 64/128-bit WEP, WPA, WPA-PSK and WPA-AES encryption and authentication allowing you to experience the most secure wireless connectivity available.

The Hamlet 802.11n PCI CARD (HNW300CI) implements the latest 11n 2.0 technology which extremely improves wireless signal for your computer than existing wireless 802.11g technology. It supports the 1T2R architecture with fully forward compatibility with IEEE802.11n. The incredible speed of HNW300CI PCI CARD makes heavy traffic networking activities more flexible and takes the wireless into practical road. You could enjoy the racing speed of wireless connection, surfing on Internet without string wires.

Adding Hamlet HNW300CI to your Computer, it provides an excellent performance and cost-effective solution for doing media-centric activities such as streaming video, gaming, and enhances the QoS (WMM) without any reduction of performance. It extends 3 times network coverage and boosts 6 times transmission throughput than existing 11g product. Advanced power management and low power consumption among 11n products.

For more security-sensitive application, HNW300CI supports Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP, and AES. Also, it supports Wi-Fi alliance WPA and WPA2 encryption.

## 1.1 Features & Benefits

Features	Benefits
Racing Speed up to 300Mbps* data rate (2.4GHz 11N technology)	Enjoy the Internet connection in crazy-fast speed, without the bottleneck of stringing wires
Advanced power management	Low power consumption
WPA/WPA2 (IEEE 802.11i), WEP 64/128 Support	Powerful data security
Support 1Tx * 2Rx Radios	With two external Antennas
WMM (IEEE 802.11e) standard support	Wireless Multimedia Enhancements Quality of Service support (QoS) / enhanced power saving for Dynamic Networking
PCI 2.2	Fits in any PCI standard slot

*\* Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

## 1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- One Wireless 802.11b/g/n PCI CARD
- One CD-ROM with Drivers and User's Manual Included
- TWO SMA antennas
- One Quick Installation Guide and User's Manual

## 1.3 PCI CARD Description

The PCI CARD support PCI 2.2 standard PCI  
The PCI CARD has two LED indicators with two SMA external antennas.

## 1.4 System Requirements

The following are the minimum system requirements in order to use the PCI CARD

- The computer with a PCI 2.2 interface.
- Windows 2000/XP/Vista operating system.
- 30 MB of free disk space for installing the PCI CARD driver and utility program.

## 2. PCI Card Adapter for Windows 2000/XP/Vista

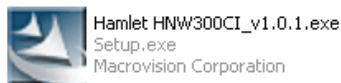
### 2.1 Before You Begin

During the installation, Vista may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers.

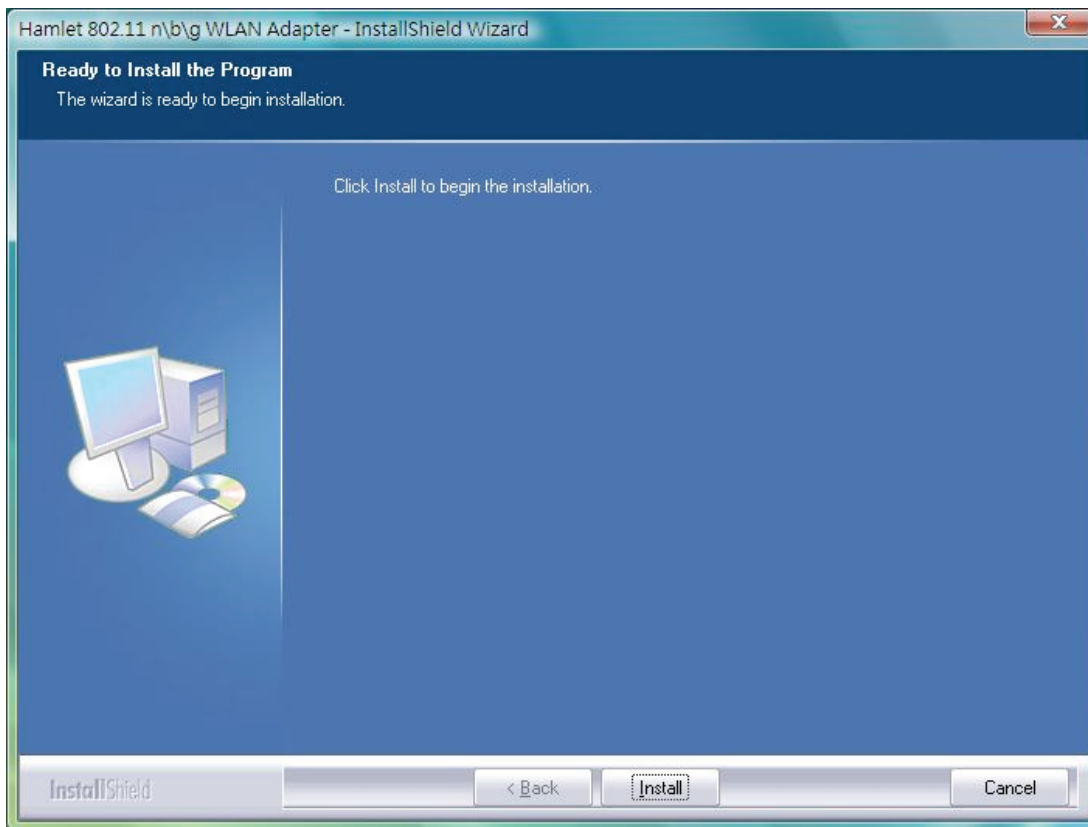
### 2.2 Installing the Drivers

Follow the steps below in order to install the PCI CARD drivers:

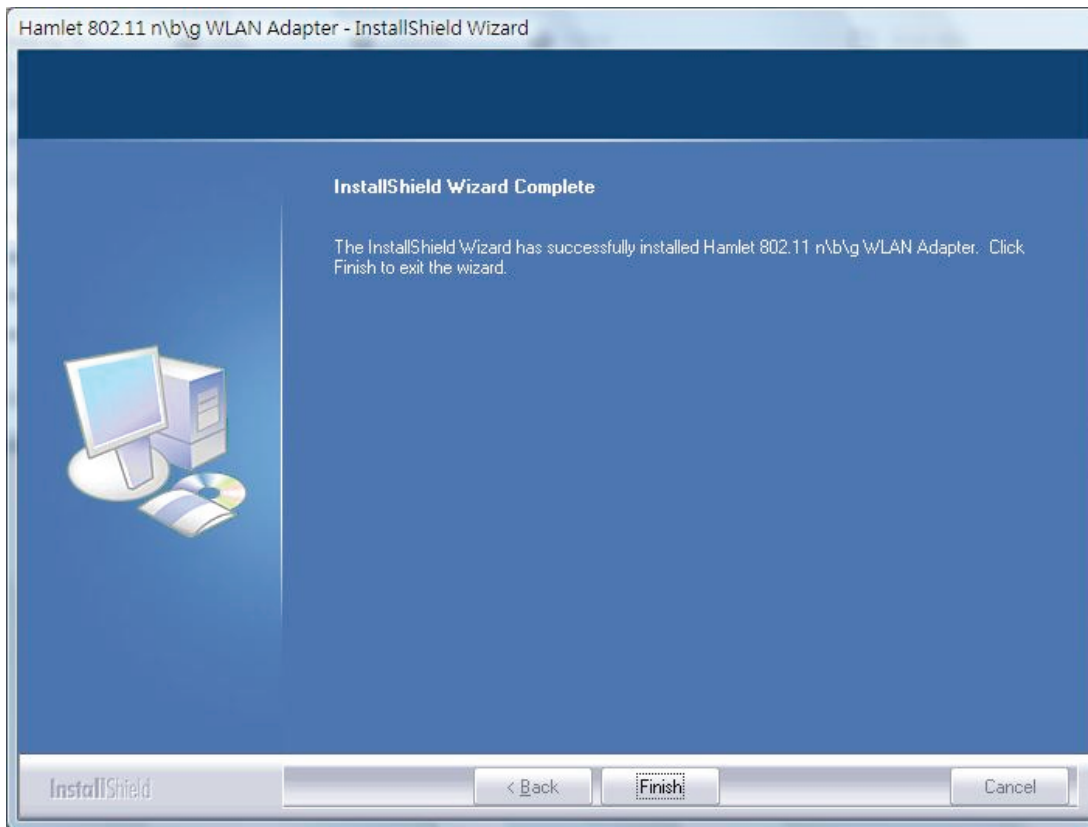
- Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **Hamlet HNW300CI\_v1.0.1.exe** file from the CD-ROM drive.



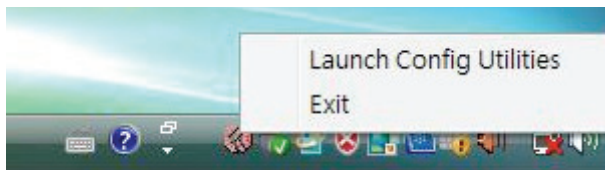
- Once the setup begins you will see the **InstallShield Wizard**.
- Click on the **Install** button to begin the installation.



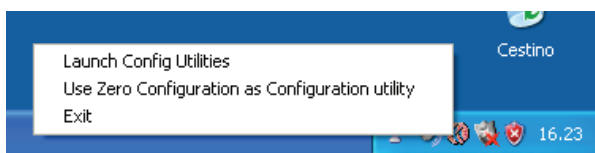
- The installation is complete. Click on the **Finish** button.



- Carefully insert the PCI Card into the PCI slot. Windows will then detect and install the new hardware.



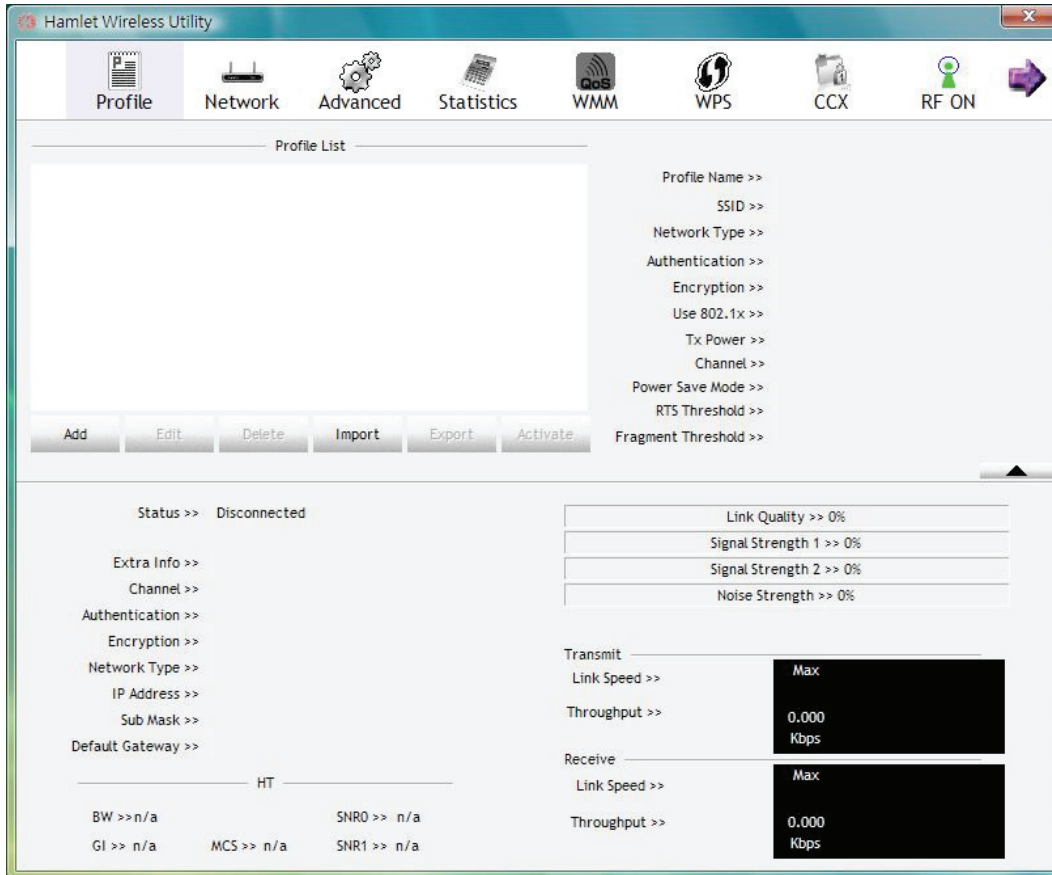
- An Hamlet icon will then appear in the system tray. Right click on the icon and then click on **Launch Config Utilities**.



**Note:** Click on **Use Zero Configuration as Configuration Utility** if you would like to use Windows Zero Config.

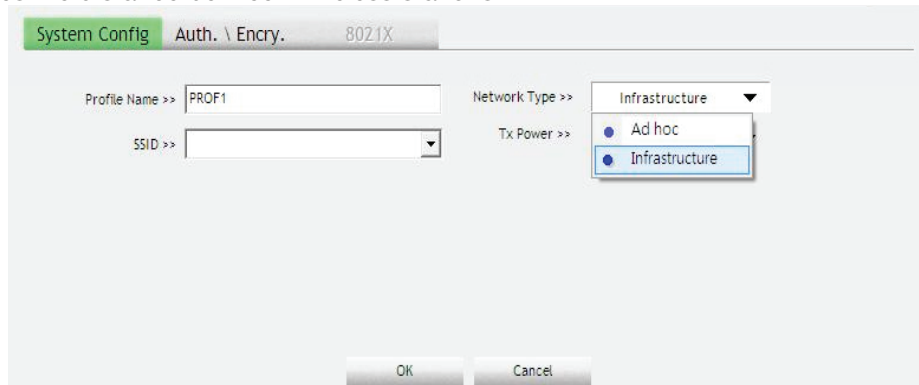
## 2.3 Profiles

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.



### 2.3.1 Infrastructure Mode

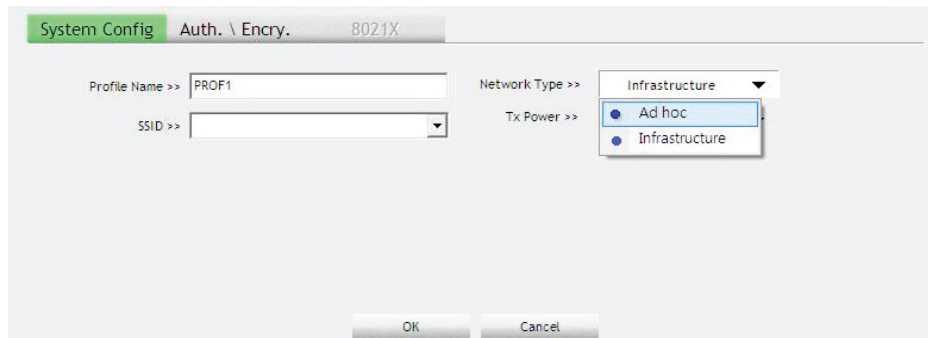
The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.



- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID:** Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Infrastructure** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- Click on the **Apply** button to save the changes.

### 2.3.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.



- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID:** Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Ad-hoc** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- Click on the **Apply** button to save the changes.

## 2.4 Authentication and Security

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK. Each security option is described in detail below.

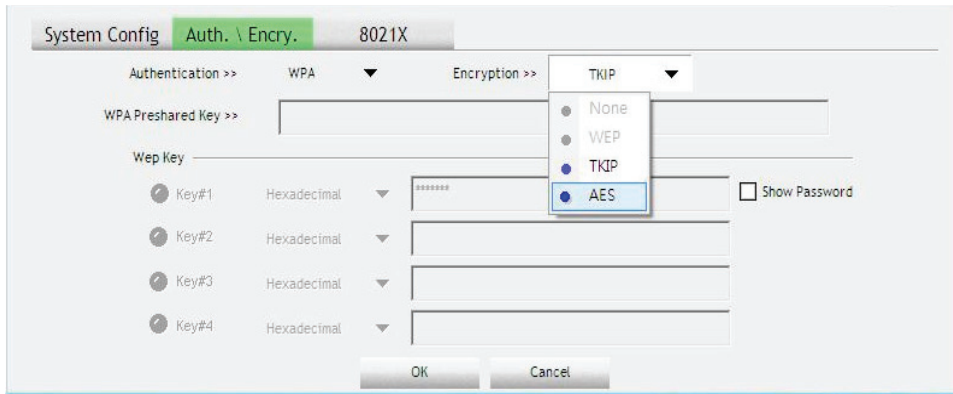
### 2.4.1 WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.

- **Authentication Type:** Select **Open** or **Shared** from the drop-down list.
- **Encryption:** Select **WEP** from the drop-down list.
- **WEP Key:** Type a character string into the field.  
For 64-bit enter 5 alphanumeric or 10 hexadecimal characters.  
For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

### 2.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption

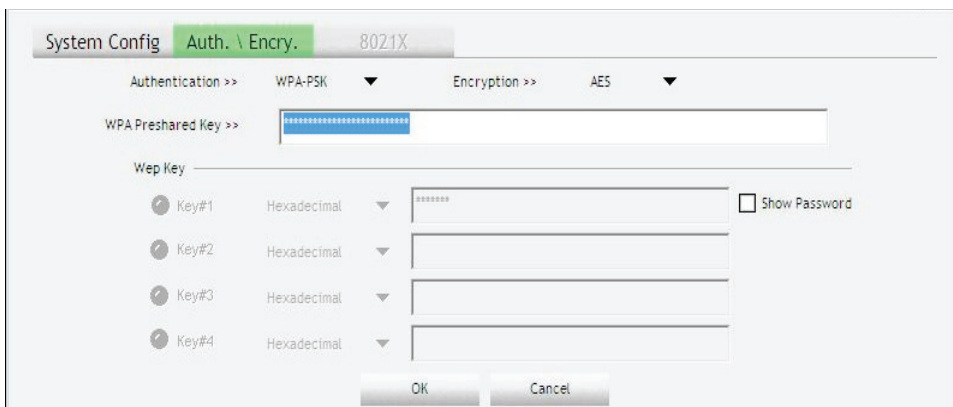
WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



- **Authentication Type:** Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

### 2.4.3 WPA-PSK Authentication & TKIP, AES Encryption

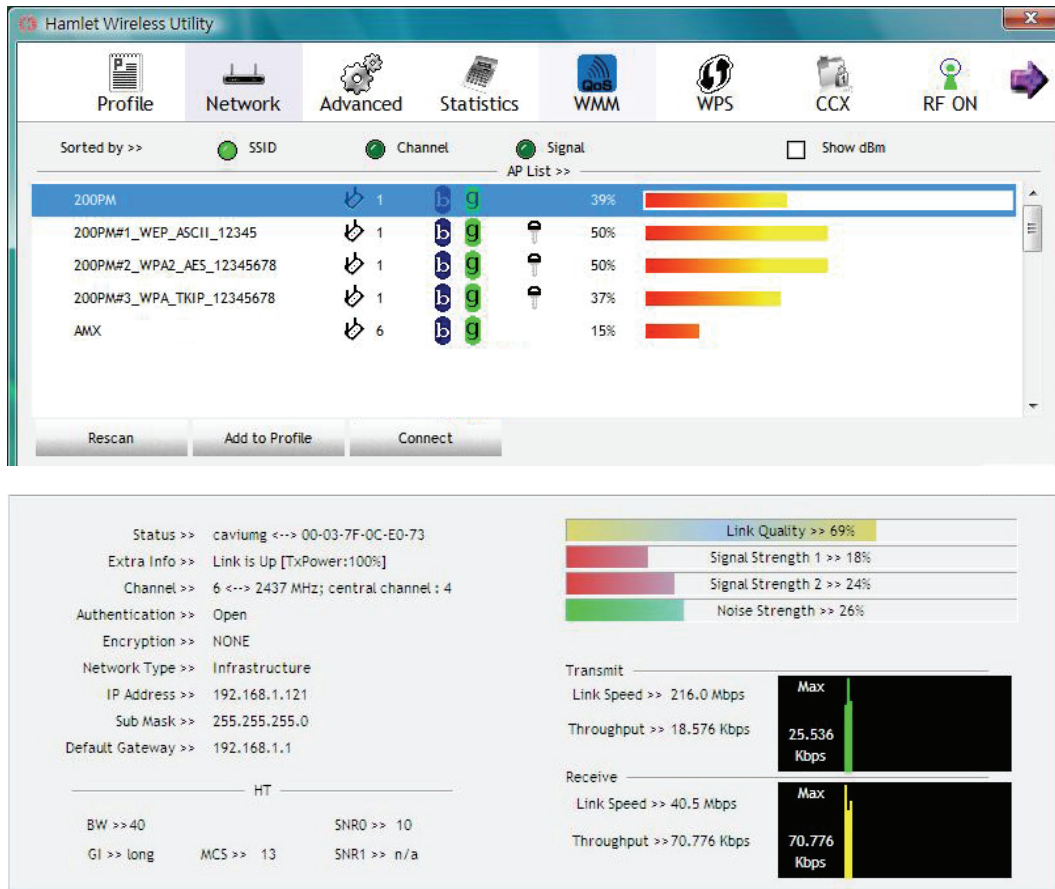
WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



- **Authentication Type:** Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- **WPA Preshared key:** Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

## 2.5 Network

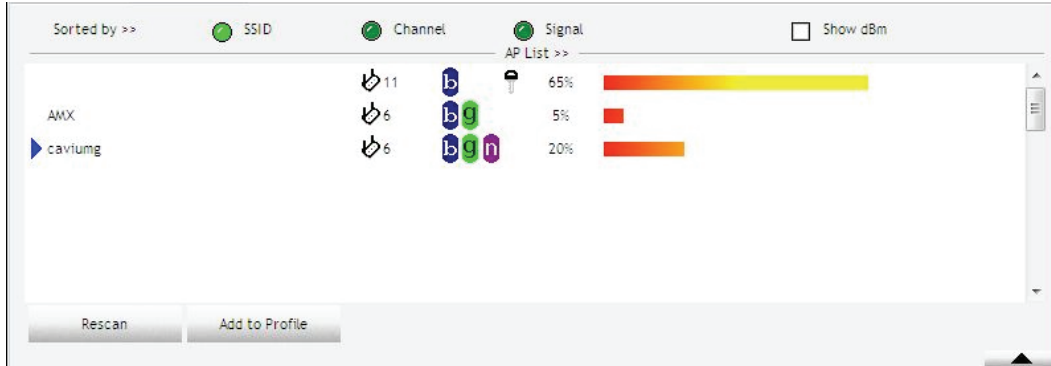
The **Network** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.



- **Status:** This indicates the state of the client. There are three options:
  - **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
  - **Scanning:** Indicates that the wireless client is searching for an AP in the area.
  - **Disconnected:** Indicates that there are no APs or clients in the area.
- **Extra Info:** Displayed here are information about the link stats and the percent of output power.
- **Current Channel:** The operating frequency channel that the client is using (infrastructure mode).
- **Link Speed:** The current rate at which the client is transmitting and receiving.
- **Throughput (bytes/sec):** Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- **Link Quality:** In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- **Signal Strength:** This bar displays the strength of the signal received from an AP or client.
- **Noise Level:** Displays the background noise level; a lower level indicates less interference.
- Click on the **OK** button to close this window.
- **dBm Check Box.** When you click on the check box as the drawing below. The signal strength and noise level will be shown as the dBm measurements.

## 2.6 Site survey

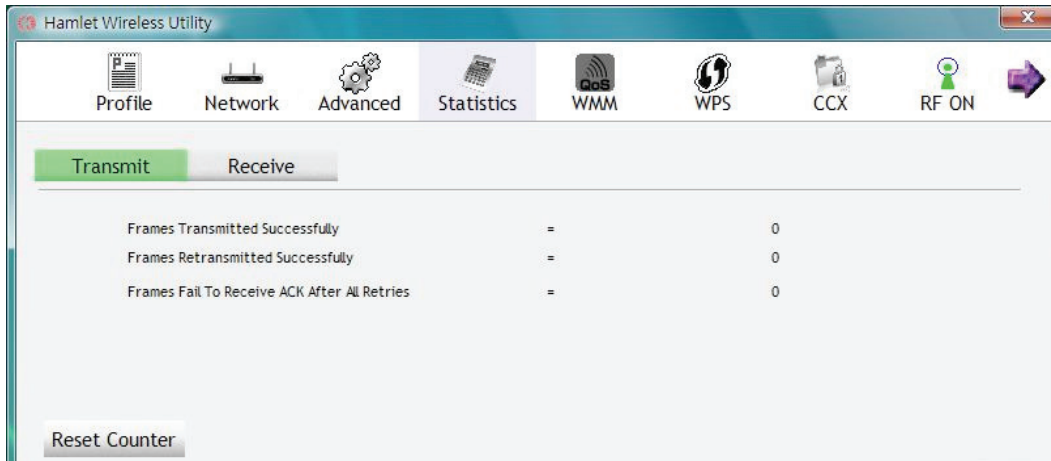
The **Network** tab also displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.



- **SSID:** Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **BSSID:** Displays the MAC address of the Access Point.
- **Signal:** Displays the receiving signal strength from the Access Point.
- **Channel:** Displays the channel number of the Access Point.
- **Encryption:** Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- **Authentication:** displays the authentication on the Access Point, this includes WPA, WPA-PSK, WPA2, or Unknown.
- **Network Type:** Indicates whether the SSID is a Station (Ad-hoc) or Access Point (Infrastructure).
- **Rescan:** Click on this button to view a list of Access Points in the area.
- **Connect:** to connect with a specific Access Point, select the SSID from the list, and then click on the Connect button.
- **Add to Profile:** Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

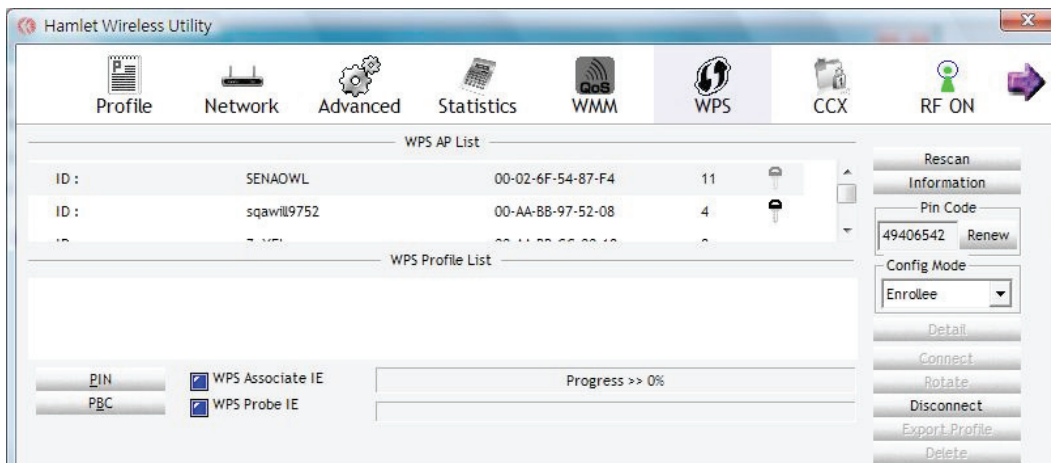
## 2.7 Statistics

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.



## 2.8 WPS

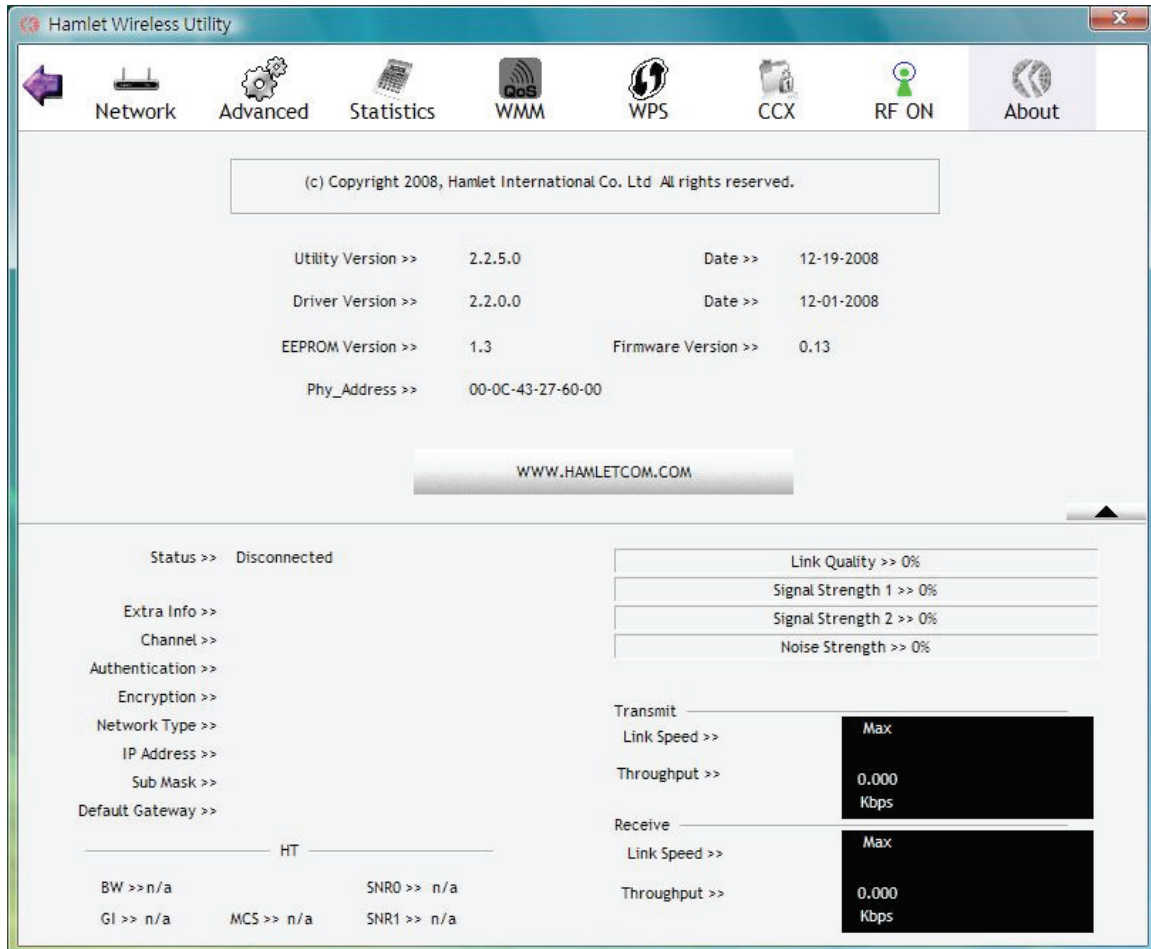
Click on the WPS Configuration tab. WPS is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.



- **Rescan:** Click on this button to view a list of Access Points in the area.
- Click on the **OK** button if you have made any changes.

## 2.9 About

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.



## 2.10 Uninstall the Drivers & Client Utility

If the PCI CARD installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the PCI CARD and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

Click on **Start > Hamlet HNW300CI > Uninstall Hamlet HNW300CI**

The **un-installation** process will then begin.

Once un-installation process is completed, select **Yes, I want to restart my computer now** radio button and then click on the **Finish** button. Finally remove the PCI Card adapter.

## 3. PCI Card Adapter for Windows 2000/XP

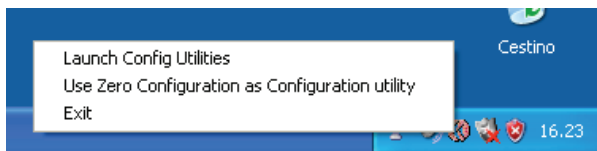
### 3.1 Before You Begin

During the installation, XP may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS\OPTIONS\CABS directory.

### 3.2 Installing the Drivers

Follow the steps below in order to install the PCI CARDadapter drivers:

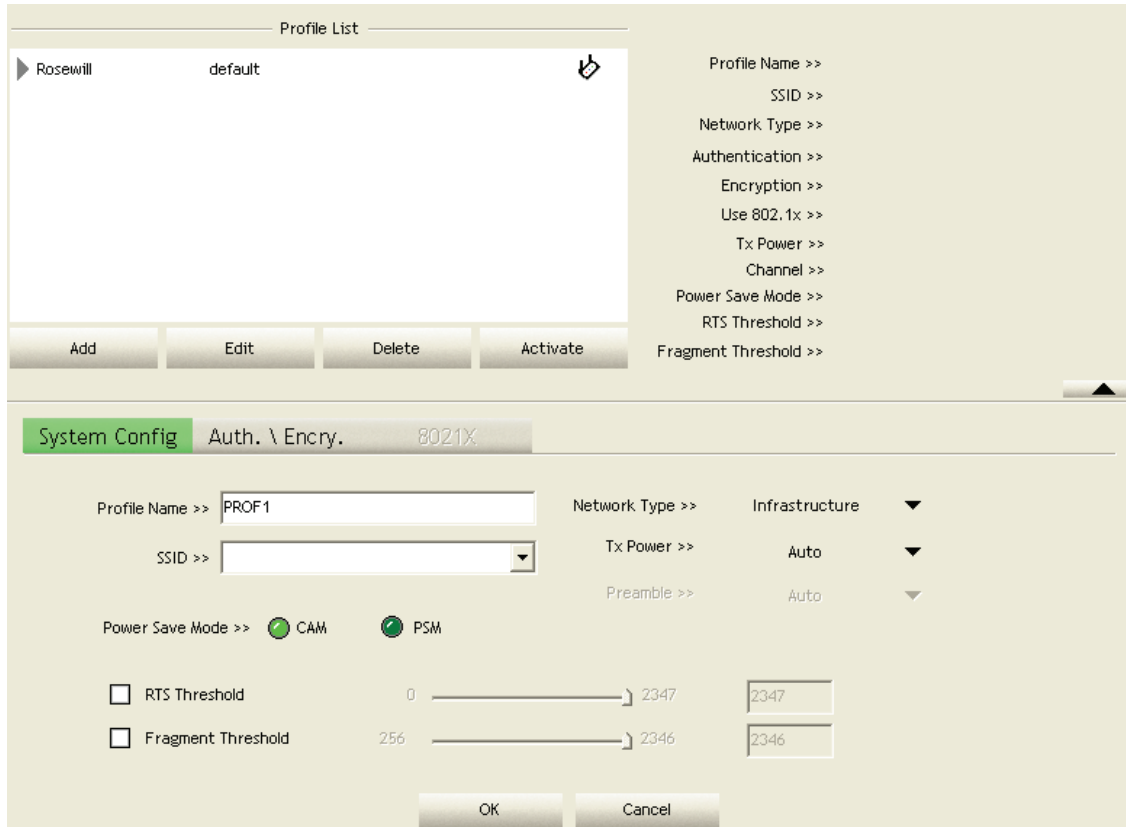
- Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.
- Once the setup begins you will see the **InstallShield Wizard**.
- Click on the **Install** button to begin the installation.
- Wait for a few seconds until the driver and client utility is installed.
- The installation is complete. Click on the **Finish** button.
- **Carefully insert the PCI CARD into the PCI slot . Windows will then detect and install the new hardware.**
- An **Hamlet** icon will then appear in the system tray. Right click on the icon and then click on **Launch Config Utilities**.



**Note:** Click on **Use Zero Configuration as Configuration Utility** if you would like to use Windows Zero Config.

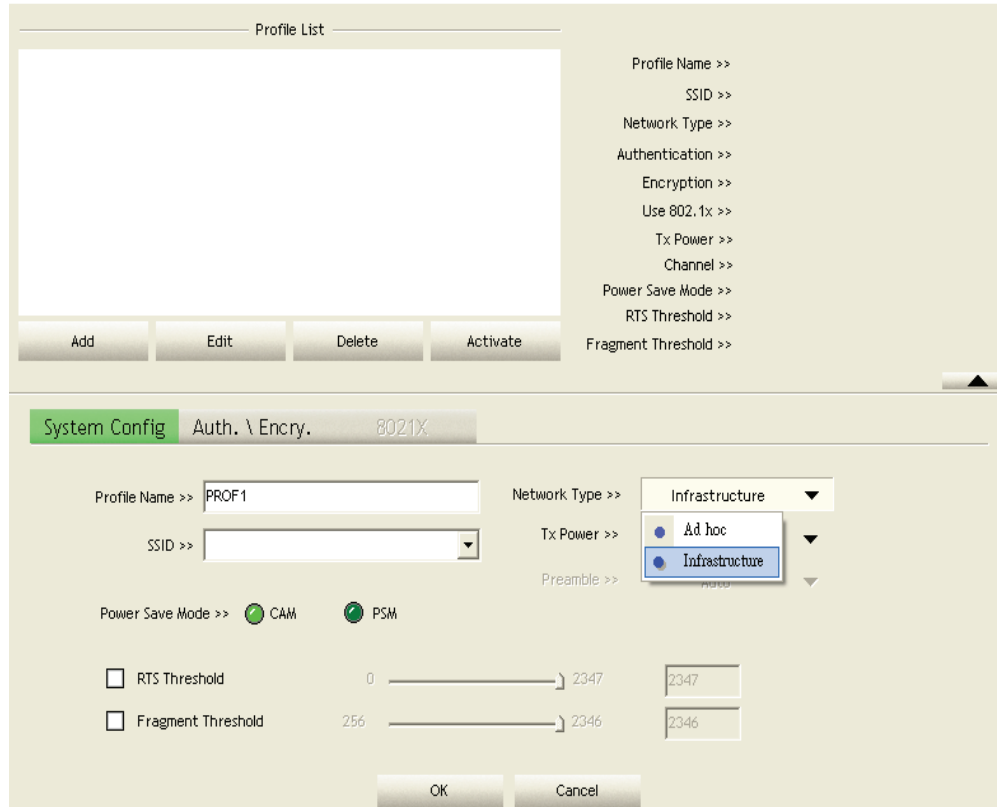
### 3.3 Profiles

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.



### 3.3.1 Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.



- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID:** Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Power Save Mode:** Select a power saving mode (PSM) option.
  - **CAM (Continuously Awake Mode):** Select this option if your notebook is always connected to the power supply.
  - **PSM (Power Saving Mode):** Select this option if your notebook uses its battery power. This option minimizes the battery usage while the network is idle.
- **Network Type:** Select **Infrastructure** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- **RTS Threshold:** Place a check in this box if you would like to enable RTS Threshold. Any packet in the RTS/CTS handshake larger than the specified value (bytes) will be discarded.
- **Fragment Threshold:** Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be discarded.
- Click on the **OK** button to save the changes.

### 3.3.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the

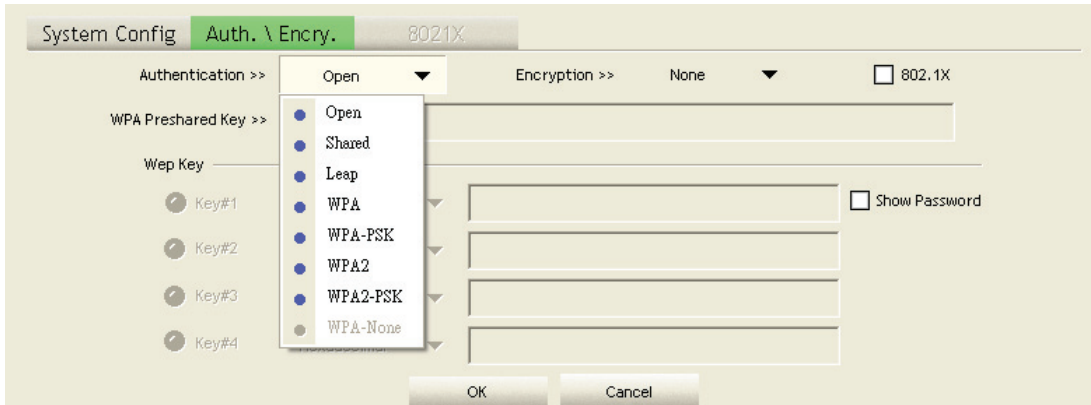
other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.

The screenshot displays the configuration interface for a wireless network profile. The top section, titled 'Profile List', contains a list of profiles and buttons for 'Add', 'Edit', 'Delete', and 'Activate'. Below this is the 'System Config' window for 'Auth. \ Encry. 8021X'. The 'Profile Name' is set to 'PROF1'. The 'Network Type' dropdown menu is open, showing 'Ad hoc' and 'Infrastructure' options. The 'Power Save Mode' has radio buttons for 'CAM' and 'PSM'. There are sliders and input boxes for 'RTS Threshold' (0 to 2347) and 'Fragment Threshold' (256 to 2346). 'OK' and 'Cancel' buttons are at the bottom.

- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID:** Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Ad-hoc** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select 100% or auto, if not, select one of the lower values for power saving.
- Click on the **OK** button to save the changes.

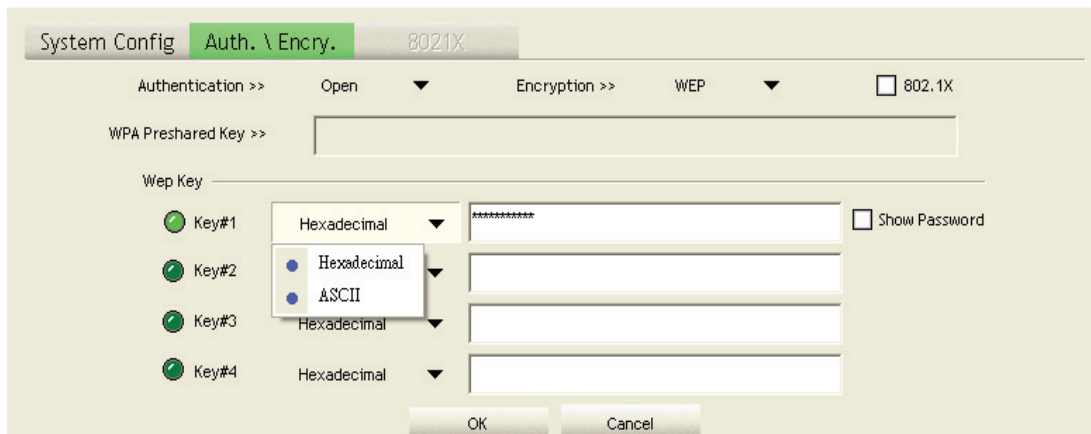
## 3.4 Authentication and Security

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK, WPA2, and 802.1x. Each security option is described in detail below.



### 3.4.1 WEP Encryption

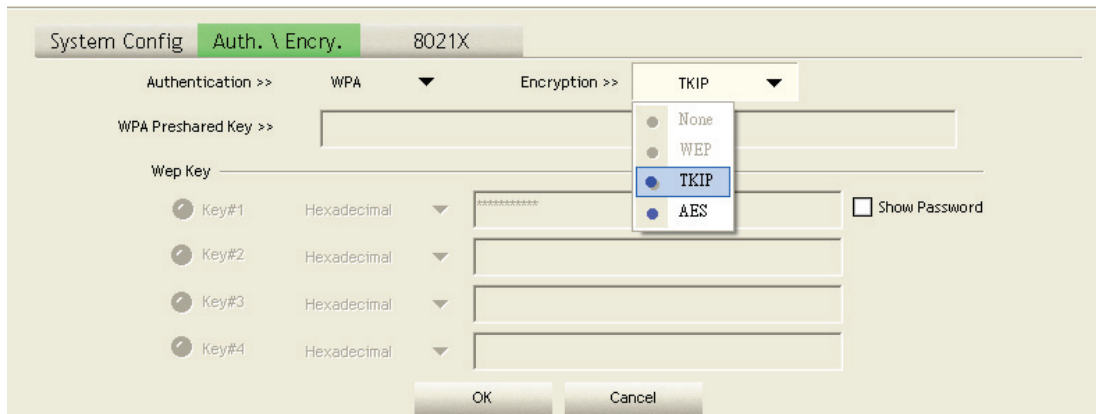
The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.



- **Authentication Type:** Select **Open** or **Shared** from the drop-down list.
- **Encryption:** Select **WEP** from the drop-down list.
- **WEP Key:** Type a character string into the field.  
For 64-bit enter 5 alphanumeric or 10 hexadecimal characters.  
For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

### 3.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



- **Authentication Type:** Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

### 3.4.3 WPA-PSK Authentication & TKIP, AES Encryption

WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

The screenshot shows the 'System Config' window with the 'Auth. \ Encry.' tab selected. The 'Authentication' dropdown is set to 'WPA-PSK' and the 'Encryption' dropdown is set to 'TKIP'. A 'WPA Preshared Key' field is present. Below it, there are four 'Wep Key' entries, each with a radio button, a label (Key#1 to Key#4), a 'Hexadecimal' dropdown, and a text input field. A 'Show Password' checkbox is located to the right of the first key field. 'OK' and 'Cancel' buttons are at the bottom.

- **Authentication Type:** Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- **WPA Preshared key:** Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

### 3.4.4 LEAP Authentication

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

The screenshot shows a configuration window for 802.1X authentication. The window has a title bar with 'System Config', 'Auth. \ Encry.', and '802.1X'. Below the title bar, there is a breadcrumb 'Authentication >>' and a dropdown menu set to 'LEAP'. The main area contains three text input fields: 'Identity >>' with 'admin', 'Password >>' with '\*\*\*\*\*', and 'Domain Name >>' with 'domain.com'. To the right of the password field is a checkbox labeled 'Show Password'. Below the input fields are three radio button options for encryption: 'WEP', 'WPA-TKIP', and 'WPA2-AES', all of which are selected. At the bottom of the window are 'OK' and 'Cancel' buttons.

- **Authentication Type:** Select **LEAP** from the drop-down list.
- **Identity:** Enter the user name.
- **Password:** Enter the password.
- **Domain:** Enter a domain name.
- **Encryption:** Select **WEP**, **WPA-TKIP** or **WPA2-AES** encryption.
- Click on the **OK** button to save the changes.

### 3.4.5 802.1x with PEAP

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

#### 3.4.5.1 PEAP AUTHENTICATION WITH EAP/TLS SMARTCARD

EAP/TLS Smartcard provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

The screenshot shows a configuration window for 802.1X. At the top, there are tabs for 'System Config', 'Auth. \ Encry.', and '802.1X'. Below these, there are dropdown menus for 'EAP Method >>' (set to PEAP) and 'Tunnel Authentication >>' (set to EAP-TLS/SmartCard). A 'Session Resumption' checkbox is checked. The 'ID \ PASSWORD' tab is active, showing two sections: 'Authentication ID / Password' and 'Tunnel ID / Password'. Each section has 'Identity >>', 'Password >>', and 'Domain Name >>' fields. A 'Show Password' checkbox is located at the bottom of the form. 'OK' and 'Cancel' buttons are at the bottom of the window.

- **Authentication Type:** Select **PEAP** from the drop-down list.
- **Protocol:** If your network uses TLS or Smart Card to authenticate its users, select **TLS/Smartcard** from the drop down list. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.
- **Identity:** Enter the user name.
- Click on the **OK** button to save the changes.

### 3.4.6 802.1x with TTLS with EAP-MD5, MS-CHAP, MS-CHAPv2

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate based authentication of both the client and authentication server.

The screenshot shows a configuration window for 802.1X authentication. The window title is "System Config Auth. \ Encry. 8021X". At the top, there are dropdown menus for "EAP Method >>" (set to PEAP) and "Tunnel Authentication >>" (set to EAP-MSCHAP v2). A "Session Resumption" checkbox is checked. Below these are three tabs: "ID \ PASSWORD" (selected), "Client Certification", and "Server Certification". The "ID \ PASSWORD" section contains two groups of fields. The first group, "Authentication ID / Password", includes "Identity >>", "Password >>", and "Domain Name >>". The second group, "Tunnel ID / Password", includes "Identity >>", "Password >>", and a "Show Password" checkbox. At the bottom of the window are "OK" and "Cancel" buttons.

- **Authentication Type:** Select **TTLS** from the drop-down list.
- **Protocol:** Select **EAP-MSCHAP v2**, **MS-CHAP**, or **CHAP** from the drop-down list.
- **Identity:** Enter the user name.
- **Password:** Enter the password.
- Click on the **OK** button to save the changes.

### 3.4.7 802.1x CA Server

Depending on the EAP in use, only the server or both the server and client may be authenticated and require a certificate. Server certificates identify a server, usually an authentication or RADIUS server to clients. Most EAPs require a certificate issued by a root authority or a trusted commercial Certificate Authority.

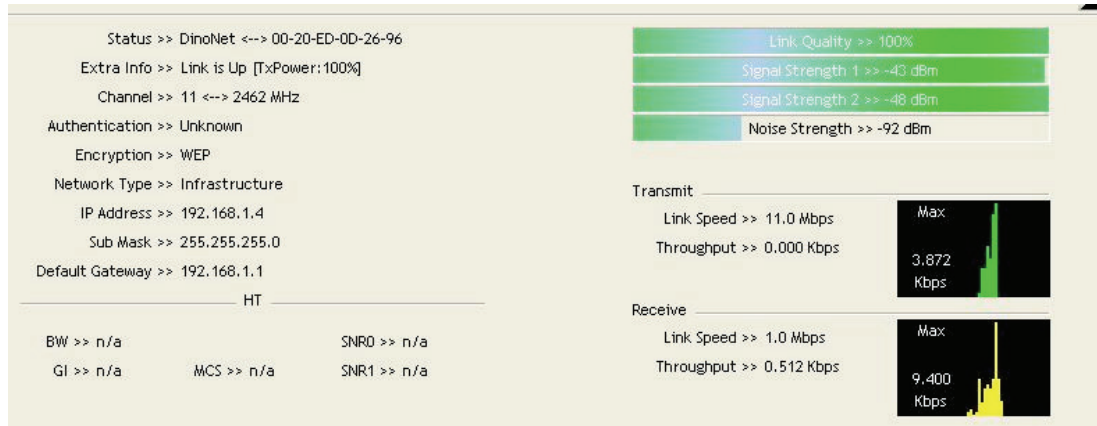
The screenshot shows the 'Client Certification' tab in the 802.1x configuration window. The 'Use Client certificate' checkbox is checked. Below it, there are fields for 'Issued To >>', 'Issued By >>', 'Expired On >>', and 'Friendly Name >>'. The 'OK' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Server Certification' tab in the 802.1x configuration window. The 'Use certificate chain' checkbox is checked. Below it, there is a dropdown menu for '- Any Trusted CA -', an unchecked checkbox for 'Allow intermediate certificates', and a text field for 'Server name >>'. There are also two checked radio buttons: 'Server name must match' and 'Domain name must end in specified name'. The 'OK' and 'Cancel' buttons are at the bottom.

- **Use certificate chain:** Place a check in this to enable the certificate use.
- **Certificate issuer:** Select the Certification Authority from the drop-down list.
- **Allow intermediate certificates:** During tunnel creation the client must verify the server's certificate. When checking this certificate the signature is verified against a list of trusted certificate authorities. If this parameter is true then the client will also accept a signature from a trusted intermediate certificate authority, otherwise it will not.
- **Server name:** Enter the server name if not selected from the existing drop-down list above.
- Click on the **OK** button to save the changes.

### 3.5 Network

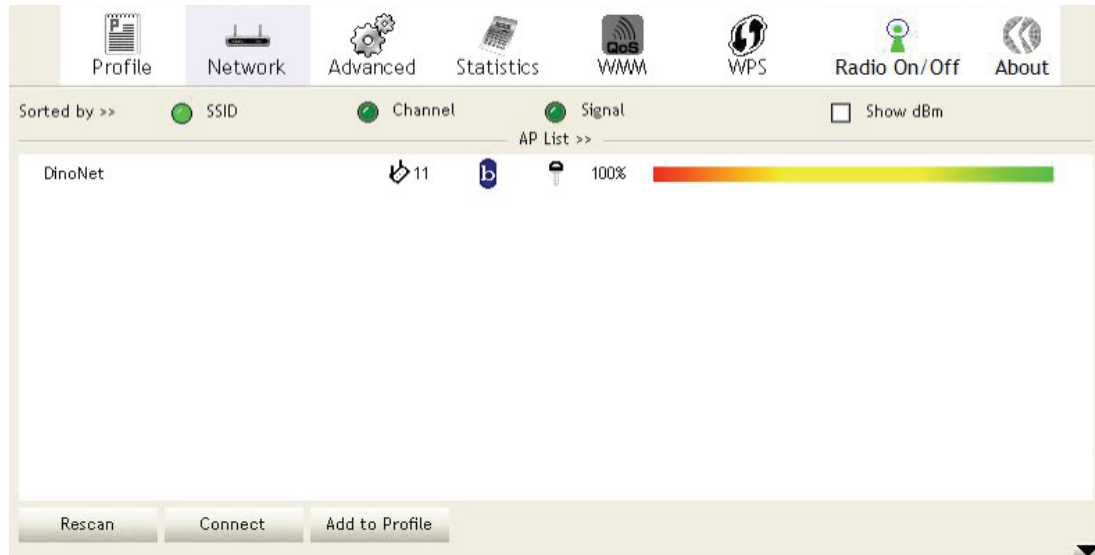
The **Network** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.



- **Status:** This indicates the state of the client. There are three options:
  - **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
  - **Scanning:** Indicates that the wireless client is searching for an AP in the area.
  - **Disconnected:** Indicates that there are no APs or clients in the area.
- **Extra Info:** Displayed here are information about the link stats and the percent of output power.
- **Channel:** The operating frequency channel that the client is using (infrastructure mode).
- **Authentication:** Displays the authentication type.
- **Encryption:** Displays the encryption type.
- **Network Type:** Displays the network type; infrastructure or ad-hoc.
- **IP Address:** Displays the IP address.
- **Sub Mask:** Displays the subnet mask IP address.
- **Default Gateway:** Displays the IP address of the default gateway.
- **Link Speed:** The current rate at which the client is transmitting and receiving.
- **Transmit/Receive Throughput:** Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- **Link Quality:** In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- **Signal Strength:** This bar displays the strength of the signal received from an AP or client.
- **Noise Level:** Displays the background noise level; a lower level indicates less interference.
- Click on the **OK** button to close this window.

### 3.5.1 Site Survey

The **Network** tab also displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.



- **SSID:** Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Channel:** Displays the channel number of the Access Point.
- **Encryption:** Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- **Signal:** Displays the receiving signal strength from the Access Point.
- **Rescan:** Click on this button to view a list of Access Points in the area.
- **Connect:** to connect with a specific Access Point, select the SSID from the list, and then click on the Connect button.
- **Add to Profile:** Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

## 3.6 Advanced Configuration

The **Advanced** tab is used to configure the wireless mode (802.11g, 802.11b/g-mixed, or 802.11b/g/n-mixed), Tx burst, and CCX.

- **Wireless mode:** Select **802.11 b/g/n** mix if the wireless network uses both 11b, 11g, and 11n stations and APs. **B/G Protection:** This is the ERP protection mode of 802.11g. Selecting **auto** will dynamically send frames with and without protection. Select **On** to send a frame without protection, and **Off** to send it with protection.
- **Enable Tx BURST:** Click the check box will enhance the throughput
- **Enable TCP Window Size:** Enhance the throughput if enable this function.
- **CCX:** Enable this option if the network supports Cisco Compatible Extensions.
- Click on the **Apply** button to close this window.

## 3.7 Statistics

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.

Transmit		Receive	
Frames Transmitted Successfully	=		1934
Frames Retransmitted Successfully	=		0
Frames Fail To Receive ACK After All Retries	=		0
RTS Frames Successfully Receive CTS	=		0
RTS Frames Fail To Receive CTS	=		0

Reset Counter

### 3.8 WMM (Wireless Multimedia)

Click on the **WMM** tab. Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories), however it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

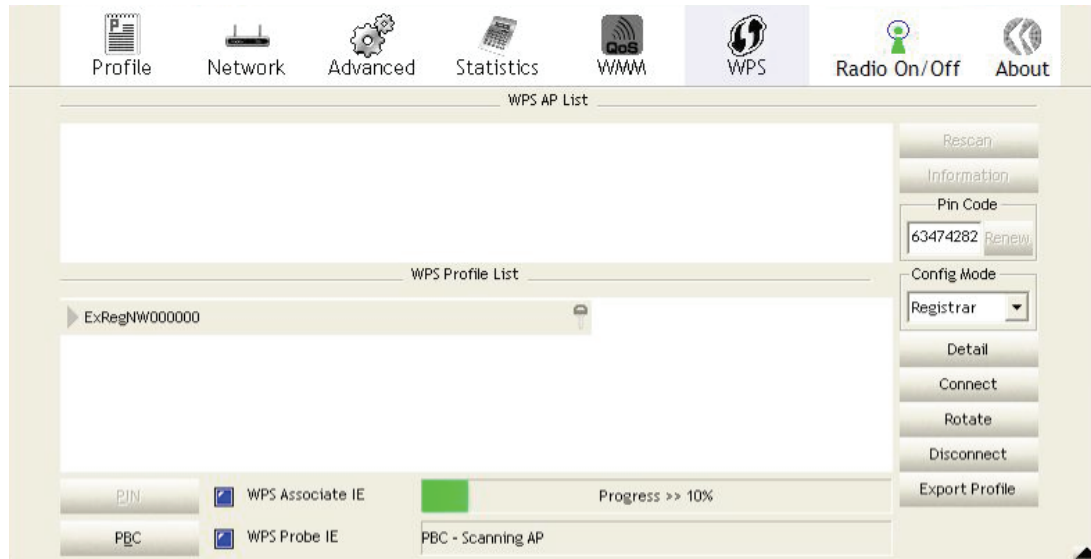
The screenshot shows the WMM Setup Status window with the following settings:

- WMM >> Enabled
- Power Save >> Enabled:AC\_BE:AC\_BK:AC\_VI:AC\_VO
- Direct Link >> Enabled
- WMM Enable
- WMM - Power Save Enable
- AC\_BK
- AC\_BE
- AC\_VI
- AC\_VO
- Direct Link Setup Enable
- MAC Address >> [ ][ ][ ][ ][ ][ ]
- Timeout Value >> 60 sec
- Buttons: Apply, Tear Down

- **WMM Enable:** Choose to enable or disable WMM.
- **WMM Power Save Enable:** Choose to enable or disable power save mode on WMM.
- **Direct Link Setup Enable:** Specify a MAC address and timeout value.
- Click on the **Apply** button to close this window.

### 3.9 WPS

WPS is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.



- **Rescan:** Click on this button to view a list of Access Points in the area.
- **WPS Information:** Display the information about WPS on the selected network. List information include Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands
- **Pin Code:** 8-digit numbers. It is required to enter PIN Code into **Registrar** using PIN method. When HNW300CI is **Enrollee**, you can use "Renew" button to re-generate new PIN Code.
- **Config Mode:** The HNW300CI role-playing as an **Enrollee** or an external **Registrar**
- **Detail:** Information about Security and Key in the credential.
- **Connect:** Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
- **Rotate:** Command to rotate to connect to the next network inside credentials.
- **Disconnect:** Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exist. If there is an empty profile page, the driver will select any non-security AP.
- **Export Profile:** Export all credentials to Profile.
- **PBC:** Start to add to AP using PBC configuration method.
- **WPS Associate IE:** Send the association request with WPS IE during WPS setup. It is optional for HNW300CI.
- **WPS Probe IE:** Send the probe request with WPS IE during WPS setup. It is optional for HNW300CI.
- Click on the **OK** button if you have made any changes.

### 3.10 About

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.



### 3.11 Radio

The **Radio** tab allows you to enable or disable the radio.



## 3.12 Uninstall the Drivers & Client Utility

If the PCI CARD installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the PCI Card Adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

- Click on **Start > Hamlet HNW300CI > Uninstall Hamlet HNW300CI**
- The **un-installation** process will then begin.
- Click on the **Yes** button to confirm the un-installation process.
- Then click on the **Finish** button. Then remove the PCI CARD.

## 4. Appendix A – Glossary

### 8

#### 802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

### A

#### Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

#### Access Point

AP. Device that allows wireless clients to connect to it and access the network

#### ActiveX

A Microsoft specification for the interaction of software components.

#### Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

#### Ad-hoc network

Peer-to-Peer network between wireless clients

#### ADSL

Asymmetric Digital Subscriber Line

#### Advanced Encryption Standard

AES. Government encryption standard

#### Alphanumeric

Characters A-Z and 0-9

#### Antenna

Used to transmit and receive RF signals.

#### AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

#### Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

#### ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

#### Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

#### Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

#### Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

### B

#### Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

**Bandwidth**

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

**Basic Input/Output System**

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

**Baud**

Data transmission speed

**Beacon**

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

**Bit rate**

The amount of bits that pass in given amount of time

**Bit/sec**

Bits per second

**BOOTP**

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

**Bottleneck**

A time during processes when something causes the process to slowdown or stop all together

**Broadband**

A wide band of frequencies available for transmitting data

**Broadcast**

Transmitting data in all directions at once

**Browser**

A program that allows you to access resources on the web and provides them to you graphically

**C****Cable modem**

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

**CardBus**

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

**CAT 5**

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

**Client**

A program or user that requests data from a server

**Collision**

When do two devices on the same Ethernet network try and transmit data at the exact same time.

**Cookie**

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

**D****Data**

Information that has been translated into binary so that it can be processed or moved to another device

**Data Encryption Standard**

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

**Database**

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

**Data-Link layer**

The second layer of the OSI model. Controls the movement of data on the physical link of a network

**DB-25**

A 25 pin male connector for attaching External modems or RS-232 serial devices

**DB-9**

A 9 pin connector for RS-232 connections

**dBd**

Decibels related to dipole antenna

**dBi**

Decibels relative to isotropic radiator

**dBm**

Decibels relative to one milliwatt

**Decrypt**

To unscramble an encrypted message back into plain text

**Default**

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

**Demilitarized zone**

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

**DHCP**

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

**Digital certificate:**

An electronic method of providing credentials to a server in order to have access to it or a network

**Direct Sequence Spread Spectrum**

DSSS: Modulation technique used by 802.11b wireless devices

**DMZ**

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

**DNS**

Domain Name System: Translates Domain Names to IP addresses

**Domain name**

A name that is associated with an IP address

**Download**

To send a request from one computer to another and have the file transmitted back to the requesting computer

**DSL**

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

**Duplex**

Sending and Receiving data transmissions at the same time

**Dynamic DNS service**

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

**Dynamic IP address**

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

**E****EAP**

Extensible Authentication Protocol

**Email**

Electronic Mail is a computer-stored message that is transmitted over the Internet

**Encryption**

Converting data into cyphertext so that it cannot be easily read

**Ethernet**

The most widely used technology for Local Area Networks.

**F****Fiber optic**

A way of sending data through light impulses over glass or plastic wire or fiber

**File server**

A computer on a network that stores data so that the other computers on the network can all access it

**File sharing**

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

**Firewall**

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

**Firmware**

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

**FTP**

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

**Full-duplex**

Sending and Receiving data at the same time

**G****Gain**

The amount an amplifier boosts the wireless signal

**Gateway**

A device that connects your network to another, like the internet

**Gbps**

Gigabits per second

**Gigabit Ethernet**

Transmission technology that provides a data rate of 1 billion bits per second

**GUI**

Graphical user interface

**H****H.323**

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

**Half-duplex**

Data cannot be transmitted and received at the same time

**Hashing**

Transforming a string of characters into a shorter string with a predefined length

**Hexadecimal**

Characters 0-9 and A-F

**Hop**

The action of data packets being transmitted from one router to another

**Host**

Computer on a network

**HTTP**

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

**HTTPS**

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

**Hub**

A networking device that connects multiple devices together

**I****ICMP**

Internet Control Message Protocol

**IEEE**

Institute of Electrical and Electronics Engineers

**IGMP**

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

**IIS**

Internet Information Server is a WEB server and FTP server provided by Microsoft

**IKE**

Internet Key Exchange is used to ensure security for VPN connections

**Infrastructure**

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

**Internet**

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

**Internet Explorer**

A World Wide Web browser created and provided by Microsoft

**Internet Protocol**

The method of transferring data from one computer to another on the Internet

**Internet Protocol Security**

IPsec provides security at the packet processing layer of network communication

**Internet Service Provider**

An ISP provides access to the Internet to individuals or companies

**Intranet**

A private network

**Intrusion Detection**

A type of security that scans a network to detect attacks coming from inside and outside of the network

**IP**

Internet Protocol

**IP address**

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

**IPsec**

Internet Protocol Security

**IPX**

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

**ISP**

Internet Service Provider

**J****Java**

A programming language used to create programs and applets for web pages

**K****Kbps**

Kilobits per second

**Kbyte**

Kilobyte

**L****L2TP**

Layer 2 Tunneling Protocol

**LAN**

Local Area Network

**Latency**

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

**LED**

Light Emitting Diode

**Legacy**

Older devices or technology

**Local Area Network**

A group of computers in a building that usually access files from a server

**LPR/LPD**

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

**M****MAC Address**

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

**Mbps**

Megabits per second

**MDI**

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

**MDIX**

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

**MIB**

Management Information Base is a set of objects that can be managed by using SNMP

**Modem**

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

**MPPE**

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

**MTU**

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

**Multicast**

Sending data from one device to many devices on a network

**N****NAT**

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

**NetBEUI**

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

**NetBIOS**

Network Basic Input/Output System

**Netmask**

Determines what portion of an IP address designates the Network and which part designates the Host

**Network Interface Card**

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

**Network Layer**

The third layer of the OSI model which handles the routing of traffic on a network

**Network Time Protocol**

Used to synchronize the time of all the computers in a network

**NIC**

Network Interface Card

**NTP**

Network Time Protocol

**O****OFDM**

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

**OSI**

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

**OSPF**

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

**P****Password**

A sequence of characters that is used to authenticate requests to resources on a network

**Personal Area Network**

The interconnection of networking devices within a range of 10 meters

**Physical layer**

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

**Ping**

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

**PoE**

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

**POP3**

Post Office Protocol 3 is used for receiving email

**Port**

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

**PPP**

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

**PPPoE**

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

**PPTP**

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

**Preamble**

Used to synchronize communication timing between devices on a network

**Q****QoS**

Quality of Service

**R****RADIUS**

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

**Reboot**

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

**Rendezvous**

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

**Repeater**

Retransmits the signal of an Access Point in order to extend it's coverage

**RIP**

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

**RJ-11**

The most commonly used connection method for telephones

**RJ-45**

The most commonly used connection method for Ethernet

**RS-232C**

The interface for serial communication between computers and other related devices

**RSA**

Algorithm used for encryption and authentication

**S****Server**

A computer on a network that provides services and resources to other computers on the network

**Session key**

An encryption and decryption key that is generated for every communication session between two computers

**Session layer**

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

**Simple Mail Transfer Protocol**

Used for sending and receiving email

**Simple Network Management Protocol**

Governs the management and monitoring of network devices

**SIP**

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

**SMTP**

Simple Mail Transfer Protocol

**SNMP**

Simple Network Management Protocol

**SOHO**

Small Office/Home Office

**SPI**

Stateful Packet Inspection

**SSH**

Secure Shell is a command line interface that allows for secure connections to remote computers

**SSID**

Service Set Identifier is a name for a wireless network

**Stateful inspection**

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass through the firewall

**Subnet mask**

Determines what portion of an IP address designates the Network and which part designates the Host

**Syslog**

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

**T****TCP**

Transmission Control Protocol

**TCP Raw**

A TCP/IP protocol for transmitting streams of printer data.

**TCP/IP**

Transmission Control Protocol/Internet Protocol

**TFTP**

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

**Throughput**

The amount of data that can be transferred in a given time period

**Traceroute**

A utility displays the routes between your computer and specific destination

**U****UDP**

User Datagram Protocol

**Unicast**

Communication between a single sender and receiver

**Universal Plug and Play**

A standard that allows network devices to discover each other and configure themselves to be a part of the network

**Upgrade**

To install a more recent version of a software or firmware product

**Upload**

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

**UPnP**

Universal Plug and Play

**URL**

Uniform Resource Locator is a unique address for files accessible on the Internet

**USB**

Universal Serial Bus

**UTP**

Unshielded Twisted Pair

**V****Virtual Private Network**

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

**VLAN**

Virtual LAN

**Voice over IP**

Sending voice information over the Internet as opposed to the PSTN

**VoIP**

Voice over IP

**W****Wake on LAN**

Allows you to power up a computer through its Network Interface Card

**WAN**

Wide Area Network

**WCN**

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

**WDS**

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

**Web browser**

A utility that allows you to view content and interact with all of the information on the World Wide Web

**WEP**

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

**Wide Area Network**

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

**Wi-Fi**

Wireless Fidelity

**Wi-Fi Protected Access**

An updated version of security for wireless networks that provides authentication as well as encryption

**Wireless ISP**

A company that provides a broadband Internet connection over a wireless connection

**Wireless LAN**

Connecting to a Local Area Network over one of the 802.11 wireless standards

**WISP**

Wireless Internet Service Provider

**WLAN**

Wireless Local Area Network

**WPA**

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP

**X****xDSL**

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

**Y****Yagi antenna**

A directional antenna used to concentrate wireless signals on a specific location

## 5. Appendix B – Specifications

### Data Rates

1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 72, 84, 150 and 300Mbps (300 Rx PHY rate; 150Mbps Tx PHY support)

### Standards / Compliance

IEEE802.3, IEEE802.3u, IEEE802.11b, IEEE802.11g, 802.11n (2.0)

### Regulation Certifications

FCC Part 15, ETSI 300/328/CE

### Operating Voltage

3.3V ± 0.25V

### Status LEDs

LINK/ACTIVITY

### Drivers

Windows 2000/XP/Vista

### RF INFORMATION

#### Frequency Band

U.S., Europe and Japan product covering 2.4 to 2.484 GHz, programmable for different country regulations

#### Media Access Protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

#### Modulation Technology

802.11g: OFDM (64-QAM, 16-QAM, QPSK, BPSK)  
802.11b: DSSS (DBPSK, DQPSK, CCK)

#### Operating Channels

11 for North America, 14 for Japan, 13 for Europe

#### Receive Sensitivity (Typical)

- 2.412~2.472G(IEEE802.11b) (1Rx)  
-91dBm @ 1Mbps  
-87dBm @ 11Mbps

- 2.412~2.472G(IEEE802.11g) (2Rx)  
-90dBm @ 6Mbps  
-75dBm @ 54Mbps
- 2.412~2.472G(IEEE802.11N) (2Rx)  
-88 dBm MCS 8  
-65 dBm MCS 15

#### Available transmit power

- 2.412~2.472G(IEEE802.11b)  
18dBm @1~11Mbps
- 2.412~2.472G(IEEE802.11g)  
15 dBm @6Mbps  
14 dBm @54Mbps
- 2.412~2.472G(IEEE802.11N)  
15dBm

#### Antenna Configuration

1T2R Mode

### NETWORKING

#### Topology

Ad-Hoc, Infrastructure

#### Security

WPA/WPA2 (AES, 64,128-WEP with shared-key authentication)

### PHYSICAL

#### Form Factor

PCI Card

### ENVIRONMENTAL

#### Temperature Range

Operating: 0°C to 45°C  
Storage: -10°C to 70°C

#### Humidity (non-condensing)

15%~95% Typical

#### Package Contents

- Wireless-N PCI Card
- Two Detachable Antennas
- User's Manual
- CD-ROM with Drivers and Manual

## 6. Appendix C – FCC Interference Statement

### Federal Communication Commission Interference Statement

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

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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

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