

# **Wireless\_N PCI Adaptor**

## **PC812Rn**

---

---

### **User Guide**

---

---



# Table of Contents

---

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
<b>Package Contents .....</b>	<b>1</b>
<b>LEDs .....</b>	<b>1</b>
<b>Operation .....</b>	<b>1</b>
<b>CHAPTER 2 INITIAL INSTALLATION .....</b>	<b>2</b>
<b>Requirements .....</b>	<b>2</b>
<b>Procedure .....</b>	<b>2</b>
<b>CHAPTER 3 USING THE WINDOWS UTILITY .....</b>	<b>5</b>
<b>Overview .....</b>	<b>5</b>
<b>System Tray Icon .....</b>	<b>5</b>
<b>Auto Profile Connect .....</b>	<b>6</b>
<b>Site Survey Screen .....</b>	<b>6</b>
<b>Profile Manager Screen .....</b>	<b>9</b>
<b>Network Status Screen .....</b>	<b>14</b>
<b>About Screen .....</b>	<b>16</b>
<b>APPENDIX A SPECIFICATIONS .....</b>	<b>17</b>
<b>Wireless Adapter .....</b>	<b>17</b>
<b>APPENDIX B ABOUT WIRELESS LANS .....</b>	<b>18</b>
<b>Modes .....</b>	<b>18</b>
<b>BSS/ESS .....</b>	<b>18</b>
<b>Channels .....</b>	<b>19</b>
<b>WEP &amp; WPA-PSK .....</b>	<b>19</b>
<b>WPA2-PSK .....</b>	<b>19</b>
<b>Wireless LAN Configuration .....</b>	<b>20</b>

P/N: 956YK80001

Copyright © 2008. All Rights Reserved.

Document Version: 1.0 (January, 2008)

All trademarks and trade names are the properties of their respective owners.



# Chapter 1



# Introduction

*This Chapter provides an overview of the Wireless Adapter's features and capabilities.*

Congratulations on the purchase of your new Wireless Adapter. The Wireless Adapter provides a wireless network interface for your Notebook or PC.

## Package Contents

The following items should be included:

- The Wireless Adapter Unit
- 2 Antennas
- Quick Start Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

## LEDs

### Wireless Adapter

The Wireless Adapter has a single Link/Activity LED.

<b>Link/Act LED</b>	<ul style="list-style-type: none"><li>• On - Associated with the network.</li><li>• Off - Not associated with the network.</li><li>• Blinking - Data being transferred.</li></ul>
---------------------	---

## Operation

**You should install the supplied software on the CD-ROM before inserting the Wireless adapter.**

## Chapter 2

# Initial Installation



*This Chapter covers the software installation of the Wireless Adapter.*

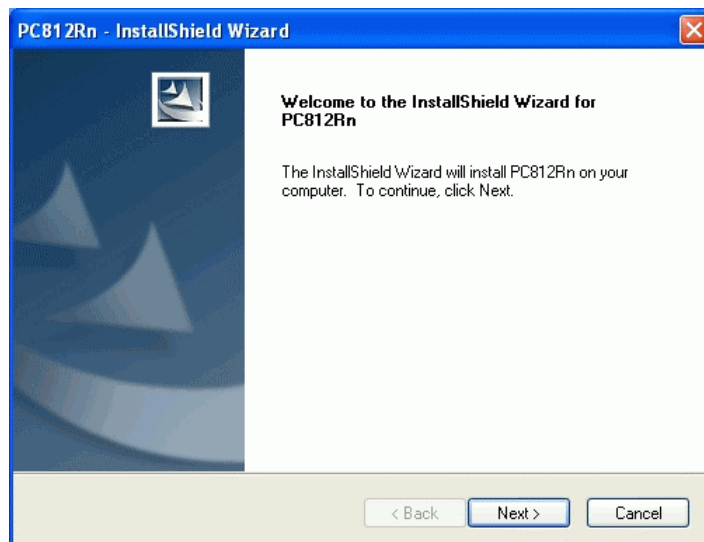
### Requirements

- Windows 2000/XP/Vista.
- CD-ROM drive.
- IEEE802.11n, IEEE802.11b or IEEE802.11g wireless LAN.

### Procedure

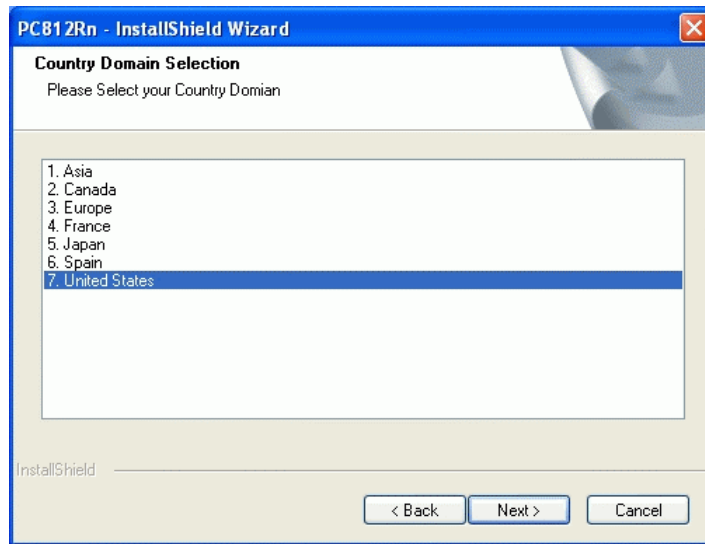
**You should install the supplied software BEFORE inserting the Wireless Adapter.**

1. Insert the CD-ROM into the drive on your PC.
2. The installation program should start automatically. If it does not, run the SETUP.EXE program.
3. Select the desired installation language on the screen.



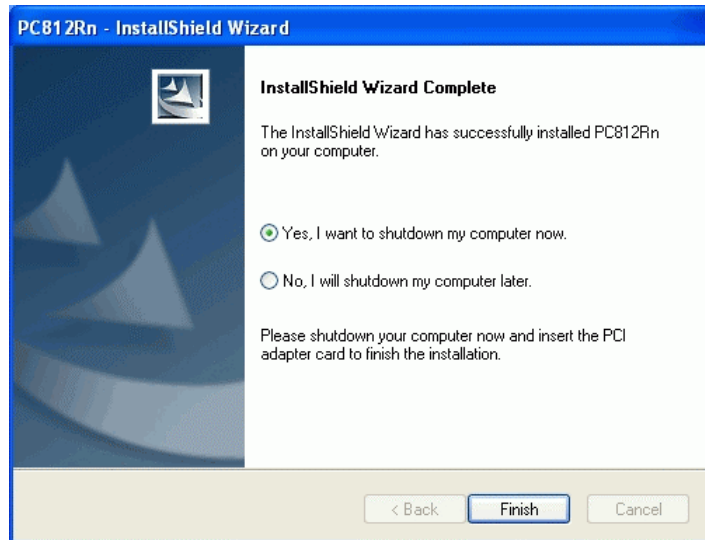
**Figure 1: Start Installation**

4. On the screen above, click "Next" to start the installation.
5. Select the location on the screen.



**Figure 2: Country Domain Screen**

6. Step through the procedure.
7. After the installation is complete, select *Yes, I want to shutdown my computer now* and then click "Finish".



**Figure 3: Installation Screen**




8. Insert the Card into your computer.
  - Remove the cover on one side of the computer.
  - Find an empty PCI expansion slot inside the computer.
  - Press the Card firmly into the slot.
  - Connect the supplied antenna cable to the port on the Card.
  - Replace the computer's cover and power it on.
9. The Windows "New Hardware" wizard will then start.
  - Select *Install the software automatically* to allow it to complete the installation of the Windows driver

10. When the Windows wizard is complete, you will now have a new icon in your system tray, as shown below.



**Figure 4: System Tray Icon**

**Wireless Adapter Icon Table**

	Connection to the Wireless Adapter is established. The length of green color indicates the signal strength.
	No connection to the Wireless Adapter.
	The Wireless Adapter is unplugged.

11. You can double-click this icon to configure the Wireless interface. See the following chapter for details.



## Chapter 3

# 3

# Using the Windows Utility

*This Chapter provides Setup details for the AP mode of the Wireless Adapter.*

## Overview

If using Windows, you can use the supplied utility to configure the Wireless interface.

### To Use the supplied Windows utility for Configuration

- Double-click the *PC812Rn WLAN Application* icon in the desktop.
- Click *Start - Programs - SerComm - PC812Rn - WLAN Application*.

This Chapter assumes you are using the supplied **WLAN Application** utility.

## System Tray Icon

If the WLAN Application program is running, you can double-click the icon in the System Tray or right-click the icon and select "Restore" to open the application.

## Status Information

The menu options available from the System Tray icon are:

- **Restore** - This will display the main screen.
- **Radio Off** - The wireless adapter is not associated with the network when the radio is off.
- **WZC On** - Click this to turn the Wireless Zero Configuration on.
- **Exit** - Terminate the connection to the Wireless Adapter.



**Figure 5: Wireless Adapter menu**

## Connecting to a Wireless Network

Double-click the Icon to open the Site Survey screen, when you can select the Wireless network you wish to join.

## Auto Profile Connect

Normally, this option should be enabled. The adapter will then connect to an available network which was connected successfully last time.

There are various methods to specify the required network.

- On the Profile Manager tab, select the desired profile in the list, and click the Apply Profile button.
- On the Site Survey tab, either double-click the network in the list, or select the network and click the Connect button.

## Site Survey Screen

This screen is displayed when you double-click the system tray icon. You can also click the Site Survey Tab in the screen.

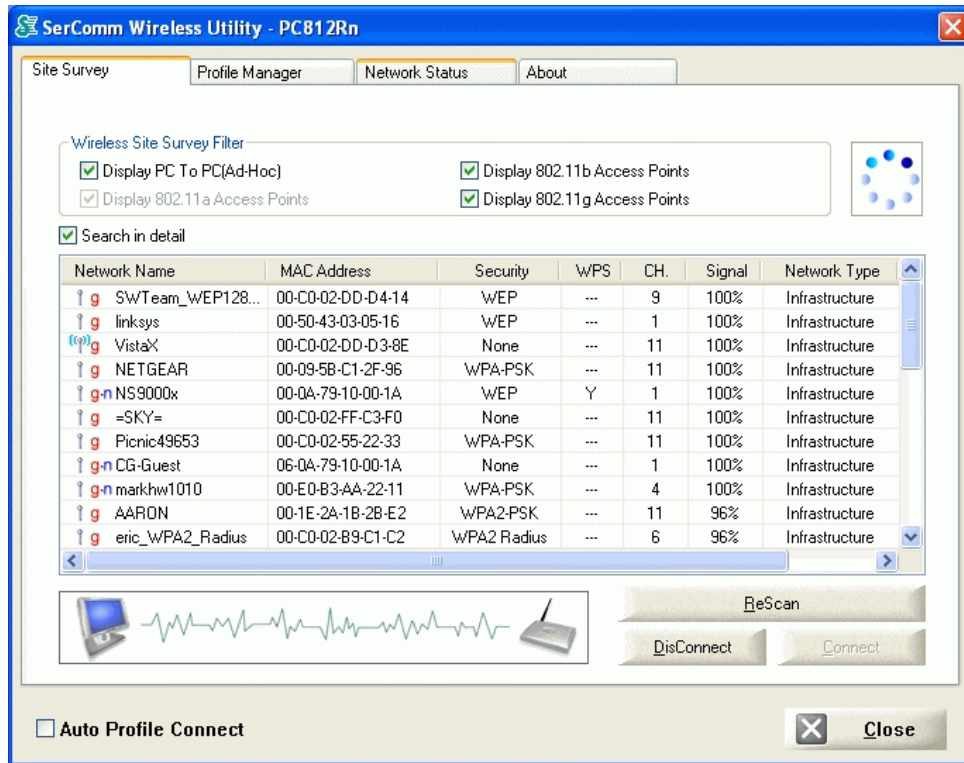


Figure 6: Site Survey Screen

### Data - Site Survey Screen

**Display PC To PC (Ad-Hoc)**

Select this check box to display ad-hoc (computer-to-computer) networks.

<b>Display 802.11b Access Points</b>	Select this check box to display 802.11b (infrastructure) networks.
<b>Display 802.11a Access Points</b>	Select this check box to display 802.11a (infrastructure) networks.
<b>Display 802.11g Access Points</b>	Select this check box to display 802.11g (infrastructure) networks.
<b>Network Name</b>	Available wireless networks are listed.
<b>MAC Address</b>	This is the MAC address of the Access Point (or Wireless station, if the network is an Ad-hoc network).
<b>Security</b>	Data encryption and authentication methods used on the wireless network
<b>WPS</b>	It will display "Y" if the Access Point has WPS function.
<b>CH.</b>	The channel used by the Wireless network.
<b>Signal</b>	This is displayed as percentage (0 ~ 100%).
<b>Network Type</b>	This will indicate "Infrastructure" (displayed device is an Access Point) or "Ad-hoc". (displayed device is a Wireless station)
<b>Frequency</b>	The Wireless band used by this Wireless network.
<b>Status</b>	The area to the left of the "Rescan" button shows the current status. In the example above, it shows "Connected".
<b>Rescan</b>	Click this button to rescan for all Wireless networks.
<b>Disconnect</b>	Click this button to exit the current Wireless network.
<b>Connect</b>	Click this button to connect the Wireless network.

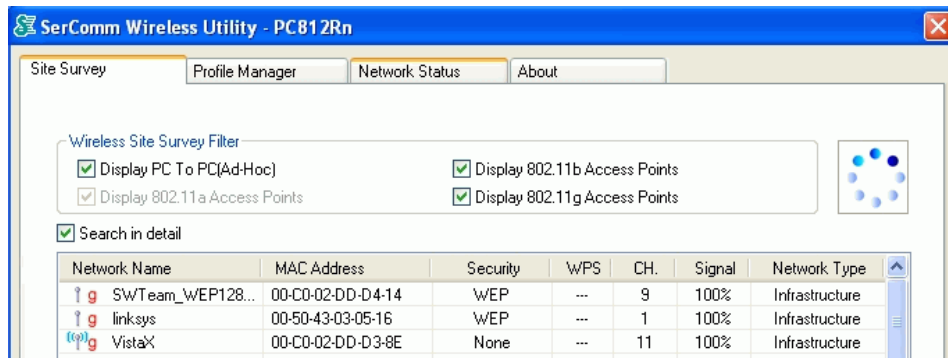
### Wireless Network Sequence (order)

You can click the headings (ex. Network Name, MAC Address, Security...) of the Wireless network table to arrange the Wireless network in the desired order.

### To Connect to a Wireless Network

- Double-click on the desired network.
- Click the name of the wireless network to which you want to connect, and then click **Connect**.

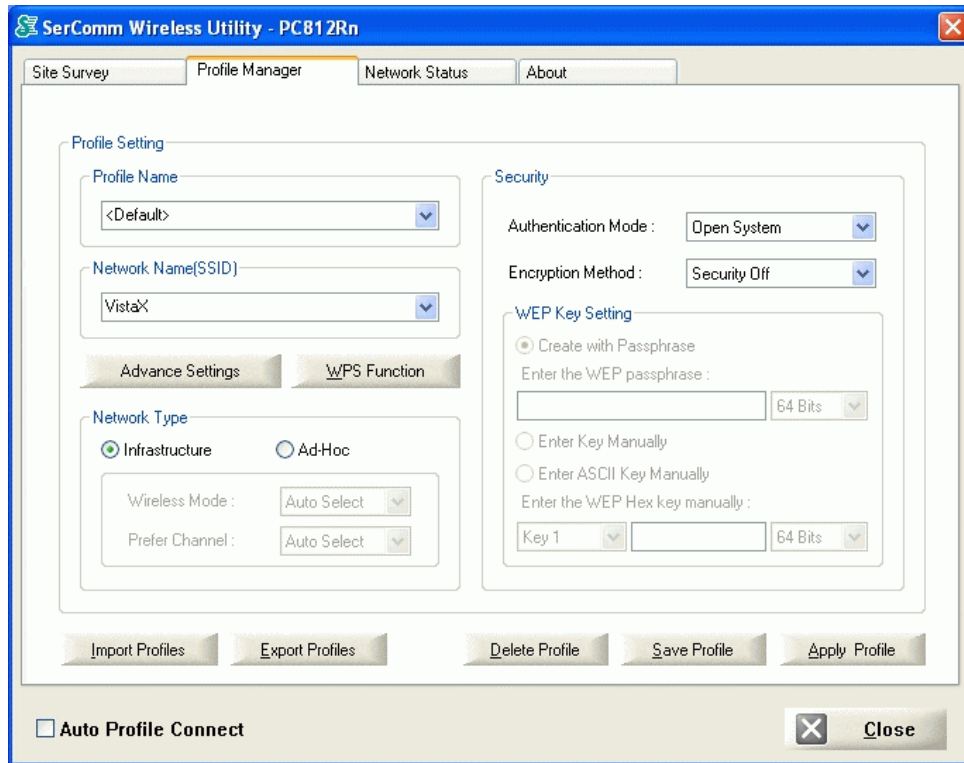
Note that once you are connected to a Wireless network, the **Site Survey** screen will identify the current wireless network with a blue icon, as shown below.



**Figure 7: Site Survey Screen - Connected**

## Profile Manager Screen

This screen is accessed by clicking the *Profile Manager* tab on the main screen.



**Figure 10: Profile Manager Screen**

### Data - Profile Manager Screen

<b>Profile Name</b>	Enter or select a suitable name for this profile. Each profile must have a unique name.
<b>Network Name (SSID)</b>	If the desired wireless network is currently available, you can select its SSID. Otherwise, type in the SSID of the desired wireless network.
<b>Advanced Settings</b>	On the resulting sub-screen, enter the required data for the advanced settings.
<b>WPS Function</b>	Click this button to configure the WPS settings in the sub-screen.
<b>Network Type</b>	Select the desired option: <ul style="list-style-type: none"> <li>• <b>Infrastructure</b> - Select this to connect to an Access point.</li> <li>• <b>Ad-Hoc</b> - Select this if you are connecting directly to another computer.</li> </ul>
<b>Wireless Mode</b>	Select the desired wireless mode to which you want to connect.
<b>Prefer Channel</b>	Select the channel you would like to use.

<b>Authentication Mode</b>	<p>You MUST select the option to match the Wireless LAN you wish to join. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Open System</b> - Broadcast signals are not encrypted. This method can be used only with no encryption or with WEP.</li> <li>• <b>Shared Key</b> - Broadcast signals are encrypted using WEP. This method can only be used with WEP.</li> <li>• <b>Auto Switch</b> - This is another WEP system; it will select either Open System or Shared Key as required.</li> <li>• <b>WPA-PSK</b> - PSK means "Pre-shared Key". You must enter this Passphrase value; it is used for both authentication and encryption.</li> <li>• <b>WPA2-PSK</b> - This is a further development of WPA-PSK, and offers even greater security. You must enter this Passphrase value; it is used for both authentication and encryption.</li> <li>• <b>WPA Radius</b> - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.</li> <li>• <b>WPA2 Radius</b> - This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.</li> </ul>
<b>Encryption Method</b>	<p>The available options depend on the Authentication method selected above. The possible options are:</p> <ul style="list-style-type: none"> <li>• <b>Security Off</b> - No data encryption is used.</li> <li>• <b>WEP</b> - If selected, you must enter the WEP data shown below. This WEP data must match the Access Point or other Wireless stations.</li> <li>• <b>AES, TKIP</b> - These options are available with WPA-PSK, WPA2-PSK, WPA-Radius and WPA2-Radius. Select the correct option.</li> </ul>
<b>Create with Passphrase</b>	<p>Enable this check box and enter a word or group of printable characters in the Passphrase box, select the desired encryption to automatically configure the WEP Key.</p>
<b>Enter Key Manually</b>	<p>Enable this check box and select the desired key in the drop-down list. Then enter the key values you wish to use and select the desired encryption. Other stations must have matching key values.</p>
<b>Enter ASCII Key Manually</b>	<p>Enable this check box and select the desired key in the drop-down list. Then enter the key values you wish to use and select the desired encryption. Other stations must have matching key values.</p>
<b>Passphrase</b>	<p>For WPA-PSK and WPA2-PSK modes, you need to enter the desired value (8~63 characters). Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.</p>

---

<b>Confirm</b>	For WPA-PSK and WPA2-PSK modes, re-enter the value in this field.
<b>802.1x Authentication Protocol</b>	For WPA Radius and WPA2 Radius modes, select the desired option in the drop-down list.
<b>Configure WPA Radius</b>	For WPA Radius and WPA2 Radius modes, click this button to open a sub-window where you can enter details of the Radius Server.

---

**To add a profile**

1. On the Profile Manager tab, complete the settings on this screen.
2. Verify that the settings you configured are correct.
3. Click Save Profile.

**To export profiles**

1. On the Profile Manager tab, click Export Profiles. The Save As dialog box appears.
2. Type a name for the profile that you are saving, and then verify that the file name extension is set to .cfg.
3. Click Save.

**To import profiles**

1. On the Profile Manager tab, click Import Profiles. The open dialog box appears.
2. Select the profile set that you want to import.
3. Click Open.

**To delete a profile**

1. On the Profile Manager tab, select the profile that you want to delete.
2. Click Delete Profile.

**To edit a profile**

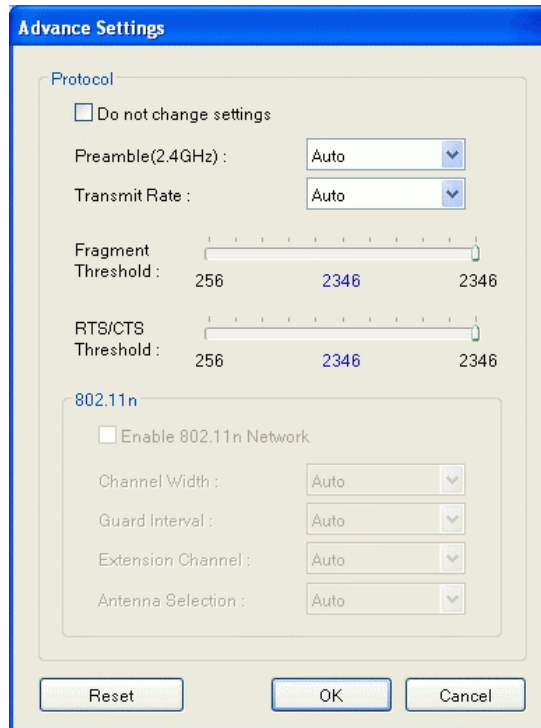
1. On the Profile Manager tab, select the profile that you want to edit.
2. Change the profile settings as necessary.
3. Click Save Profile.

**To enable a profile**

1. In the list of available profiles, click the profile that you want to enable.
2. Click Apply Profile.

## Advanced Settings Screen

Once you have created a profile, as described above, the **Advanced Settings** tab will be available on the Profile Manager screen.



**Figure 8: Advanced Settings Screen**

### Data - Advanced Settings Screen

<b>Do not change settings</b>	Enable this check box if you don't want to modify the settings in this screen.
<b>Preamble (2.4GHz)</b>	Normally, this should be left at "Auto".
<b>Transmit Rate</b>	Use this to manually set the speed, if desired. The default is "Auto".
<b>Fragment Threshold</b>	The default value is 2346. In some cases, you may be able to improve performance by adjusting this value.
<b>RTS/CTS Threshold</b>	The default value is 2346. In some cases, you may be able to improve performance by adjusting this value.
<b>802.11n</b>	
<b>Enable 802.11n Network</b>	Enable this if you want to use the 802.11n network.
<b>Channel Width</b>	Select the desired channel width.
<b>Guard Interval</b>	Use this to manually set the interval, if desired. The default is "Auto".
<b>Extension Channel</b>	Select the desired channel.
<b>Antenna Selection</b>	Select the desired option. The default is set to "Auto".



## WPS Screen

WPS (Wi-Fi Protected Setup) can simplify the process of connecting any device to the wireless network by using the push button configuration (PBC) on the Wireless Access Point, or entering a PIN code.

You will see the WPS screen when you try to connect the wireless network with the WPS function.

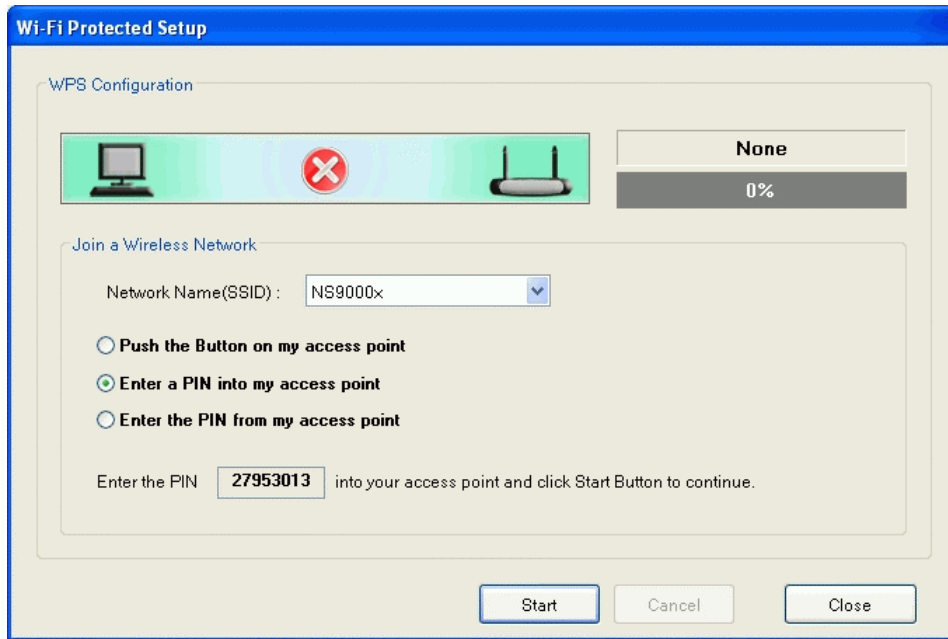


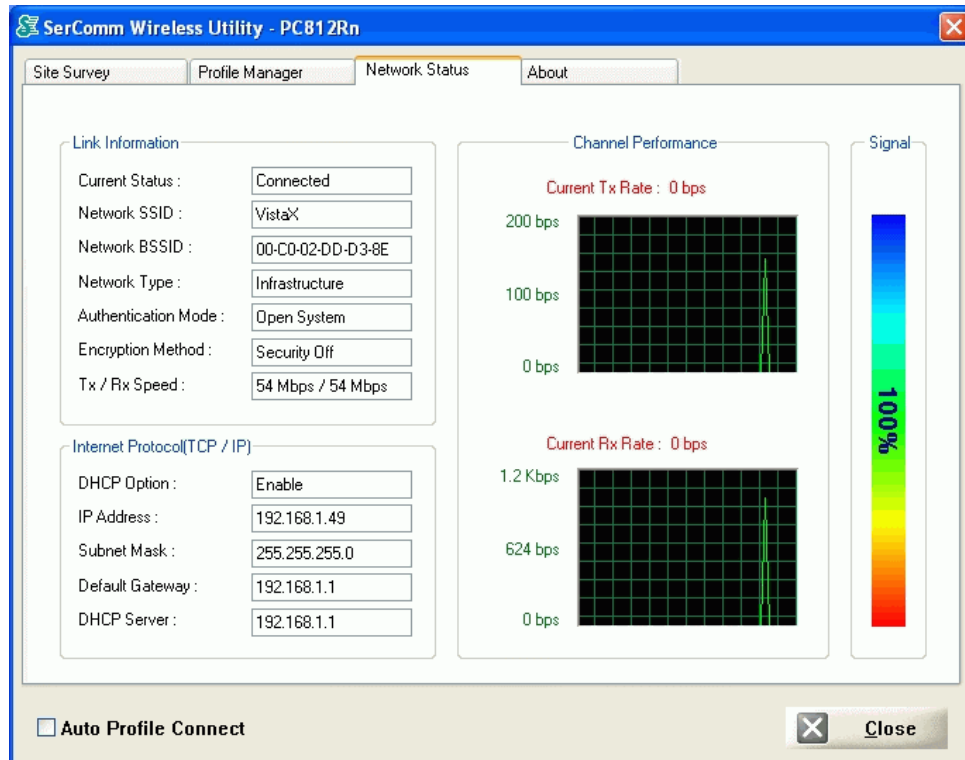
Figure 9: Wi-Fi Protected Setup Screen

### Data - Wi-Fi Protected Setup Screen

<b>WPS Status</b>	The image indicates the status of WPS.
<b>Join a Wireless Network</b>	
<b>Network Name</b>	Select the desired network name from the list.
<b>Push the Button on my access point</b>	Push the WPS button of the access point and enable this button.
<b>Enter a PIN into my access point</b>	Enable this and enter the PIN code displayed in the following field to the WPS screen of the access point.
<b>Enter a PIN from my access point</b>	Enable this and enter the PIN code of the access point in the following field.
<b>Start</b>	Click this button to start the WPS process.

## Network Status Screen

This screen displays the status of the current wireless link. Clicking the **Network Status** tab will display a screen like the following.



**Figure 10: Network Status Screen**

You may have to wait a few seconds for the screen to be populated.

### Data - Network Status Screen

Link Information	
<b>Current Status</b>	It will indicate the current link status.
<b>Network SSID</b>	It shows the SSID or network name of the selected wireless network.
<b>Network BSSID</b>	It shows the MAC address of the access point.
<b>Network Type</b>	This will indicate "Infrastructure" or "Ad-hoc".
<b>Authentication Mode</b>	It will indicate the current authentication mode in use.
<b>Encryption Method</b>	It shows the wireless security that the wireless network is using.
<b>Tx/Rx Speed</b>	It shows the current wireless connection speed.
Internet Protocol	
<b>DHCP Option</b>	It shows if the IP address was automatically obtained from a DHCP server.
<b>IP Address</b>	It shows the current IP address on the wireless interface.

<b>Subnet Mask</b>	Subnet mask for the current IP address.
<b>Default Gateway</b>	Gateway IP address associated with the current IP address.
<b>DHCP Server</b>	It shows the IP address of the DHCP Server.
<b>Channel Performance</b>	
<b>Channel Performance</b>	It graphically presents the Transmission (Tx) rate and Receiving (Rx) rate over time.
<b>Signal</b>	
<b>Signal</b>	It graphically presents the Signal strength.

## About Screen

This screen displays details of the traffic sent or received on the current Wireless network.



**Figure 11: About Screen**

This tab shows the following information:

- Regional Domain
- Firmware Version
- Driver Version
- MAC Address
- SerComm DLL Version
- SerComm Utility Version

# Appendix A

## Specifications



### Wireless Adapter

<b>Model:</b>	PC812Rn
<b>Standards:</b>	IEEE 802.11b, IEEE 802.11g, Draft 802.11n compliant
<b>Computer Slot Type:</b>	PCI Card
<b>Data Rates:</b>	20 MHz BW: 145, 130, 117, 104, 78 40 MHz BW: 300, 270, 243, 240, 216, 180, 162, 120, 108 Receive PHY Rate: 300Mbps Transmit PHY Rate: 150Mbps (802.11n)
	54, 48, 36, 24, 18, 12, 9, and 6 Mbps (802.11g)
	11, 5.5, 2, 1 Mbps (802.11b)
<b>Operating Channels:</b>	USA: channel 1-11
<b>Operating Frequency:</b>	USA: 2.412 ~ 2.462 GHz
<b>Modulation Technique:</b>	
	Draft 802.11n: OFDM
	802.11g: DBPSK, DQPSK, CCK, BPSK, QPSK, QAM
	802.11b: CCK, DQPSK, DBPSK
<b>Media Access Protocol:</b>	CSMA/CA
<b>Operating Voltage:</b>	3.3V±5%
<b>Antenna Type</b>	Detachable antenna*2
<b>Security:</b>	64/128/152-bit WEP Shared-key encryption WPA-PSK(Personal)/WPA2-PSK(Personal) WPA-EAP(Enterprise)/WPA2-EAP(Enterprise) 802.1x WEP TKIP/AES encryption
<b>OS Requirements</b>	Windows Vista/XP/2000

# About Wireless LANs

*This Appendix provides some background information about using Wireless LANs (WLANs).*

## Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

### Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

### Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.



Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

## BSS/ESS

### BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

**Using the same SSID is essential.** Devices with different SSIDs are unable to communicate with each other.

### ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

## Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

## WEP & WPA-PSK

Both WEP and WPA-PSK are standards for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

WPA-PSK is a later standard than WEP, and is more secure.

## WPA2-PSK

This is a later version of WPA (WPA-PSK). The major change is the use of AES (Advanced Encryption System) for protecting data. AES is very secure, considered to be unbreakable. The PSK (Pre-shared Key) must be entered on each Wireless station.

**If WPA2-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:**

<b>WPA2 PSK (Pre-shared Key)</b>	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
<b>Encryption</b>	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

## Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

- |                     |   |
|---------------------|---|
| <b>Mode</b>         | On client Wireless Stations, the mode must be set to "Infrastructure".<br>(The Access Point is always in "Infrastructure" mode.)  |
| <b>SSID (ESSID)</b> | Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.  |
| <b>Security</b>     | The Wireless Stations and the Access Point must use the same settings for Wireless security (Disabled, WEP, WPA-PSK, WPA2-PSK, WPA Radius, WPA2 Radius) <ul style="list-style-type: none"><li>• If Wireless security remains disabled on the Access Point, all stations must have wireless security disabled.</li><li>• If Wireless security is enabled on the Access Point, each station must use the same settings.</li></ul> |



# Regulatory Approvals

## FCC 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.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

## FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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.

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

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

## Channel

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

Note: This equipment marketed in USA is restricted by firmware to only operate on 2.4G channel 1-11