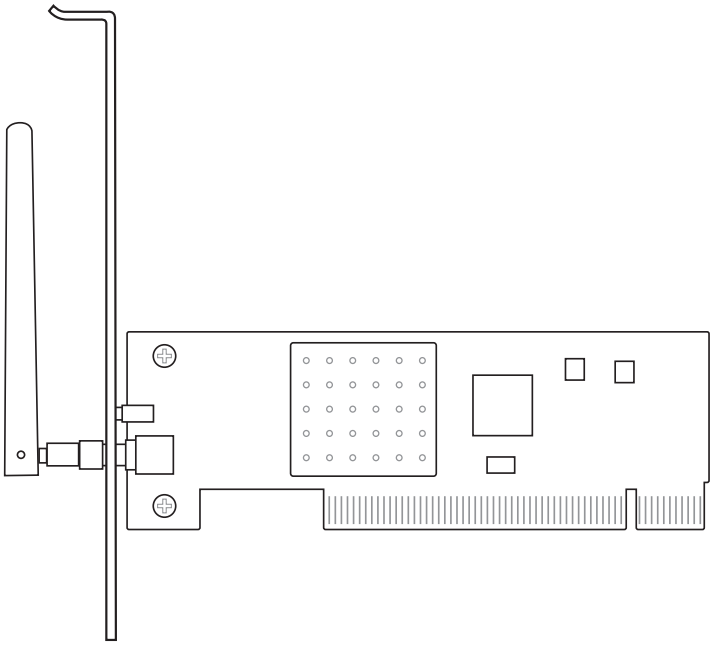
Wireless Local Area Network Card

WL-138g V2 / WL-138gE

(For 802.11g & 802.11b Wireless Networks)



User's Manual

E2270 / Sep 2005

Copyright Information

ASUSTeK COMPUTER INC.

Company address: 15 Li-Te Road, Beitou, Taipei 11259
General (tel): +886-2-2894-3447
Web site address: www.asus.com.tw
General (fax): +886-2-2894-7798
General email: info@asus.com.tw

Technical support

Technical support
General support (tel): +886-2-2894-3447
Online support: http://support.asus.com

ASUS COMPUTER INTERNATIONAL (America)

Company address: 44370 Nobel Drive, Fremont, CA 94538, USA
General (fax): +1-510-608-4555
Web site address: usa.asus.com

Technical support

Technical support
General support (tel): +1-502-995-0883
Online support: http://support.asus.com
Notebook (tel): +1-510-739-3777 x5110
Support (fax): +1-502-933-8713

ASUS COMPUTER GmbH (Germany & Austria)

Company address: Harkort Str. 25, D-40880 Ratingen, Germany
General (tel): +49-2102-95990
Web site address: www.asuscom.de
General (fax): +49-2102-959911
Online contact: www.asuscom.de/sales

Technical support

Technical support
Component support: +49-2102-95990
Online support: http://support.asus.com
Notebook support: +49-2102-959910
Support (fax): +49-2102-959911

Table of Contents

1. Introduction

Overview

Thank you for purchasing the ASUS WLAN Card. The ASUS WLAN Card is designed to be fully compliant with both the IEEE 802.11g and 802.11b wireless local area network (Wireless LAN) standards. As a result of the completion of the standard, the interoperability of Wireless LAN products among multiple manufacturers will be guaranteed. The ASUS WLAN Card product provides high-speed, standards-based Wireless LAN solutions.

The ASUS WLAN Card configuration utility is a user-friendly application that helps you quickly setup multiple roaming nodes using the ASUS WLAN Card. You can even export the configuration settings to a file and import them to other computers for fast multiple installations using ASUS Mobile Manager. Wireless LANs are complementary extensions to existing wired LANs, offering complete mobility while maintaining continuous network connectivity to both corporate and home Intranets. They add a new level of convenience for LAN users. PC users stay connected to the network anywhere throughout a building without being bound by a LAN wires. This is accomplished through the use of ASUS WLAN Access Points or ASUS WLAN Home Gateways. ASUS WLAN Home Gateways with built-in Internet gateway capability, allows your family to share a broadband Modem and one ISP account simultaneously from different rooms without wires! ASUS WLAN products can keep you connected anywhere, any time.

System Requirements

To begin using the ASUS WLAN Card, you must have the following minimum requirements:

- Windows XP/2000/ME/98SE
- Standard 32-bit PCI Slot
- 32MB system memory or larger
- 300MHz processor or higher

The Product Package

When you receive the ASUS WLAN Card package, it should contain the following items:

- ASUS WLAN PCI Card
- Dipole Antenna
- ASUS WLAN Card Quick Start Guide
- CD-ROM Disc (Drivers, Utilities, Documentation)

Note: If any of the above items are not included or damaged, contact your local dealer for instructions.

2. Installation

Installation Procedures

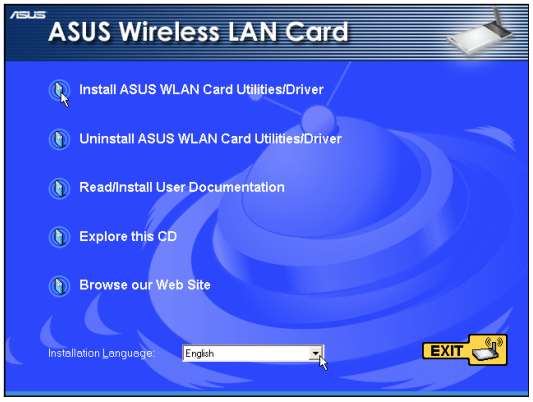
Important: Install the ASUS WLAN card utilities before inserting the ASUS WLAN Card into your computer.

Follow these instructions to setup the ASUS WLAN card.

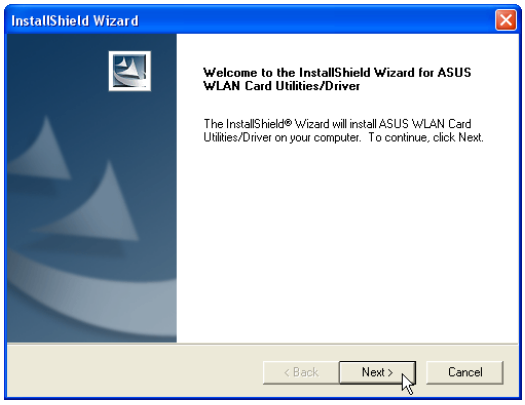
1. Install the ASUS WLAN card utilities and driver from the support CD.
2. Insert the ASUS WLAN card into your computer.

Installing the ASUS WLAN Card Utilities & Driver

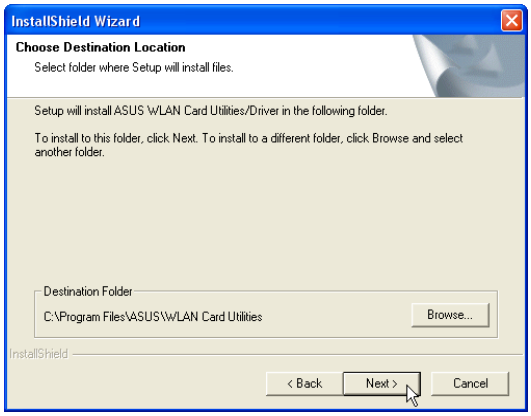
1. Insert the ASUS WLAN Card support CD and an autorun menu will appear. If your autorun is disabled, double click **SETUP.EXE** in the root directory of the support CD.



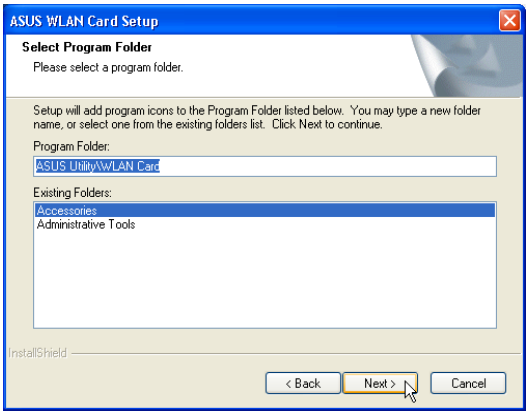
2. From the autorun menu, select your language and click **Install ASUS WLAN Card Utilities / Driver**.



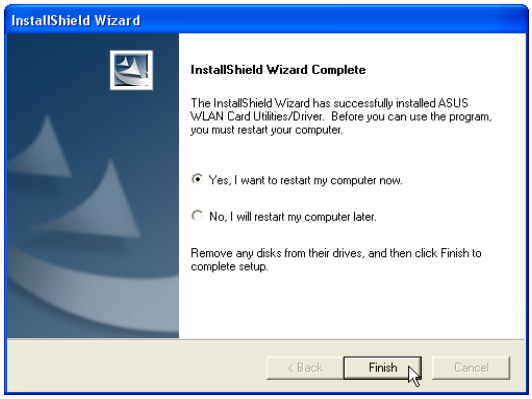
3. Click **Next** on the Welcome screen.



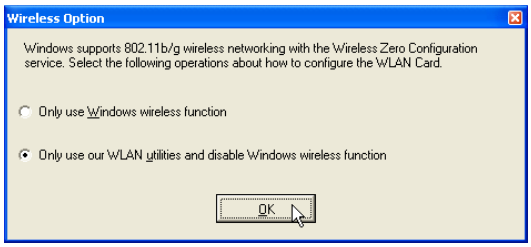
4. Click **Next** to use the default Destination Folder or click Browse for another folder.



5. Click **Next** to place icons in the default program folder or type another name.



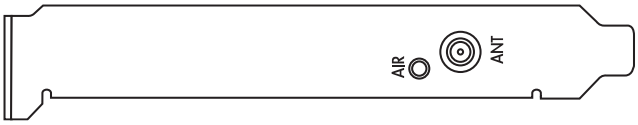
6. When Setup is complete, click **Finish** to exit the installation wizard.



7. When the program is launched for the first time, you will be asked which function to use. Select to use our WLAN utilities for more functionality.

Reading the ASUS WLAN Status Indicators

The ASUS WLAN card consists of one AIR indicator that shows the status of the ASUS WLAN Card.

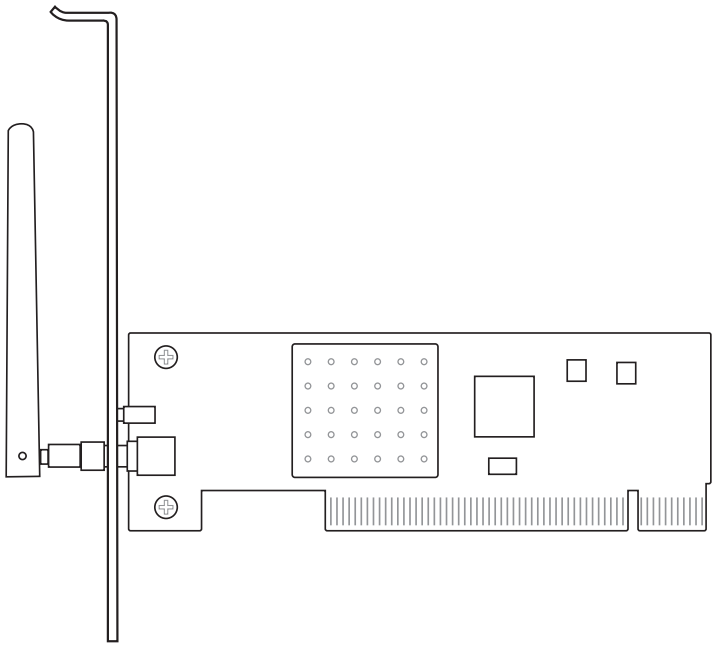


OFF: No wireless activity.

Blinking: Transmitting or receiving wireless data.

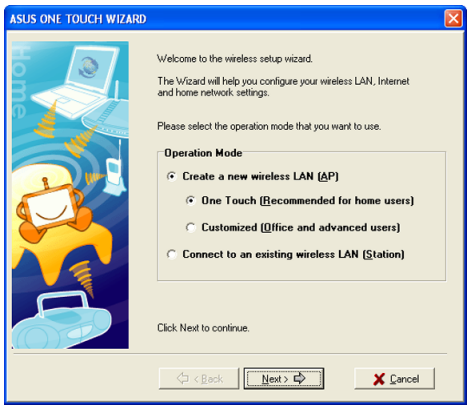
Orientating the Antenna

The ASUS WLAN Card has one external antenna. It is recommended that you adjust the external antenna straight up for maximum range and higher link quality.

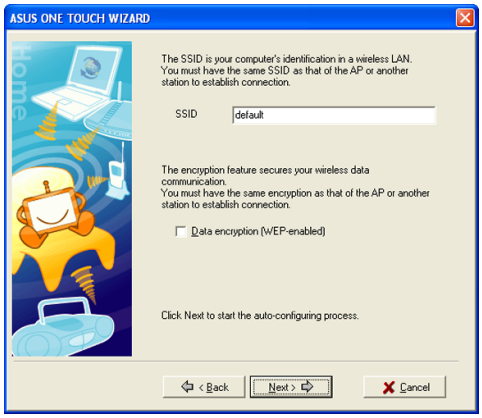


One Touch Wizard (new wireless LAN)

Use the One Touch Wizard to setup your wireless connection.

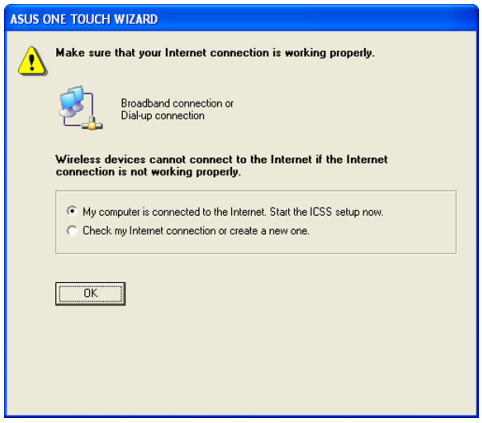


1. Select **Create a new**... and click **Next** to use the simplest configuration or select another option first.

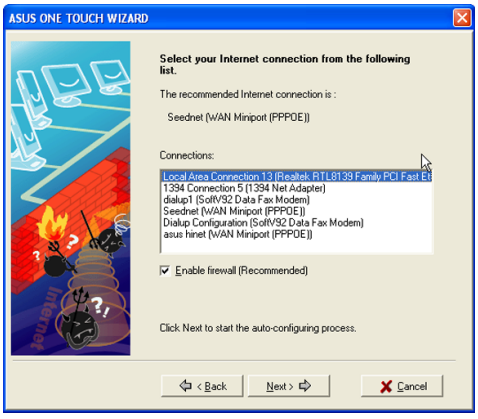


2. Enter the SSID name of the access point that you wish to connect to. Select **Data encryption** if secured connections are enabled.

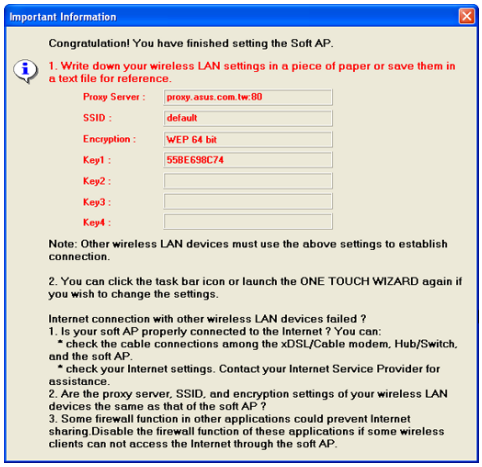
3. Setup is complete. Click **Finish** to exit the wizard or click **Next** to continue with more advanced features.



4. Click **OK** to start ICSS setup.



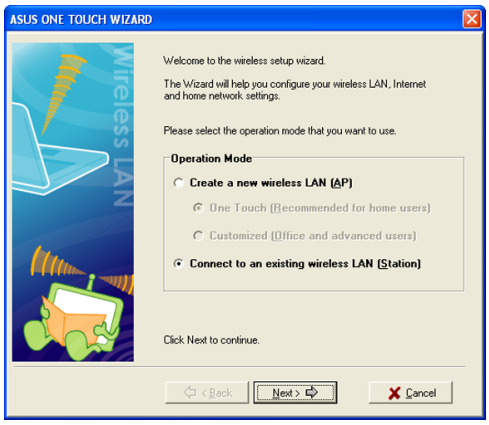
5. Select your Internet connection from the list.



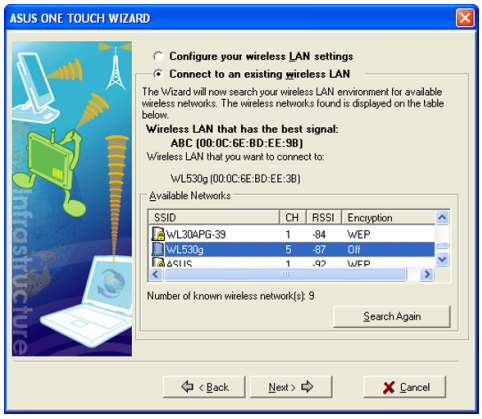
6. Setup is complete. You can review your settings here.

One Touch Wizard (existing LAN)

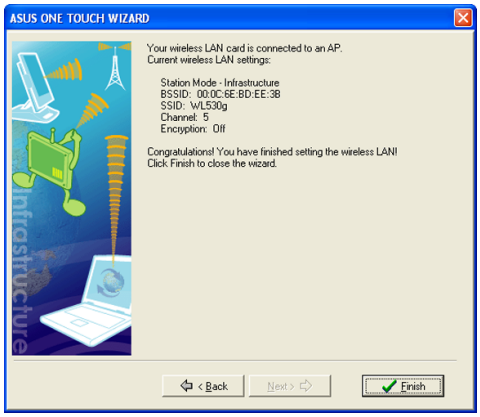
Use the One Touch Wizard to setup your wireless connection.



1. Select **Connect to**... and click **Next** to use the simplest configuration or select another option first.



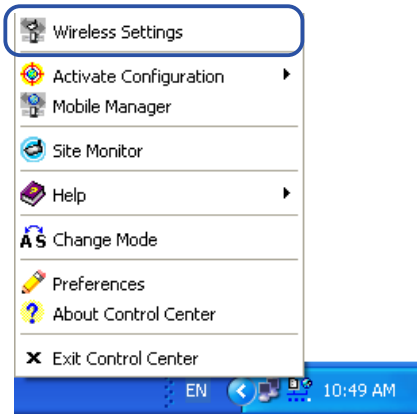
2. Select an AP from the available networks.



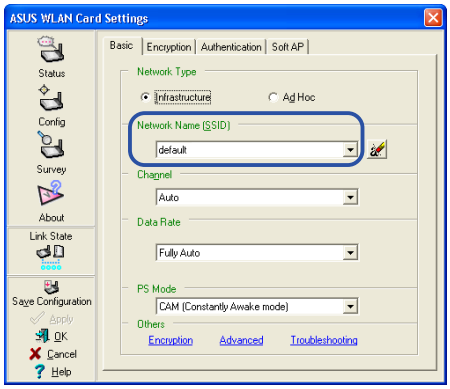
3. Setup is complete. Click **Finish** to exit the wizard.

Configuring the WLAN utility

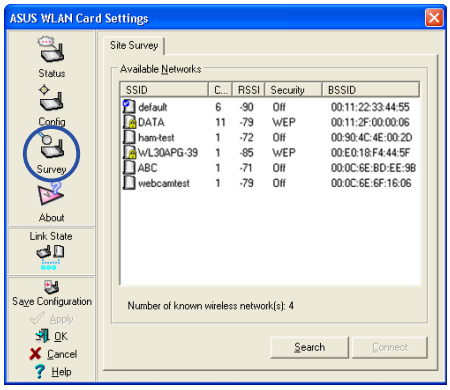
After installing the WLAN Card Utilities, you will need to make some settings before being able to use your wireless connection. Double-click the WLAN Control Center icon to start the utility.



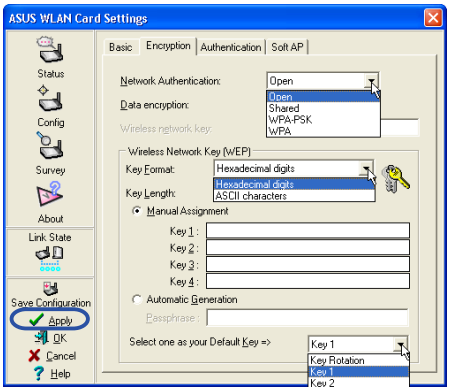
1. Right-click the WLAN icon and select "Wireless Settings"



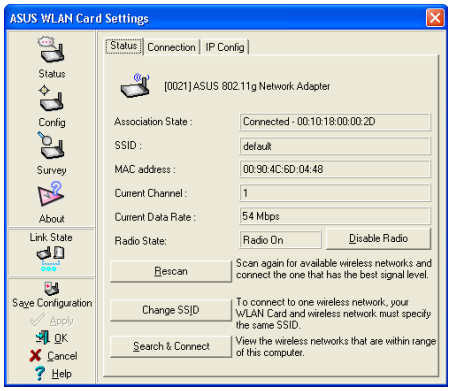
2. Set the Network Name (SSID) to the same name as the SSID set in your wireless access point.



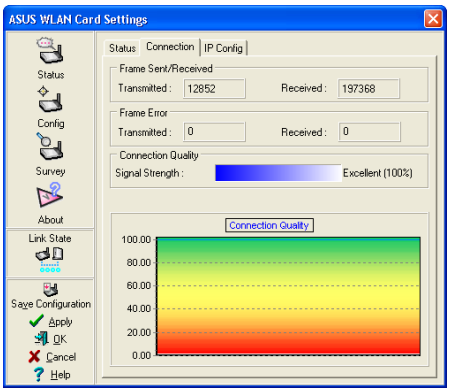
3. Use "Site Survey" if you don't know the name of your access point(s).



4. Encryption settings must also match those set in the access point. Ask your network administrator about settings if necessary. Click **Apply** to save your settings



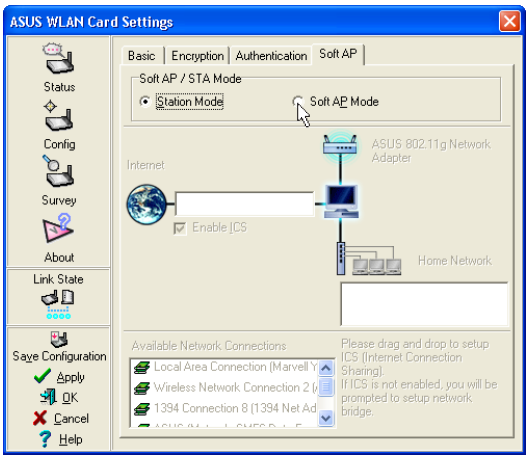
5. Check the "Status" page to see the "Association State". It should show "Connected - xx:xx:xx:xx:xx:xx".



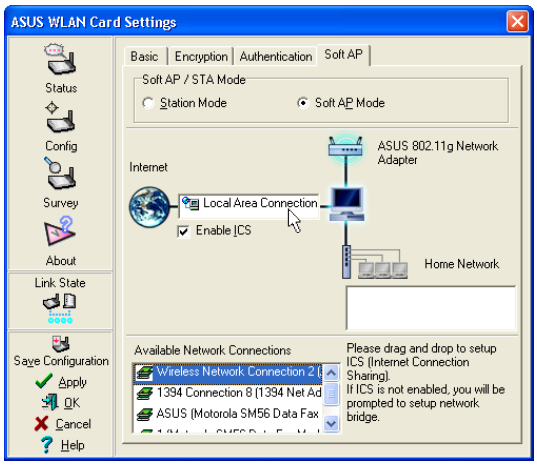
6. You can also see the connection quality on the "Connection" page. Click **OK** to exit the utility.

Soft AP (Windows XP Only)

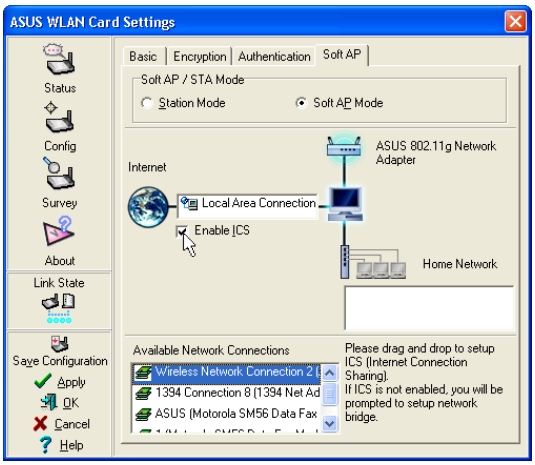
Soft AP mode allows the WLAN card to act as a virtual access point. The computer needs to be connected to a wired network using an Ethernet connection in order to provide network access to WLAN clients.



1. Select Soft AP Mode



2. Drag and drop a wired network connection next to the globe icon.



3. Enable ICS* and Firewall if desired. Refer to Windows help for information on “Internet Connection Sharing”.

4. You can easily switch between Soft AP and Station mode by right clicking the taskbar icon and selecting “A-S Change Mode”.

*ICS is used to share this computer’s Internet connection with the rest of the computers on your network. When this computer is connected to the Internet, communication to and from the Internet to all the computers on your network are sent through this computer, called the host computer. Other computers can send and receive email and access the Web as if it were connected directly to the Internet.

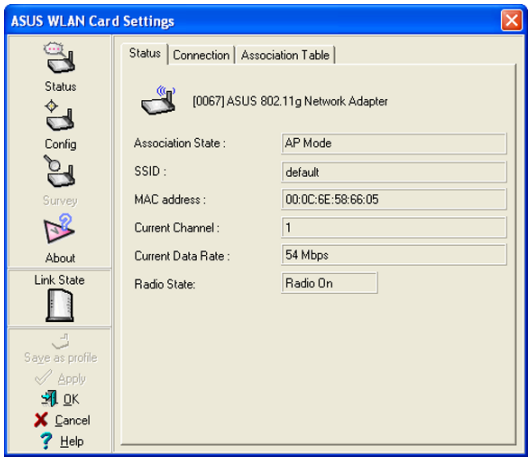
Soft AP (Windows XP Only) Cont.

Soft AP mode allows for Access Control configuration.

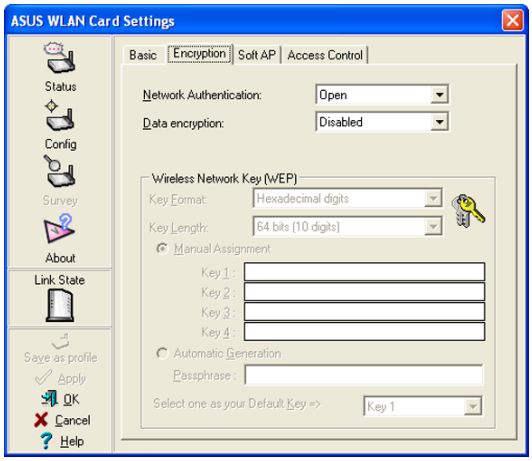
Access Control

The AP provides facilities to limit the wireless clients that associate with it and the data packets that can forward through it. Filters provide network security or improve performance by eliminating broadcast/multicast packets from the radio network.

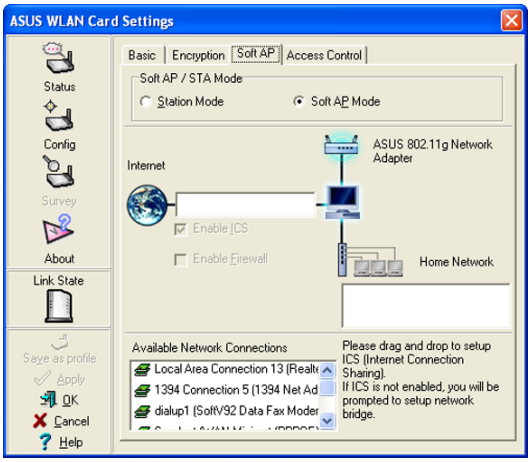
The Access Control List (ACL) contains MAC addresses for wireless clients allowed to associate with the AP. This provides security by preventing unauthorized access. The AP also uses a disallowed address list of destinations. This feature prevents the AP from communicating with specified destinations. This can include network devices that do not require communication with the AP or its wireless clients.



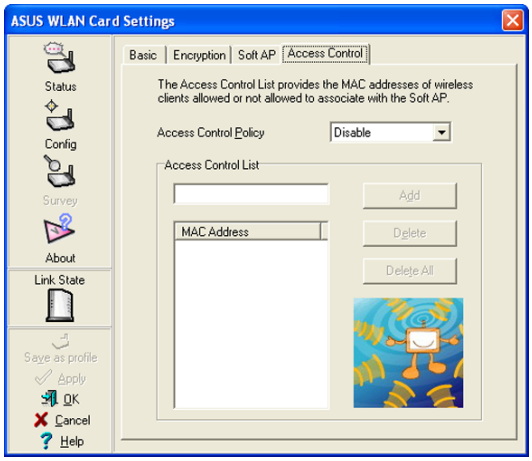
Status Page



Encryption Page

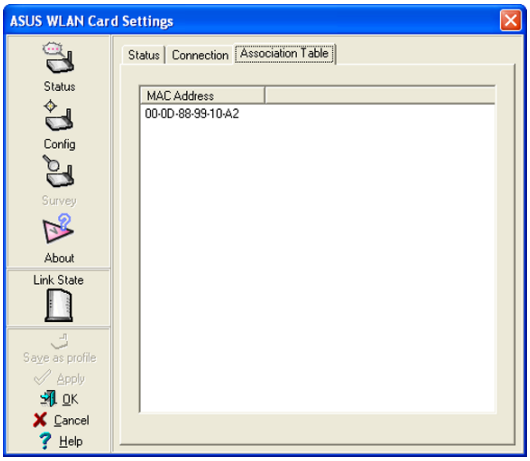


Clicking **Apply** after configuring Soft AP will show the “Access Control” tab.

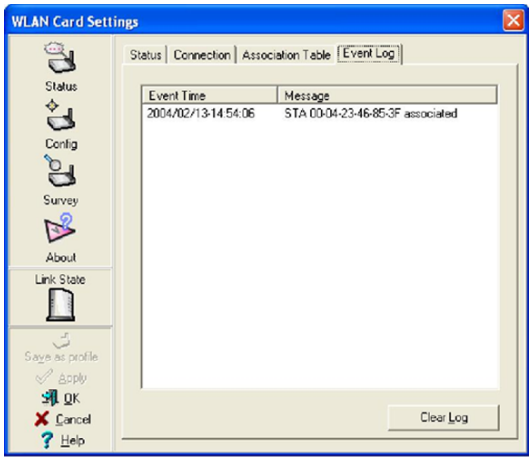


Enter a MAC Address on the Access Control page and select “Accept” or “Reject” or “Disable” from the pull-down menu.

Soft AP (Windows XP Only) Cont.



Soft AP Mode will also provide two extra tabs on the Status pages - Association Table and Event Log. The Association Table shows clients that are currently connected to the Soft AP.



The Event Log tracks messages associated with the Soft AP.

IMPORTANT: If the end points of a chain are connected to each other a loop is created. Normally it is advised to avoid loops involving bridges as it can lead to performance breakdowns, and broadcast and multicast storms.

3. Software Reference

Chapter Overview

The WLAN Card software includes several utilities:

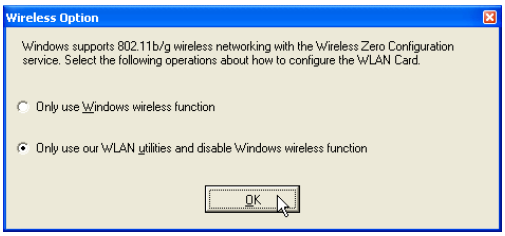
- **WLAN Control Center** – Makes it easy to launch applications and activate network location settings.
- **Wireless Settings** – Allows users to control the WLAN Card.

Additional Reference

- **Windows XP Wireless Properties** - Brief overview of the wireless settings provided in Windows XP.

Windows XP Wireless Options

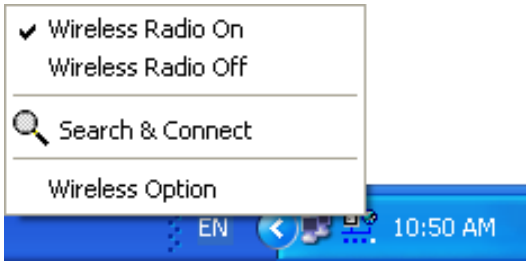
The wireless options shown below is only available for Windows XP. The first time you run the Control Center utility, it will automatically show. Select one of the radio buttons to decide which interface to use with your WLAN Card.



Only use XP wireless function – Only use "Windows XP" wireless network settings to configure the WLAN Card.

Only use utilities and disable XP wireless function – Only use "WLAN Card utilities" to configure the WLAN Card. (recommended)

You can return to the Wireless Option setting at any time by left clicking the control center icon and choosing "Wireless Option".



Taskbar Left-Click Menu

WLAN Control Center

Control Center is an application that makes it easy to launch applications and activate network location settings. Control Center starts automatically when the system boots. Whenever Control Center is running, you will see a Control Center icon displayed on the Windows taskbar.

Starting the Control Center manually

- Select **WLAN Control Center** in Windows Start menu.

or

- Double click the **WLAN Control Center** icon on the desktop.

Using the Control Center Taskbar

The Control Center Taskbar menu display the following information:

- The link quality of the WLAN Card (Excellent, Good, Fair, Poor, Not Linked)
- Whether the WLAN Card is connected to the Internet (Blue: Connected, Gray: Not Connected)

Taskbar Icon and Status (station mode)

Taskbar Icon and Status (access point mode)

Wireless Status Icons (on the taskbar)


Excellent link quality and **connected to Internet** (Infrastructure)


Good link quality and **connected to Internet** (Infrastructure)


Fair link quality and **connected to Internet** (Infrastructure)


Poor link quality and **connected to Internet** (Infrastructure)


Not linked but **connected to Internet** (Infrastructure)


Excellent link quality but **not connected to Internet** (Infrastructure)


Good link quality but **not connected to Internet** (Infrastructure)


Fair link quality but **not connected to Internet** (Infrastructure)


Poor link quality but **not connected to Internet** (Infrastructure)


Not linked and **not connected to Internet** (Infrastructure)

Taskbar Icon - Right Menu

Right-clicking the taskbar icon shows the following menu items:

- **Wireless Settings** – Launches Wireless Settings application.
- **Activate Configuration** – Allows you to set which profile to use.
- **Mobile Manager** – Launches Mobile Manager application.
- **Site Monitor –** Launches the Site Monitor application.
- **Change Mode** (Windows XP Only) - Configures your card in Station (STA) or Soft Access Point (Soft AP) mode. In STA mode, your card connects to an access point to access a wireless network or the Internet. In Soft AP mode, your card transmits and receives signals to and from other WiFi devices in a wireless network.
- **Preferences** – Customizes the way the Control Center program behaves. You can create a Control Center shortcut on the desktop. You can also set whether Control Center starts up with Windows.
- **Exit** – Closes the Control Center program.

Taskbar Icon - Left Menu

Left-clicking the taskbar icon shows the following menu:

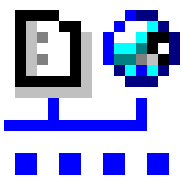
Taskbar Left-Click Menu

- **Wireless Radio On** – Turns the wireless radio ON.
- **Wireless Radio Off** – Turns the wireless radio OFF.
- **Search & Connect** – View the properties of available Access Points within range.
- **Wireless Option** (Windows XP only) – Sets your Windows XP wireless networking environment.

Taskbar Icon - Launch Wireless Settings

Double-clicking the taskbar icon:

- Launches the Wireless Settings application.



Wireless Settings Utility

Wireless Settings is an application that allows you to control your WLAN Card. Use Wireless Settings to View or Modify the configuration settings and monitor the operational status of your PC Card. Once Wireless Settings is launched, you can see the tabbed property sheet. This property sheet is composed of tabbed "pages", each with its own group of feature-specific settings.

Starting Wireless Settings

- Open the Windows **Control Panel**, and then double-click the **WLAN Card Settings** icon.

or

- Click the Windows **Start** button, select **Programs | ASUS Utility | WLAN Card | Wireless Settings**.

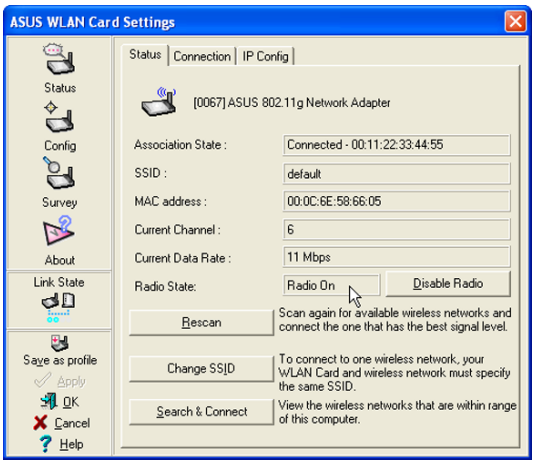
or

- Right-click the **Control Center icon** on the Windows taskbar, select **Wireless Settings**.

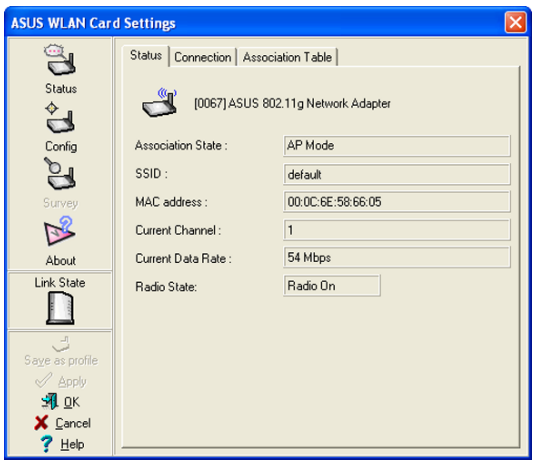
NOTE: If you have more than one WLAN device, you will be given a device selection window when you launch the "Wireless Settings" utility. Select the appropriate model if you face this situation.

Status - Status Tab

You can view the information about the WLAN Card from the general menu. These fields are blank if the WLAN Card does not exist. You can turn OFF the WLAN Card by clicking the "Disable Radio" button.



Station Mode



Access Point Mode

Association State

Displays the connection status as follows:

Connected - The station is now associated with one wireless LAN device. When operating in Infrastructure mode, this field shows the MAC address of the Access Point with which you are communicating. When operating in Ad Hoc* mode, this field shows the virtual MAC address used by computers participating in the Ad Hoc* network.

Scanning... - The station is now attempting to authenticate and associate with the desired Access Point or Ad Hoc* node.

Disconnected - The link is connected, but no beacon received.

SSID

Displays the Service Set Identifier (SSID) that the card is either associated or intending to join.

MAC address

Indicates the hardware address of the card. MAC address is a unique identifier for networking devices (typically written as twelve hexadecimal digits 0 through 9 and A through F, six hexadecimal numbers separated by colons, i.e. 00:E0:18:F0:05:C0).

Current Channel

Displays the radio channel that the card is currently tuned. This number changes as the radio scans the available channels.

Current Data Rate

Displays the current transmit data rate in megabits per second (Mbps).

* **See Chapter 5 - Glossary**

Radio State

Shows the wireless radio ON or OFF.

Radio On - When the wireless radio is turned ON, the following icon appears in the upper left of the Settings property page.

Radio Off- When the wireless radio is turned OFF, the following icon appears in the upper left of the Settings property page.

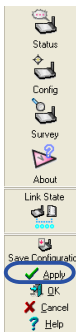
Rescan – Force the radio to rescan all available channels. If your link quality or signal strength is poor, rescanning can be used to push the radio off a weak Access Point and search for a better link with another Access Point. This function will take some time to complete.

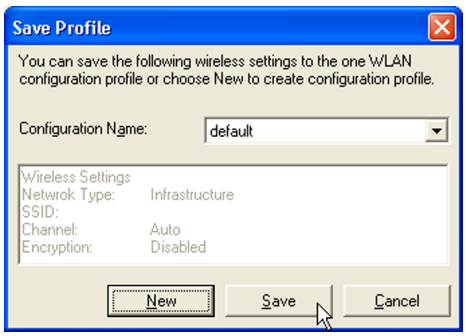
Change SSID – Click on this to set the SSID.

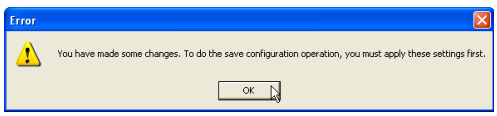
Search & Connect – Click on this to connect to an available network.

Save as Profile

Later, when you make individual settings, you may want to use profiles to save your settings. Profiles will help you combine all your settings for work, home, roaming, and other locations so that you do not have to repeat individual settings. When you travel from work to home, for example, choose a "home" profile that contains all your settings for home use. When you travel back to work, choose an "office" profile.







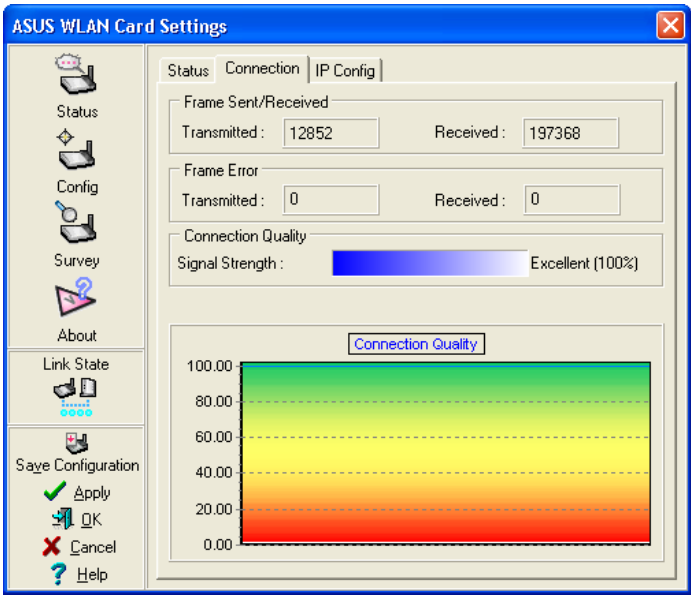
Click apply first if you have not.

Activate Configuration

Auto roaming is enabled by default and will automatically switch to stronger access points. You can uncheck it if you have many access points and do not want to constantly switch to different networks. If you want to use a particular profile. You can also check it here.

Status - Connection

You can view the current link statistics about the WLAN Card. These statistics are updated once per second and are valid only if the WLAN Card exists.



Frame Sent/Received

Transmitted - The number of frames that were transmitted.

Received - The number of frames that were received.

Frame Error

Transmitted - The number of frames that were not successfully transmitted.

Received - The number of frames that were not successfully received.

Connection Quality

Signal Strength - Reflects the signal level related to the Access Point or Ad Hoc node the station is currently connected to. Ratings are: Excellent, Good, Fair, and Poor.

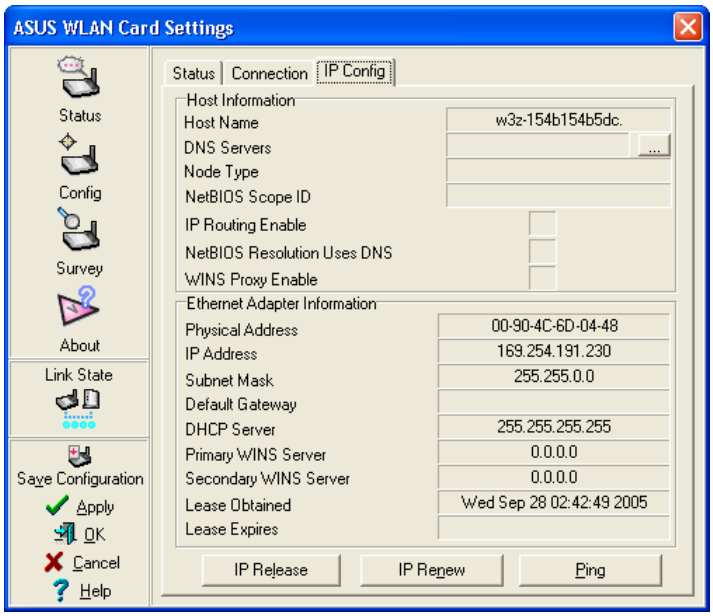
Overall Connection Quality

It is derived from the current "Signal Strength". A graph displays a connection quality range between 0 and 100 percent.

Status - IP Config

IP Config tab shows all the current network configuration information for the WLAN Card. Use it to verify your network settings.

IP CONFIG will display all the current TCP/IP configuration values including the IP address, subnet mask, default gateway and Windows Internet Naming Service (WINS) and DNS configuration.



Button

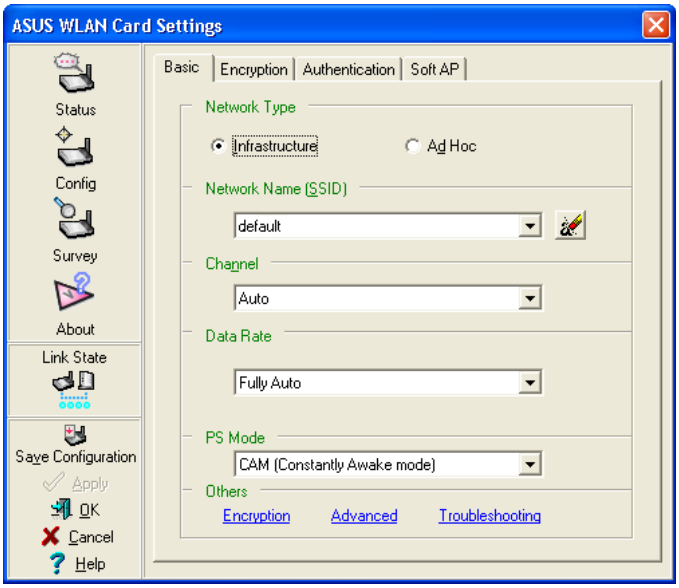
IP Release - Clicking this button will attempt to release the DHCP IP address for the WLAN Card in case you wish to remove your IP address.

IP Renew - Clicking this button will attempt to renew the DHCP IP address for the WLAN Card in case you want to obtain a new IP address.

NOTE: The IP Release and IP Renew buttons can only be used on the WLAN Card that is configured with DHCP.

Config - Basic

Lets you can change the WLAN Card configurations without rebooting your computer.



Network Type

Infrastructure – Select the Infrastructure mode to establish a connection with an Access Point. Your computer is able to access wireless LAN and wired LAN (Ethernet), via an associated access point. The Channel field turns to "Auto" when "Infrastructure" is selected.

Ad Hoc – Select the "Ad Hoc" mode to communicate directly with each other without using an Access Point. An "Ad Hoc" network is typically formed quickly and easily without pre-planning. For example, share meeting notes between networked computers in a meeting room.

Network Name (SSID)

Use the SSID field to configure the SSID for the WLAN Card. You can enter a new SSID or select one from the drop-down list box. SSID stands for "Service Set Identifier", which is a string used to identify a wireless LAN. You will only be able to connect Access Points which has the same SSID as the one you set. Use different SSIDs to segment the wireless LAN and increase security. SSIDs must all be printable characters and having a maximum of 32 case sensitive characters, such as " Wireless LAN".

NOTE: Set the SSID to a null string, if you wish to allow your station to connect to any Access Point it can find. But you cannot use null string in Ad Hoc mode.

Channel

Use the Channel field to select the radio channel for WLAN Card. In an "infrastructure" network, your WLAN Card will automatically select the correct frequency channel required to communicate with an Access Point, this parameter will be fixed in "Auto" and cannot be changed. In an "Ad Hoc" network, you can decide the channel number for the WLAN Card. Any WLAN Card can communicate in the same network if they have the same frequency channel setting.

The radio channels you may use depend on the regulations in your country. For United States (FCC) and Canada (IC), channels 1 to 11 are supported. For Europe (ETSI), channels 1 to 13 are supported. For operation in Japan (MKK), channels 1 to 14 are supported.

Data Rate

Select the transmit data rate (fix or auto). The data rates supported for the WLAN Cards are:

Auto – The adapter will adjust to the most suitable transmission rate.

Fix – 11g: Fix data rate to 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.

11b: Fix data rate to 1, 2, 5.5, or 11 megabits per second.

Others

Encryption – Click on this to show the "Encryption" tab.

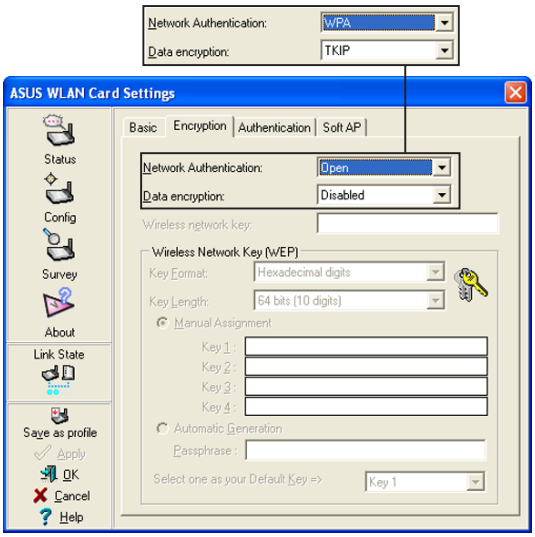
Advanced – Click on this to show the "Advanced" tab. In most cases, the default values do not have to be changed.

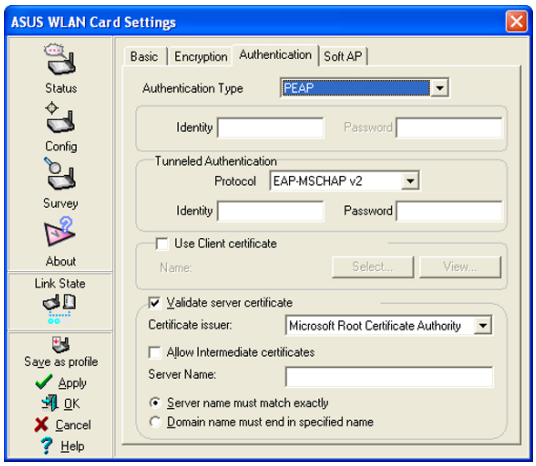
Troubleshooting – Click on this to show the Troubleshooting utility.

Click Apply to save and activate the new configurations.

Config - Encryption

Lets you configure the Wireless LAN Card encryption settings. For data confidentiality in a wireless environment, IEEE 802.11 specifies a Wired Equivalent Privacy (WEP) algorithm to offer transmission privacy similar to wired network. The WEP uses keys to encrypt transmit data packets and decrypt received data packets. The encryption process can scramble frame bits to avoid disclosure to others. The WPA (Wi-Fi Protected Access) is an improved security system for 802.11 that encryption data sent over radio waves. The WPA was developed to overcome the weakness of the WEP protocol.





Network Authentication

Because there is no precise bound in wireless LANs, it needs to be implemented in another mechanism to provide higher level of security. That is where Authentication services come in. If a mutual authentication relationship has not been established between stations and Access Point, an association cannot be established.

Open - Select this option allows the network to operate on an Open System mode. A null authentication algorithm. A station can authenticate with any other station or Access Point and without checking any WEP Key, even if one exists.

Shared - Select this option allows the network to operate on an Shared Key mode. In a Share Key Authentication system, four-step exchange of frames is required to validate that the station is using the same WEP Key as the Access Point.

WPA-PSK - Specifies the use of a preshared key with infrastructure mode. Enables WPA Preshared key, which enables your client adapter to associate to Access Point using WPA-PSK.

WPA-None - Specifies the use of a preshared key with Ad Hoc mode.

WPA - The network is operating in IEEE 802.1x authentication mode. This mode is environments with a RADIUS (Remote Access Dial-in User Service) infrastructure. In a RADIUS environment, various Extensible Authentication Protocol (EAP) are supported, including PEAP, TLS/Smart Card, TTLS, and LEAP.

Data encryption

For open and shared authentication mode, the selection of encryption type are Disable and WEP. For WPA-PSK and WPA authentication mode, it must support TKIP (Temporal Key Integrity Protocol) encryption, and may support AES (Advanced Encryption Standard) encryption.

Disabled - Disable the encryption function.

WEP - A WEP Key is used to encrypt your data before it is transmitted over the air. You will only be able to communicate with wireless devices that have use the same WEP keys.

TKIP: TKIP uses an encryption algorithm methods which is more stringent than the WEP algorithm and also uses existing WLAN calculation facilities to perform encryption operations. TKIP verifies the security configuration after the encryption keys are determined.

AES: AES is a symmetric 128-bit block encryption technique which works simultaneously on multiple network layers.

Wireless Network Key

Selecting “TKIP” or “AES” in the encryption filed is used as a password to begin the encryption proceed. Note: 8 to 63 characters are required.

Wireless Network Key (WEP)

This option is enable only if you enable WEP Encryption. The WEP Key is a 64 bits (5 byte) or 128 bits (13 byte) Hexadecimal digits that is used to encrypt transmit data packets and decrypt received data packets.

Key Format

You can enter the WEP Key as a Hexadecimal digits (0~9, a~f, and A~F), or as ASCII characters, based on the state of the Key Format.

Key Length

For 64 bits encryption, each Key contains exactly 10 hex digits, or 5 ASCII characters. For 128 bits encryption, each Key contains exactly 26 hex digits, or 13 ASCII characters.

Two ways to assign WEP keys

1. **Manual Assignment** - When you click this button, the cursor appears in the field for Key 1. For 64-bit encryption, you are required to enter four WEP Keys. Each Key contains exactly 10 hex digits (0~9, a~f, and A~F). For 128-bit encryption, you are required to enter four WEP Keys. Each Key contains exactly 26 hex digits (0~9, a~f, and A~F).
2. **Automatic Generation** - Type a combination of up to 64 letters, numbers, or symbols in the Passphrase column, then the Wireless Settings Utility uses an algorithm to generate four WEP Keys for encryption.

NOTE: This function ease users from having to remember their passwords and is compatible to some existing WLAN utilities, but it is not very secure. "Manual Assignment" is more secure.

Select one as your Default Key

The Default Key field lets you specify which of the four encryption keys you use to transmit data on your wireless LAN. You can change the default key by clicking on the down arrow at the right of this field, selecting the number of the key you want to use and then clicking the Apply button. As long as the Access Point or station with which you are communicating has the same key in the same position, you can use any of the keys as the default.

You then click the Apply button to create your encryption keys. After you click the Apply button, the Wireless Settings Utility uses asterisks to mask your keys.

64/128bits versus 40/104bits

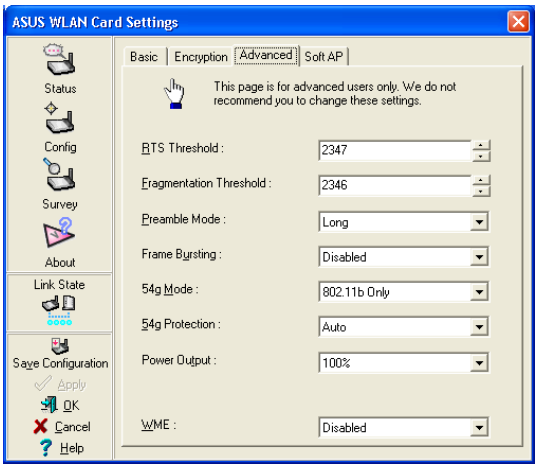
You may be confused about configuring WEP encryption, especially when using multiple wireless LAN products from different vendors. There are two levels of WEP Encryption: 64 bits and 128 bits.

Firstly, 64 bit WEP and 40 bit WEP are the same encryption method and can interoperate in the wireless network. This lower level of WEP encryption uses a 40 bit (10 Hex character) as a "secret key" (set by user), and a 24 bit "Initialization Vector" (not under user control). This together makes 64 bits (40 + 24). Some vendors refer to this level of WEP as 40 bits and others refer to this as 64 bits. Our Wireless LAN products use the term 64 bits when referring to this *lower* level of encryption.

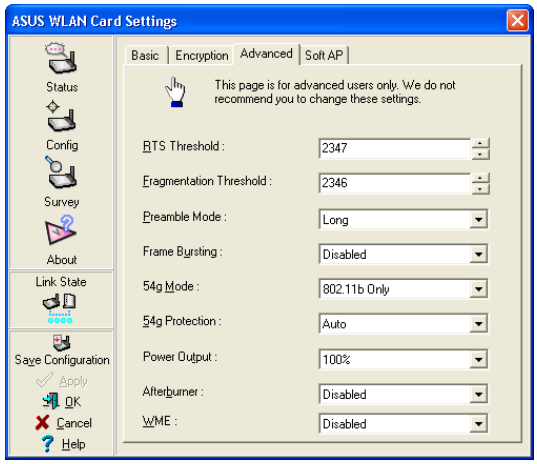
Secondly, 104 bit WEP and 128 bit WEP are the same encryption method and can interoperate in the wireless network. This higher level of WEP encryption uses a 104 bit (26 Hex character) as a "secret key" (set by user), and a 24 bit "Initialization Vector" (not under user control). This together makes 128 bits (104 + 24). Some vendors refer to this level of WEP as 104 bits and others refer to this as 128 bits. Our Wireless LAN products use the term 128 bits when referring to this *higher* level of encryption.

Status - Advanced

This section allows you to set up additional parameters for the wireless router function. We recommend that you use the default values for all items in this window.



WL-138g V2



WL-138gE (includes Afterburner)

RTS Threshold (0-2347)

The RTS/CTS (Request to Send/Clear to Send) function is used to minimize collisions among wireless stations. When RTS/CTS is enabled, the router refrains from sending a data frame until another RTS/CTS handshake is completed. Enable RTS/CTS by setting a specific packet size threshold. The default value (2347) is recommended.

Fragmentation Threshold (256-2346)

Fragmentation is used to divide 802.11 frames into smaller pieces (fragments) that are sent separately to the destination. Enable fragmentation by setting a specific packet size threshold. If there is an excessive number of collisions on the WLAN, experiment with different fragmentation values to increase the reliability of frame transmissions. The default value (2346) is recommended for normal use.

Preamble Mode

This parameter is used to control whether frames will transmit with the Long or Short Preamble. The default value is Long Tx Preamble.

Frame Bursting

Frame Bursting technology is standards-based Wi-Fi performance enhancement technology that improves wireless network efficiency and boosts throughput.

54g Mode

54g LRS (Limited Rate Support) - is used to communicate with older 11b clients that only support 4 rates. But 54g cards can still use all 12 rates.

54g Auto - support both 802.11b and 802.11g adapters.

54g Performance - will support ONLY high-performance 54g adapters.

All of these modes only pertain to when the STA is creating their own IBSS network.

802.11b only - support both 802.11b adapters.

All of these modes only pertain to when the STA is creating their own IBSS network. The default ad-hoc mode is 802.11b only.

54g Protection

Extended Rate PHY (ERP) protection mechanism of 802.11g definition.

Auto – Automatically change as AP announcement.

Enabled - Always send frame with protection.

Disabled - Always send frame without protection.

Power Output

Indicates transmit power level.

Afterburner (WL-138gE)

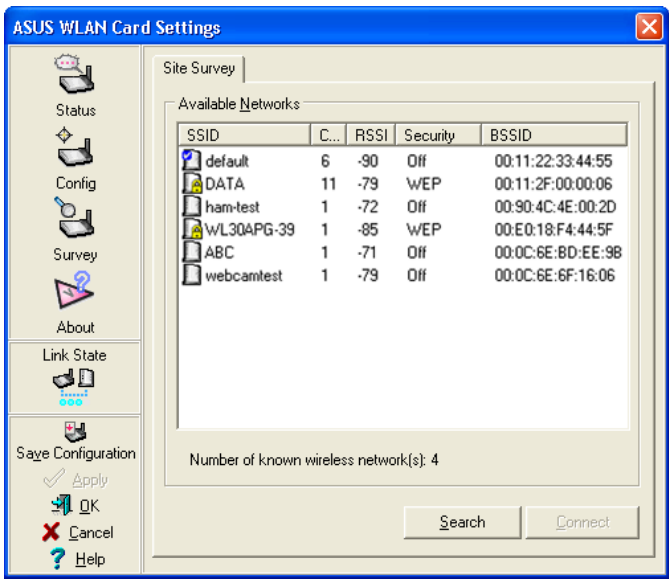
It's is a proprietary solution to take advantage of the high data rate (125 Mbps), the consumer will have to possess a wireless card and router compliant with the Afterburner technology.

Click Apply to save and activate the new configurations.

Survey - Site Survey

Use the Site Survey tab to view statistics on the wireless networks available to the WLAN Card. The Site Survey tab is read-only with no user configurable data fields. Use the Site Survey tab to view the following network parameters.

- **SSID:** View the SSID (service set identification) of the available networks.
- **CH:** View the direct-sequence channel used by each network.
- **RSSI:** View the Received Signal Strength Indication (RSSI) transmitted by each network. This information is helpful in determining which network to associate to. The value is then normalized to a dBm value.
- **Encryption:** View wireless network encryption information. All devices in the network should use the same encryption method to ensure the communication.
- **BSSID:** View the media access control (MAC) address of the Access Point or the Basic Service Set ID of the Ad Hoc node.



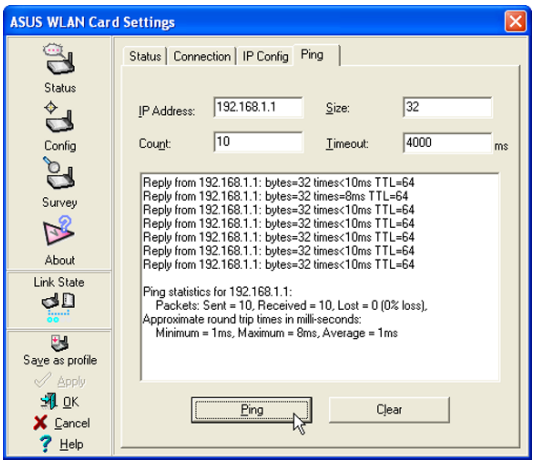
NOTE: Some Access Points can disable broadcasting SSID to hide themselves from "Site Survey" or "Site Monitor" for added security but still allow you to join if you know their SSID.

Buttons

Search – Scan all available wireless networks and show the scan result in the "Available Network List".

Connect – To associate a network, select it from the "Available Network List" and click this button.

Ping



The Ping tab allows you to verify the connection of your computer with another computer in a network. To ping a connection:

1. Type the IP address of the connection you want to verify in the **IP Address** field.
2. Configure the ping session by assigning the size and count of packet to send, and the time limit for a ping session to continue (in milliseconds).
3. Click the **Ping** button.

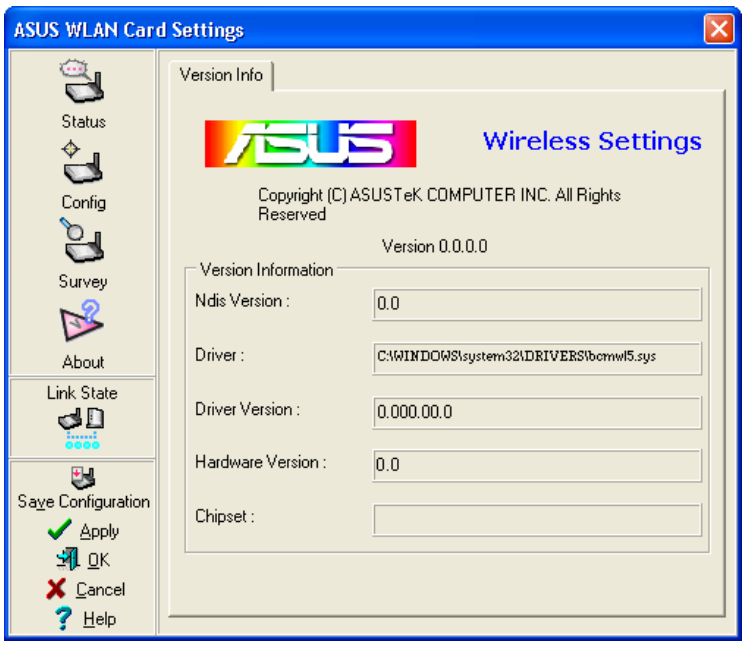
During the ping session, the **Ping** button toggles into a **Stop** button. Click **Stop** anytime to cancel the ping session.

The session field displays information on the verified connection including the roundtrip time (minimum, maximum, and average) and packets sent, received, and lost after a ping session.

Click the **Clear** button to clear the session field.

About - Version Info Tab

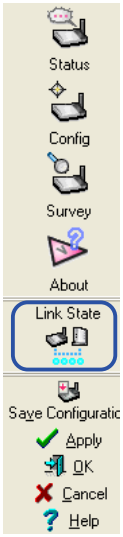
Uses the Version Info tab to view program and WLAN Card version information. The program version information field includes the Copyright and utility version. The version information includes the NDIS version, driver name, and driver version.



This screen is an example only. Your version numbers will be different from what are shown here.

Link State

WLAN Card "Link State" icon appears on the left side of the WLAN Card Settings. Use the icon to view the current signal status.



Excellent Link Quality (Infrastructure)

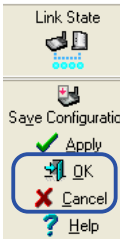
Good Link Quality (Infrastructure)

Fair Link Quality (Infrastructure)

Poor Link Quality (Infrastructure)

Not linked (Infrastructure)

Exit Wireless Settings

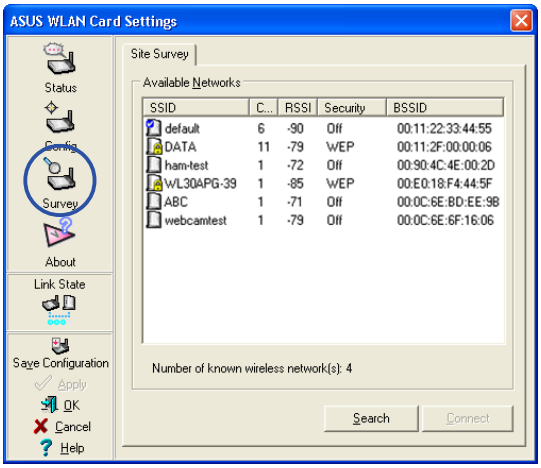


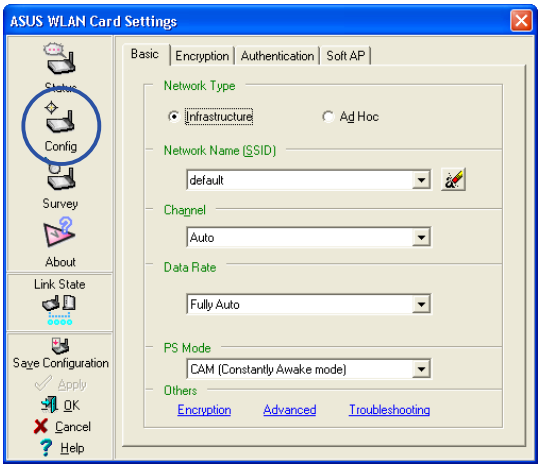
To exit Wireless Settings, you can click **OK** or **Cancel**. This utility may be closed at any time and from any tab. If you did not save the configuration settings, you will be prompted to do so.

Ad Hoc

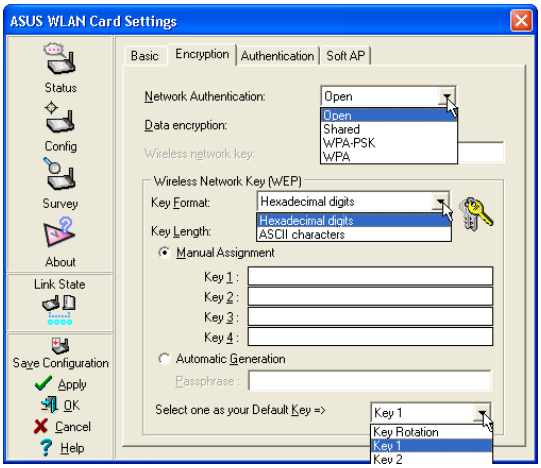
The Wireless LAN card when set to Ad Hoc mode can connect to other wireless device(s) in a wireless network called an Ad Hoc network. To connect the Wireless LAN card to another wireless device:

1. Launch the Wireless Settings utility by double-clicking the Control Center icon in the Windows® taskbar.
2. Click the **Survey** button to scan available wireless device(s) within the Wireless LAN card's range. Select the wireless device you wish to connect. A wireless device is indicated by this icon ( ).





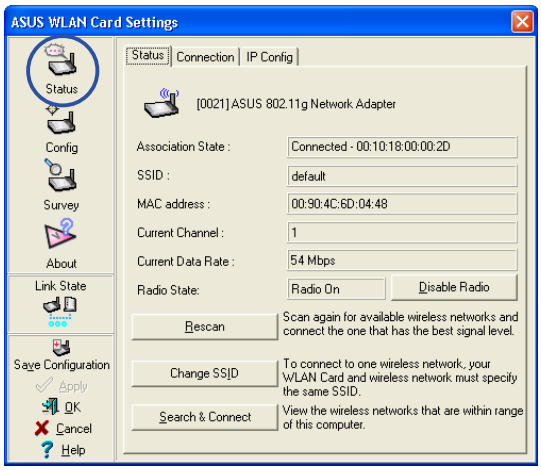
3. Click the **Config** button to configure the device settings. Set the Network type to **Ad Hoc**, then enter the **Network Name (SSID)** and **Channel** of wireless device you wish to connect. Click **Apply** when done.



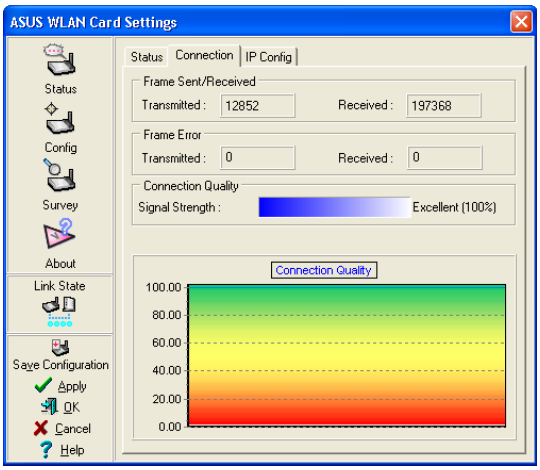
4. Click the **Encryption** tab if your selected wireless device has an enabled WEP encryption ( ).

   Obtain the WEP encryption keys from the network administrator, then enter them in the **Key 1 ~ 4** fields. Click **Apply** when finish.

IMPORTANT! The encryption settings of the Wireless LAN card and the wireless device must be identical to establish a connection.

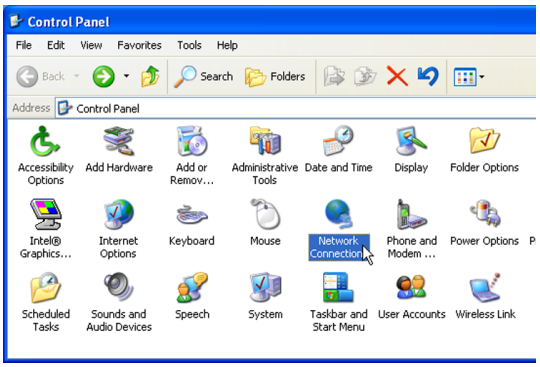


5. Click the **Status** button to verify if the Wireless LAN card is connected to the device. If connection is established, the **Association State** field shows "Connected - XX:XX:XX:XX:XX:XX"

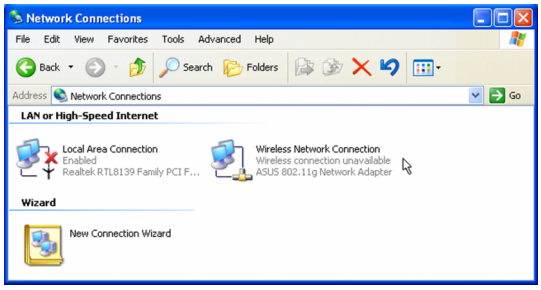


6. Click the **Connection** tab to display the connection strength and link quality between the Wireless LAN card and the wireless device.

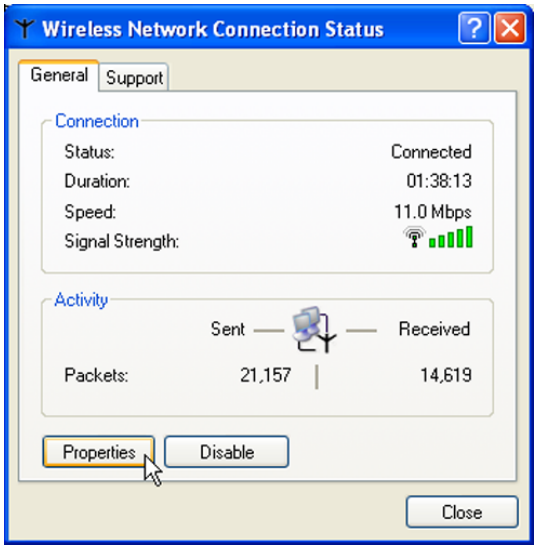
Windows XP Wireless Properties



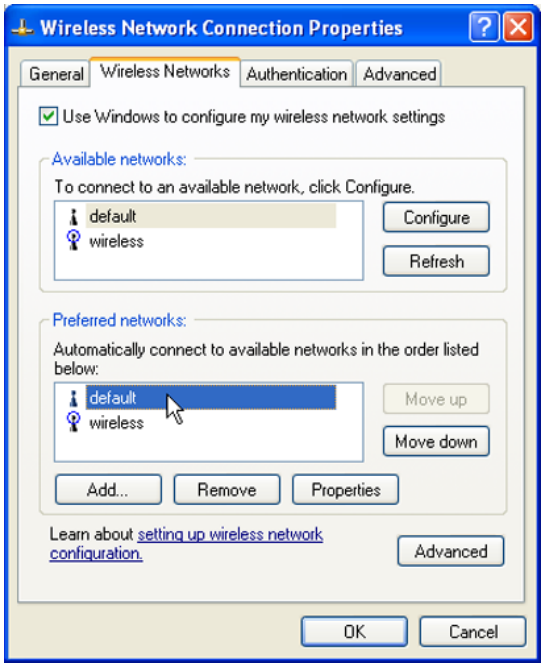
1. Double-click **System** icon in the Control Panel.



2. Double-click **WLAN ...**

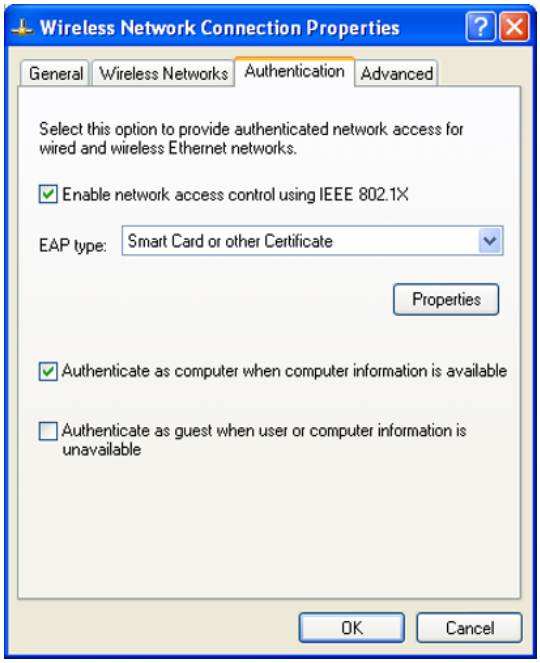


3. The “General” page will show status, duration, speed, and signal strength. Signal strength is represented by green bars with 5 bars meaning excellent signal and 1 bar meaning poor signal.

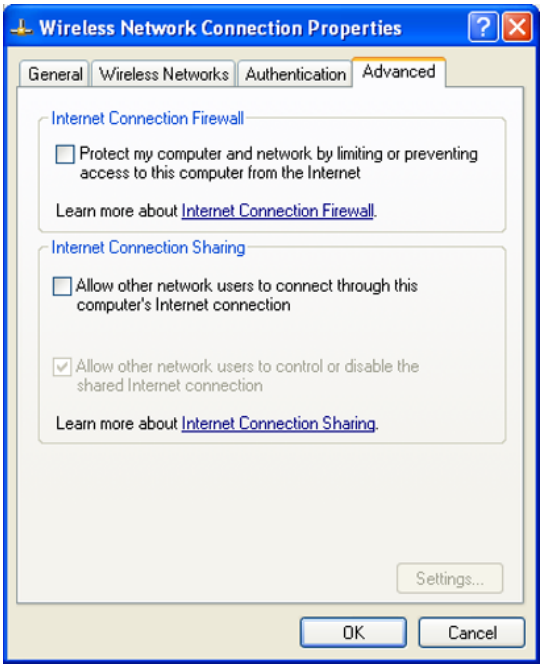


4. The “Wireless Networks” page will show Available networks and Preferred networks. Use the **Add** button to add the “SSID” of available networks and set the connection preference order with the **Move up** and **Move down** buttons. The radio tower with a signal icon identifies the currently connected access point.

Windows XP Wireless Properties (Cont.)



5. The "Authentication" page allows you to add security settings. Read Windows help for more information.



6. The "Advanced" page allows you to set firewall and sharing. Read Windows help for more information.

4. Troubleshooting

The following troubleshooting guides provide answers to some of the more common problems, which you may encounter while installing or using WLAN Card products. If you encounter difficulties that are not mentioned in this section, please contact Wireless LAN Technical Support.

Verify if the WLAN Card is installed correctly.

When the WLAN Card setup is complete, you can verify if the driver has been setup properly. Right click **My Computer**, select **Properties**, and click the **Device Manager** tab. Then double-click the **Network adapters** icon; you should see "**802.11g Network Adapter**" with an icon of an expansion card. There should not be a "!" or "?" (problem) or "x" (disabled) symbol over this icon.

There is a yellow exclamation mark or a yellow question mark in Device Manager in front of my WLAN Card.

To resolve the problem, you should update/reinstall the WLAN Card driver. In "Device Manager", right click **802.11g Network Adapter**, select **Properties**, and select **Driver** tab. Click on **Update Driver** button, then follow the "Update Device Driver Wizard" to complete the driver installation.

Cannot connect to any Access Points

Follow the procedure below to configure your WLAN Card.

a. Verify that the "Network Type" is in "Infrastructure" mode.

b. Verify that the "SSID" of your WLAN Card is set to the same "SSID" of an Access Point.

c. Verify that the "Encryption" type is the same as that of an Access Point. If you enabled "WEP" encryption, you must also set the same WEP Keys on both sides.

Cannot connect to a Station (WLAN Card)

Follow the procedure below to configure your WLAN Card.

a. Verify that the "Network Type" is in "Ad Hoc" mode.
b. Verify that the "SSID" of your WLAN Card is set to the same "SSID" of the other station (or another WLAN Card).
c. Verify that the "channel" of the WLAN Card is "Auto" or set to the same "channel" of the other station (or another WLAN Card).
d. Verify that the "Encryption" type is the same as the other station (or another WLAN Card). If "WEP" encryption is enabled, you must set the same "WEP" Keys on both stations.

Bad link quality or bad signal strength

There are two possible reasons. First is radio interference, keep the environment around the WLAN Card away from microwave ovens and large metal objects. Then try to reorient the WLAN Card antenna. Second is the distance, decrease the distance between your WLAN Card and the Access Point or station (or another WLAN Card).

The TCP/IP protocol did not bind to the WLAN PC Card.

This will occur when the computer already has six TCP/IP bindings in Windows 98 or ten bindings in Windows Me. These limits are imposed by the Microsoft operating system.

Solution: If your computer already has the maximum number of TCP/IP bindings, remove one of the network adapters from the Network configuration before installing the WLAN Card driver.

5. Glossary

Access Point (AP)

An networking device that seamlessly connects wired and wireless networks. Access Points combined with a distributed system support the creation of multiple radio cells that enable roaming throughout a facility.

Ad Hoc

A wireless network composed solely of stations within mutual communication range of each other (no Access Point).

Basic Rate Set

This option allows you to specify the data transmission rate.

Basic Service Area (BSS)

A set of stations controlled by a single coordination function.

Broadband

A type of data transmission in which a single medium (such as cable) carries several channels of data at once.

Channel

An instance of medium use for the purpose of passing protocol data units that may be used simultaneously, in the same volume of space, with other instances of medium use (on other channels) by other instances of the same physical layer, with an acceptably low frame error ratio due to mutual interference.

Client

A client is the desktop or mobile PC that is connected to your network.

COFDM (for 802.11a or 802.11g)

Signal power alone is not enough to maintain 802.11b-like distances in an 802.11a/g environment. To compensate, a new physical-layer encoding technology was designed that departs from the traditional direct-sequence technology being deployed today. This technology is called COFDM (coded OFDM). COFDM was developed specifically for indoor wireless use and offers performance much superior to that of spread-spectrum solutions. COFDM works by breaking one high-speed data carrier into several lower-speed subcarriers, which are then transmitted in parallel. Each high-speed carrier is 20 MHz wide and is broken up into 52 subchannels, each approximately 300 KHz wide. COFDM uses 48 of these subchannels for data, while the remaining four are used for error correction. COFDM delivers higher data rates and a high degree of multipath reflection recovery, thanks to its encoding scheme and error correction.

Each subchannel in the COFDM implementation is about 300 KHz wide. At the low end of the speed gradient, BPSK (binary phase shift keying) is used to encode 125 Kbps of data per channel, resulting in a 6,000-Kbps, or 6 Mbps, data rate. Using quadrature phase shift keying, you can double the amount of data encoded to 250 Kbps per channel, yielding a 12-Mbps data rate. And by using 16-level quadrature amplitude modulation encoding 4 bits per hertz, you can achieve a data rate of 24 Mbps. The 802.11a/g standard specifies that all 802.11a/g-compliant products must support these basic data rates. The standard also lets the vendor extend the modulation scheme beyond 24 Mbps. Remember, the more bits per cycle (hertz) that are encoded, the more susceptible the signal will be to interference and fading, and ultimately, the shorter the range, unless power output is increased.

Default Key

This option allows you to select the default WEP key. This option allows you to use WEP keys without having to remember or write them down. The WEP keys generated using the Pass Phrase is compatible with other WLAN products. The Pass Phrase option is not as secure as manual assignment.

Device Name

Also known as DHCP client ID or network name. Sometimes provided by an ISP when using DHCP to assign addresses.

DHCP (Dynamic Host Configuration Protocol)

This protocol allows a computer (or many computers on your network) to be automatically assigned a single IP address from a DHCP server.

DNS Server Address (Domain Name System)

DNS allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a user enters a domain name into the Internet browser, the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL Modem (Digital Subscriber Line)

A DSL modem uses your existing phone lines to transmit data at high speeds.

Direct-Sequence Spread Spectrum (for 802.11b)

Spread spectrum (broadband) uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range.

Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a chipping sequence. Each bit of transmitted data is mapped into chips and rearranged into a pseudorandom spreading code to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the output signal.

Wireless mobile clients receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the wireless device. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting wireless device to the receiving wireless mobile client.

This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving wireless mobile client to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference. The ratio of chips per bit is called the spreading ratio. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The wireless device uses a constant chip rate of 11Mchips/s for all data rates, but uses different modulation schemes to encode more bits per chip at the higher data rates. The wireless device is capable of an 11 Mbps data transmission rate, but the coverage area is less than a 1 or 2 Mbps wireless device since coverage area decreases as bandwidth increases.

Encryption

This provides wireless data transmissions with a level of security. This option allows you to specify a 64-bit or a 128-bit WEP key. A 64-bit encryption contains 10 hexadecimal digits or 5 ASCII characters. A 128-bit encryption contains 26 hexadecimal digits or 13 ASCII characters.

64-bit and 40-bit WEP keys use the same encryption method and can interoperate on wireless networks. This lower level of WEP encryption uses a 40-bit (10 hexadecimal digits assigned by the user) secret key and a 24-bit Initialization Vector assigned by the device. 104-bit and 128-bit WEP keys use the same encryption method.

All wireless clients in a network must have identical WEP keys with the access point to establish connection. Keep a record of the WEP encryption keys.

Extended Service Set (ESS)

A set of one or more interconnected basic service set (BSSs) and integrated local area networks (LANs) can be configured as an Extended Service Set.

ESSID (Extended Service Set Identifier)

You must have the same ESSID entered into the gateway and each of its wireless clients. The ESSID is a unique identifier for your wireless network.

Ethernet

The most widely used LAN access method, which is defined by the IEEE 802.3 standard. Ethernet is normally a shared media LAN meaning all devices on the network segment share total bandwidth. Ethernet networks operate at 10Mbps using CSMA/CD to run over 10-BaseT cables.

Firewall

A firewall determines which information passes in and out of a network. NAT can create a natural firewall by hiding a local network's IP addresses from the Internet. A Firewall prevents anyone outside of your network from accessing your computer and possibly damaging or viewing your files.

Gateway

A network point that manages all the data traffic of your network, as well as to the Internet and connects one network to another.

IEEE

The Institute of Electrical and Electronics Engineers. The IEEE sets standards for networking, including Ethernet LANs. IEEE standards ensure interoperability between systems of the same type.

IEEE 802.11

IEEE 802.xx is a set of specifications for LANs from the Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared. 802.11 specifies a carrier sense media access control and physical layer specifications for 1 and 2 Mbps wireless LANs.

IEEE 802.11a (54Mbits/sec)

Compared with 802.11b: The 802.11b standard was designed to operate in the 2.4-GHz ISM (Industrial, Scientific and Medical) band using direct-sequence spread-spectrum technology. The 802.11a standard, on the other hand, was designed to operate in the more recently allocated 5-GHz UNII (Unlicensed National Information Infrastructure) band. And unlike 802.11b, the 802.11a standard departs from the traditional spread-spectrum technology, instead using a frequency division multiplexing scheme that's intended to be friendlier to office environments.

The 802.11a standard, which supports data rates of up to 54 Mbps, is the Fast Ethernet analog to 802.11b, which supports data rates of up to 11 Mbps. Like Ethernet and Fast Ethernet, 802.11b and 802.11a use an identical MAC (Media Access Control). However, while Fast Ethernet uses the same physical-layer encoding scheme as Ethernet (only faster), 802.11a uses an entirely different encoding scheme, called OFDM (orthogonal frequency division multiplexing).

The 802.11b spectrum is plagued by saturation from wireless phones, microwave ovens and other emerging wireless technologies, such as Bluetooth. In contrast, 802.11a spectrum is relatively free of interference.

The 802.11a standard gains some of its performance from the higher frequencies at which it operates. The laws of information theory tie frequency, radiated power and distance together in an inverse relationship. Thus, moving up to the 5-GHz spectrum from 2.4 GHz will lead to shorter distances, given the same radiated power and encoding scheme.

Compared with 802.11g: 802.11a is a standard for access points and radio NICs that is ahead of 802.11g in the market by about six months. 802.11a operates in the 5GHz frequency band with twelve separate non-overlapping channels. As a result, you can have up to twelve access points set to different channels in the same area without them interfering with each other. This makes access point channel assignment much easier and significantly increases the throughput the wireless LAN can deliver within a given area. In addition, RF interference is much less likely because of the less-crowded 5 GHz band.

IEEE 802.11b (11Mbits/sec)

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard for wireless devices operating in the 2.4 GHz frequency band. This standard includes provisions for three radio technologies: direct sequence spread spectrum, frequency hopping spread spectrum, and infrared. Devices that comply with the 802.11 standard operate at a data rate of either 1 or 2 Mbps.

In 1999, the IEEE created the 802.11b standard. 802.11b is essentially identical to the 802.11 standard except 802.11b provides for data rates of up to 11 Mbps for direct sequence spread spectrum devices. Under 802.11b, direct sequence devices can operate at 11 Mbps, 5.5 Mbps, 2 Mbps, or 1 Mbps. This provides interoperability with existing 802.11 direct sequence devices that operate only at 2 Mbps.

Direct sequence spread spectrum devices spread a radio signal over a range of frequencies. The IEEE 802.11b specification allocates the 2.4 GHz frequency band into 14 overlapping operating Channels. Each Channel corresponds to a different set of frequencies.

IEEE 802.11g

802.11g is a new extension to 802.11b (used in majority of wireless LANs today) that broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. 802.11g allows backward compatibility with 802.11b devices but only at 11 Mbps or lower, depending on the range and presence of obstructions.

Infrastructure

A wireless network centered about an access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

IP (Internet Protocol)

The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an Internet and provides the basis for connectionless packet delivery service. IP includes the ICMP control and error message protocol as an integral part. It provides the functional equivalent of ISO OSI Network Services.

IP Address

An IP address is a 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

ISM Bands (Industrial, Scientific, and Medicine Bands)

Radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 902 MHz, 2.400 GHz, and 5.7 GHz.

ISP (Internet Service Provider)

An organization that provides access to the Internet. Small ISPs provide service via modem and ISDN while the larger ones also offer private line hookups (T1, fractional T1, etc.).

LAN (Local Area Network)

A communications network that serves users within a defined geographical area. The benefits include the sharing of Internet access, files and equipment like printers and storage devices. Special network cabling (10 Base-T) is often used to connect the PCs together.

MAC Address (Media Access Control)

A MAC address is the hardware address of a device connected to a network.

NAT (Network Address Translation)

NAT masks a local network's group of IP addresses from the external network, allowing a local network of computers to share a single ISP account. This process allows all of the computers on your home network to use one IP address. This will enable access to the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

NIC (Network Interface Card)

A network adapter inserted into a computer so that the computer can be connected to a network. It is responsible for converting data from stored in the computer to the form transmitted or received.

Packet

A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Pass Phrase

The Wireless Settings utility uses an algorithm to generate four WEP keys based on the typed combination.

PCMCIA (Personal Computer Memory Card International Association)

The Personal Computer Memory Card International Association (PCMCIA), develops standards for PC cards, formerly known as PCMCIA cards. These cards are available in three types, and are about the same length and width as credit cards. However, the different width of the cards ranges in thickness from 3.3 mm (Type I) to 5.0 mm (Type II) to 10.5 mm (Type III). These cards can be used for various functions, including memory storage, land line modems and wireless modems.

PPP (Point-to-Point Protocol)

PPP is a protocol for communication between computers using a serial interface, typically a personal computer connected by phone line to a server.

PPPoE (Point-to-Point Protocol over Ethernet)

Point-to-Point Protocol is a method of secure data transmission. PPP using Ethernet to connect to an ISP.

Preamble

Allows you to set the preamble mode for a network to Long, Short, or Auto. The default preamble mode is Long.

Radio Frequency (RF) Terms: GHz, MHz, Hz

The international unit for measuring frequency is Hertz (Hz), equivalent to the older unit of cycles per second. One megahertz (MHz) is one million Hertz. One gigahertz (GHz) is one billion Hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55-1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and wireless 802.11 LANs operate at 2.4 GHz.

SSID (Service Set Identifier)

SSID is a group name shared by every member of a wireless network. Only client PCs with the same SSID are allowed to establish a connection. Enabling the **Response to Broadcast SSID requests** option allows the device to broadcast its SSID in a wireless network. This allows other wireless devices to scan and establish communication with the device. Unchecking this option hides the SSID to prevent other wireless devices from recognizing and connecting to the device.

Station

Any device containing IEEE 802.11 wireless medium access conformity.

Subnet Mask

A subnet mask is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network.

TCP (Transmission Control Protocol)

The standard transport level protocol that provides the full duplex, stream service on which many application protocols depend. TCP allows a process or one machine to send a stream of data to a process on another. Software implementing TCP usually resides in the operating system and uses the IP to transmit information across the network.

WAN (Wide Area Network)

A system of LANs, connected together. A network that connects computers located in separate areas, (i.e., different buildings, cities, countries). The Internet is a wide area network.

WECA (Wireless Ethernet Compatibility Alliance)

An industry group that certifies cross-vender interoperability and compatibility of IEEE 802.11b wireless networking products and to promote that standard for enterprise, small business, and home environments.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (WPA) is an improved security system for 802.11. It is part of the 802.11i draft security standard. WPA encompasses TKIP (Temporal Key Integrity Protocol) along with MIC (Message Integrity Check) and other fixes to WEP such as Weak IV (Initialization Vector) filtering and Random IV generation. TKIP uses 802.1x to deploy and change temporary keys as opposed to static WEP keys once used in the past. It is a significant improvement over WEP. WPA is part of a complete security solution. WPA also requires authentication servers in enterprise security solutions.

Requirements

(1) A WPA compatible Access Point or Wireless router, (2) Operating system updates that support WPA. In XP, an updated Windows Zero Config service is needed. Users can download the Windows XP WPA patch here:

http://microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en

Please note that this patch requires the installation Windows XP Service Pack 1, which is available here: http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp

For earlier Windows Operating systems, a WPA capable supplicant is required such as Funk Software's Odyssey Client.

WLAN (Wireless Local Area Network)

This is a group of computers and other devices connected wirelessly in a small area. A wireless network is referred to as LAN or WLAN.

6. Safety Information

Federal Communications Commission

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING! The use of a shielded-type power cord is required in order to meet FCC emission limits and to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used. Use only shielded cables to connect I/O devices to this equipment. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Reprinted from the Code of Federal Regulations #47, part 15.193, 1993. Washington DC: Office of the Federal Register, National Archives and Records Administration, U.S. Government Printing Office.

FCC Radio Frequency Interference Requirements

MPE Statement: Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

This device is restricted to INDOOR USE due to its operation in the 5.15 to 5.25GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25GHz to reduce the potential for harmful interference to co-channel of the Mobile Satellite Systems.

High power radars are allocated as primary user of the 5.25 to 5.35GHz and 5.65 to 5.85GHz bands. These radar stations can cause interference with and / or damage this device.

FCC RF Exposure Guidelines (Access Points)

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247(b)(4) addressing RF Exposure from radio frequency devices. The radiation output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation – as a mobile or portable device but use in a body-worn way is strictly prohibit. When using this device, a certain separation distance between antenna and nearby persons has to be kept to ensure RF exposure compliance. In order to comply with the RF exposure limits established in the ANSI C95.1 standards, Access Point equipment should be installed and operated with minimum distance **[20cm]** between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

CAUTION: Any changes or modifications not expressly approved in this manual could void your authorization to use this device.

FCC RF Exposure Guidelines (Wireless Cards)

This device has been tested for compliance with FCC RF Exposure (SAR) limits in typical portable configurations.

In order to comply with SAR limits established in the ANSI C95.1 standards, it is recommended when using a WLAN Card adapter that the integrated antenna is positioned more than **[2.5cm]** from your body or nearby persons during extended periods of operation. If the antenna is positioned less than **[2.5cm]** from the user, it is recommended that the user limit the exposure time.

Canadian Department of Communications

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Operation Channel for Different Domains

N. America	2.412-2.462 GHz	Ch01 through CH11
Japan	2.412-2.484 GHz	Ch01 through Ch14
Europe ETSI	2.412-2.472 GHz	Ch01 through Ch13

France Restricted Frequency Band

Some areas of France have a restricted frequency band. The worst case maximum authorized power indoors is:

- 10mW for the entire 2.4 GHz band (2400 MHz–2483.5 MHz)
- 100mW for frequencies between 2446.5 MHz and 2483.5 MHz

NOTE: Channels 10 through 13 inclusive operate in the band 2446.6 MHz to 2483.5 MHz.

There are few possibilities for outdoor use: On private property or on the private property of public persons, use is subject to a preliminary authorization procedure by the Ministry of Defense, with maximum authorized power of 100mW in the 2446.5–2483.5 MHz band. Use outdoors on public property is not permitted.

In the departments listed below, for the entire 2.4 GHz band:

- Maximum authorized power indoors is 100mW
- Maximum authorized power outdoors is 10mW

Departments in which the use of the 2400–2483.5 MHz band is permitted with an EIRP of less than 100mW indoors and less than 10mW outdoors:

01 Ain Orientales	36 Indre	66 Pyrénées
02 Aisne	37 Indre et Loire	67 Bas Rhin
03 Allier	41 Loir et Cher	68 Haut Rhin
05 Hautes Alpes	42 Loire	70 Haute Saône
08 Ardennes	45 Loiret	71 Saône et Loire
09 Ariège	50 Manche	75 Paris
11 Aude	55 Meuse	82 Tarn et Garonne
12 Aveyron	58 Nièvre	84 Vaucluse
16 Charente	59 Nord	88 Vosges
24 Dordogne	60 Oise	89 Yonne
25 Doubs	61 Orne	90 Territoire de Belfort
26 Drôme	63 Puy du Dôme	94 Val de Marne
32 Gers	64 Pyrénées Atlantique	

This requirement is likely to change over time, allowing you to use your wireless LAN card in more areas within France. Please check with ART for the latest information (www.art-telecom.fr)

NOTE: Your WLAN Card transmits less than 100mW, but more than 10mW.