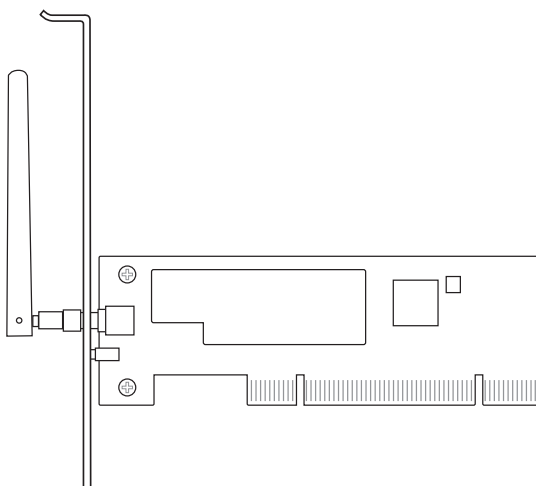




PCI-G31

Wireless Local Area Network Card
(For 802.11g & 802.11b Wireless Networks)



User Manual

Copyright © 2009 ASUSTeK Computer Inc. All Rights Reserved.

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK Computer Inc. ("ASUS").

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Manufacturer contact information

ASUSTeK Computer Inc. (Asia-Pacific)

Company address: 15 Li-Te Road, Beitou, Taipei 11259
Telephone: +886-2-2894-3447
Fax: +886-2-2890-7798
E-mail: info@asus.com.tw
Web site: <http://www.asus.com.tw>

ASUS Computer International (America)

Company address: 800 Corporate Way, Fremont, CA 94539, USA
General (tel): +1-510-739-3777
General (fax): +1-510-608-4555
Web site address: <http://usa.asus.com>

Technical support

General support: +1-502-995-0883
Support (fax): +1-502-933-8713
Online support: <http://vip.asus.com/eservice/techserv.aspx>

ASUS Computer GmbH (Germany & Austria)

Company address: Harkortstr. 21-23, 40880 Ratingen, Germany
General (tel): +49-02102-95990
General (fax): +49-02102-959911
Web site address: <http://www.asuscom.de>
Online contact: <http://www.asuscom.de/sales>

Technical support

Components: +49-02102-95990
Fax: +49-02102-959911
Online support: <http://vip.asus.com/eservice/techserv.aspx?SLanguage=de-de>



Table of contents

Notices.....	2
1. Introduction	5
1.1 Package contents	5
1.2 System requirements	5
1.3 Hardware	5
2. Installing the PCI-G31 driver and utilities.....	6
3. Configuring PCI-G31 using ASUS utility.....	7
3.1 Connecting to a wireless network manually	7
3.2 Connecting to a wireless network using WPS	8
3.3 Soft AP mode (Windows® XP/Vista)	9
4. Software information	11
4.1 ASUS WLAN Control Center	11
4.2 ASUS WLAN Card Setting Utility	11
5. Configuring PCI-G31 using Windows® WZC service	21
6. Troubleshooting	23
7. Glossary.....	25



Notices

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 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: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement

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

This equipment should be installed and operated with minimum 20cm between the radiator and your body.



CE Mark Warning

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

Operation Channels: Ch1~11 for N. America, Ch1~14 Japan, Ch1~ 13 Europe (ETSI)

DGT Warning Statement

Article 12

Without permission, any company, firm or user shall not alter the frequency, increase the power, or change the characteristics and functions of the original design of the certified lower power frequency electric machinery.

Article 14

The application of low power frequency electric machineries shall not affect the navigation safety nor interfere a legal communication, if an interference is found, the service will be suspended until improvement is made and the interference no longer exists.

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。低功率射頻電機須忍受合法通信或作業、科學及醫療用電波輻射性電機設備之干擾。

臺灣地區使用頻率範圍及使用頻導數為 CH1~11 (2.412~2.483 GHz)

IC Warning Statement

This device has been designed to operate with the antennas for a maximum gain of 2dBi, antenna type: dipole.

Antennas not described as above are strictly prohibited for use with this device.



Declaration of Conformity

We, Manufacturer/Importer
(full address)

**ASUS COMPUTER GmbH HARKORT STR. 25
40880 RATINGEN, BRD. GERMANY**

declare that the product
(description of the apparatus, system, installation to which it refers)
is in conformity with

(reference to the specification under which conformity is declared)

in accordance with 2004/108/EC-EMC Directive and 1995/5 EC-R &TTE Directive

Product name: LAN PCI Adapter

Model name : PCI-G31

- | | | | |
|---|---|---|--|
| <input type="checkbox"/> EN 50392 | Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz-300GHz) | <input type="checkbox"/> EN 61000-3-2* | Disturbances in supply systems caused |
| <input type="checkbox"/> EN 50360
EN 50361 | the limitation of exposure of the general public to electromagnetic network equipment fields (0 Hz to 300 GHz) International Commission on Non-Ionizing Radiation Protection (1998). Guidelines for limiting exposure in time-varying electric, magnetic, and electromagnetic fields | <input type="checkbox"/> EN 61000-3-3* | Disturbances in supply systems caused |
| <input type="checkbox"/> EN50081-1 | Generic emission standard Part 1: Residual, commercial and light industry | <input type="checkbox"/> EN 301893 | Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive |
| <input type="checkbox"/> EN50082-2 | Generic immunity standard Part 2: Industrial environment | <input checked="" type="checkbox"/> EN 300328 | Electromagnetic compatibility and Radio spectrum Matters (ERM); wideband transmission equipment operating in the 2.4GHz ISM band and using spread spectrum modulation techniques. Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive |
| <input type="checkbox"/> EN 55020 | Immunity from radio interference of broadcast receivers and associated equipment | <input type="checkbox"/> EN300440-1
EN300440-2 | Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 1: Technical characteristics and test methods
Part 2: Harmonized EN under article 3.2 of the R&TTE Directive |
| <input type="checkbox"/> EN 55022 | Limits and methods of measurement of radio disturbance characteristics of information technology equipment | <input type="checkbox"/> EN 301511 | Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC) |
| <input type="checkbox"/> EN 55024 | Information Technology equipment-Immunity characteristics-Limits and methods of measurement | <input type="checkbox"/> EN 301 908-1
EN 301 908-2 | Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive |
| <input type="checkbox"/> EN 55013 | Limits and methods of measurement of radio disturbance characteristics of broadcast receivers and associated equipment | <input checked="" type="checkbox"/> EN 301489-1
EN 301489-17 | Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and services; Part 17: Specific conditions for wideband data and HIPERLAN equipment, Part1: Common technical requirements |
| <input type="checkbox"/> EN 50385 | Product standard to demonstrate the compliances or radio Base stations and fixed terminal stations for wireless telecommunication systems with the basic restriction or the reference level to human exposure to radio frequency electromagnetic field (110MHz-40GHz) -General public | | |
| <input type="checkbox"/> EN 300386 | Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication Electromagnetic Compatibility (EMC) requirements | | |
| <input checked="" type="checkbox"/> CE marking | | | |



(EC conformity marking)

The manufacturer also declares the conformity of above mentioned product with the actual required safety standards in accordance with LVD 2006/95/EC

- | | | | |
|--|---|---|---|
| <input type="checkbox"/> EN 60065 | Safety requirements for mains operated electronic and related apparatus for household and similar general use | <input checked="" type="checkbox"/> EN 60950-1 | Safety for information technology equipment including electrical business equipment |
|--|---|---|---|

Manufacturer/Importer

(Stamp)

Date : Jul. 30, 2008

Signature: 

Name : Jonathan Tseng



1. Introduction

1.1 Package contents

Check your PCI-G31 WLAN Card package for the following items.

- ASUS PCI-G31 WLAN Card x1
- External dipole antenna x1
- Quick Start Guide x1
- Support CD x1
- Low profile bracket x1
- Warranty card x1



NOTE: If any of the above items is damaged or missing, contact your retailer immediately.

1.2 System requirements

Before using the PCI-G31 WLAN Card, check if your system meets the following requirements:

- Windows® Vista/XP/2000/ME
- Standard 32-bit PCI slot
- 32MB system memory or larger
- 300MHz processor or higher

1.3 Hardware

Status indicator

The PCI-G31 WLAN Card comes with a status indicator that shows the realtime status of the WLAN card.

ON: The WLAN card is enabled.

Blinking: The WLAN card has connected to a wireless network successfully and data is being received or transmitted.

OFF: The WLAN card is disabled.

External dipole antenna

The PCI-G31 WLAN Card package includes an external dipole antenna. We recommend that you straighten up the antenna for the maximum range and best link quality.



2. Installing the PCI-G31 driver and utilities



IMPORTANT: Install the ASUS PCI-G31 WLAN Card into your computer before installing the driver and utilities from the bundled Support CD.

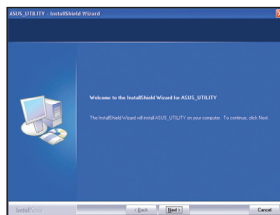
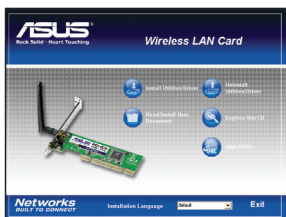
To install the driver and utilities for your ASUS PCI-G31 WLAN Card:

1. Place the bundled Support CD into the optical drive. An Autorun screen appears if the Autorun function is enabled on your computer.

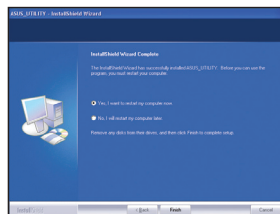
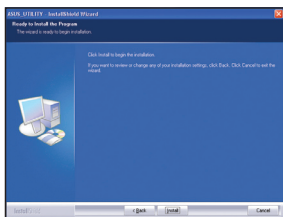


NOTE: If the Autorun function is not enabled on your computer, double-click **SETUP.EXE** from the root directory to run the Support CD.

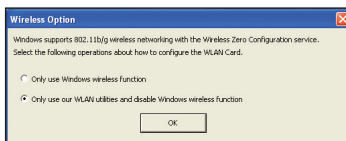
2. From the Autorun screen, select your language and click **Install Utilities/Driver**.
3. An **InstallShield Wizard** screen appears. Click **Next** to continue.



4. Click **Install** to start the installation.
5. Select **Yes, I want to restart my computer now**. Click **Finish** to complete the installation.



6. After your computer reboots, select **Only use our WLAN utilities and disable Windows wireless function** to allow the ASUS utility to manage your WLAN card. Click **OK**.





3. Configuring PCI-G31 using ASUS utility

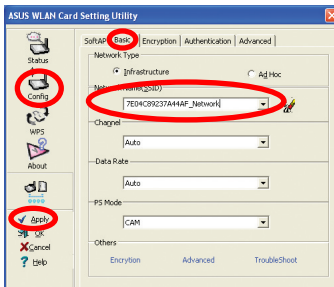
3.1 Connecting to a wireless network manually

To connect PCI-G31 to an access point (AP) (Infrastructure mode) or a station (Ad Hoc mode) manually:

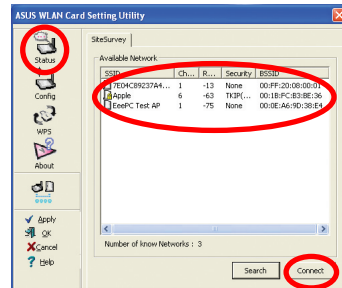
1. Right-click the ASUS WLAN Card Setting Utility icon in the Windows® system tray, then select **Wireless Setting**.



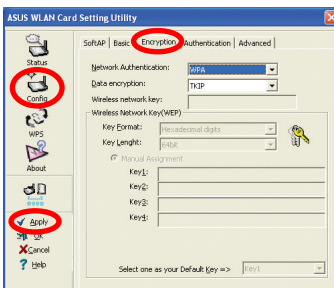
2. Set the **SSID** of your WLAN card to the same as that of the AP or station you are trying to connect to. Click **Apply**.



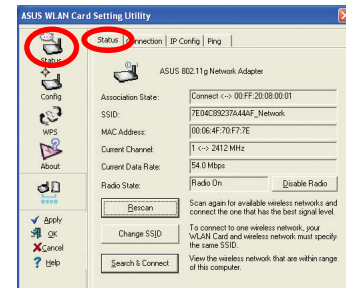
You may also click **Status > Search & Connect** to display the **SiteSurvey** page, then select a network from the **Available Network** list. Click **Connect**.



3. If Security is enabled on the AP or station, do the same security settings on your WLAN card as those on the AP or station. Click **Apply**.



Setup is completed. The **Status** page displays information such as the association state, current data rate, and radio state.





3.2 Connecting to a wireless network using WPS

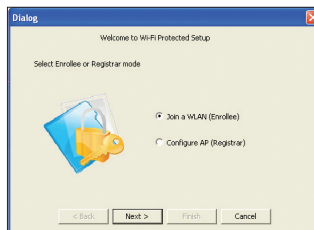
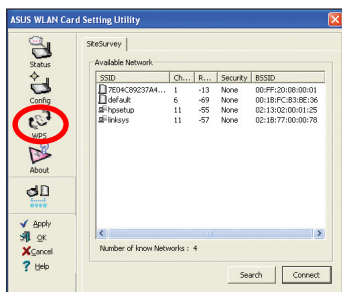
The ASUS PCI-G31 WLAN Card supports the WPS function that helps you set up a secure wireless network easily.



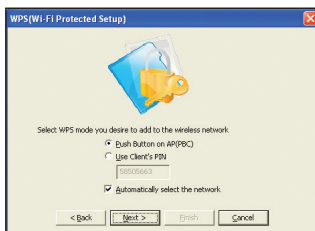
IMPORTANT: Ensure that the AP or station you are trying to connect to supports the WPS function.

To connect PCI-G31 to a WPS-enabled AP or station using the WPS push button:

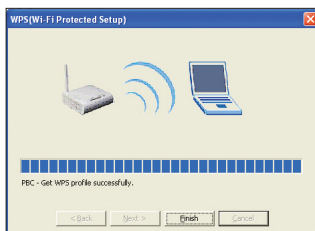
1. Click the **WPS** tab.
2. Select **Join a WLAN (Enrollee)**, then click **Next**.



3. Select **Push Button on AP (PBC)**, then click **Next**.
4. Press the WPS button on the AP or station to establish a wireless connection. The picture indicates that WPS is scanning for the network.



5. Click **Finish**. The picture indicates that your WLAN card has connected to the network successfully.





3.3 Soft AP mode (Windows® XP/Vista)

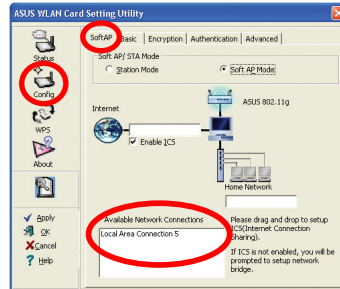
The ASUS PCI-G31 WLAN Card supports the Soft AP mode. In this mode, the WLAN card acts as a virtual AP.



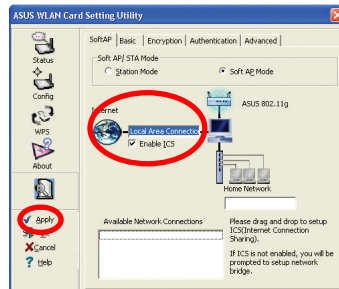
IMPORTANT: Before configuring the Soft AP mode, connect your computer to a wired network to provide network access for your wireless clients.

To switch to the Soft AP mode:



1. Click **Config > Soft AP**, then select **Soft AP_Mode**.

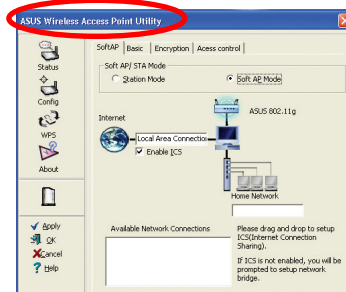


2. Select a network connection from the **Available Network Connections** box, then drag and drop it next to the globe icon. Select the **Enable ICS** checkbox.
3. Click **Apply**.



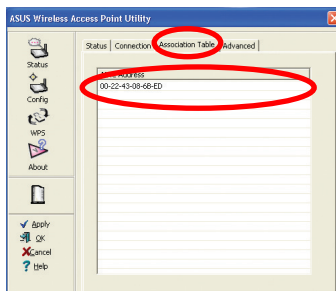
The picture on the right indicates that your WLAN card has switched to the Soft AP mode successfully.

- The utility's name switches to **ASUS Wireless Access Point Utility**.
- The ASUS WLAN Card Setting Utility icon  in the system tray switches to the ASUS Wireless Access Point Utility icon .





The Association Table page displays the wireless clients that are currently connecting to the Soft AP.

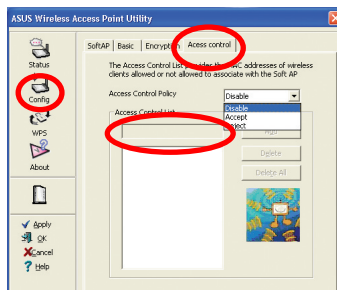


In the Soft AP mode, you can limit the wireless clients that associate with the WLAN card through the access control function.

To disable the access control function, select **Disable** from the **Access Control Policy** dropdown list.

To allow a wireless client to associate with the WLAN card:

1. Select **Accept** from the **Access Control Policy** dropdown list
2. Key in its MAC address in the **Access Control List** field.
3. Click **Add**.



Only the wireless clients on the Accept list are allowed to associate with the WLAN card.

To prevent a wireless client from associating with the WLAN card:

1. Select **Reject** from the **Access Control Policy** dropdown list.
2. Key in its MAC address in the **Access Control Policy** field.
3. Click **Add**.

The wireless clients on the Reject list are not allowed to associate with the WLAN card.



4. Software information

4.1 ASUS WLAN Control Center

ASUS WLAN Control Center includes ASUS WLAN Card Setting Utility (Station mode) and ASUS Wireless Access Point Utility (Soft AP mode) which help you manage your WLAN card easily.

4.2 ASUS WLAN Card Setting Utility

ASUS WLAN Card Setting Utility provides you with an easy interface to set up wireless connections. This section explains the buttons, fields, and configuration options on the user interface.

To launch ASUS WLAN Card Setting Utility, click **Start > All Programs > ASUS Utility > WLAN Card > ASUS WLAN Control Center**. The ASUS WLAN Card Setting Utility icon automatically appears in the system tray. It shows **No Device**, which indicates that your WLAN card is currently disabled.



To enable your WLAN card, click **Start > Control Panel > Network and Internet Connections > Network Connections > Wireless Network Connection**. The system tray icon switches as is shown in the picture.



ASUS WLAN Card Setting Utility system tray icon

Right-click the ASUS WLAN Card Setting Utility system tray icon to display the following options:

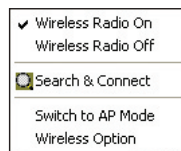
- **Wireless Settings** - Launches the ASUS WLAN Card Setting Utility.
- **Activate Configuration** - Activates a preset profile.
- **WPS** - Launches the WPS wizard.
- **Help** - Launches the help file.
- **Preferences** - Creates a WLAN Control Center shortcut on the desktop and launches it at startup.
- **About Control Center** - Displays the version of your Control Center.
- **Exit Control Center** - Closes the ASUS WLAN Control Center.





Left-click the ASUS WLAN Card Setting Utility system tray icon to display the following options:

- **Wireless Radio On** - Turns the wireless radio ON.
- **Wireless Radio Off** - Turns the wireless radio OFF.
- **Search & Connect** - Displays the available wireless networks.
- **Switch to AP Mode** - Switches your WLAN card to the AP mode.
- **Wireless Option** - Selects the ASUS utility or the Windows® WZC utility as the management software.



Double-click the icon to launch the ASUS WLAN Card Setting utility.



Status - Status

Association State - Displays the connection status:

Connect - The WLAN card is associated with a WLAN device. When the WLAN card is operating in the Infrastructure mode, this field shows the MAC address of the AP it is connecting to. When the WLAN card is operating in the Ad Hoc mode, this field shows the virtual MAC address used by computers participating in the Ad Hoc network.

Scanning - The WLAN card is trying to associate with an AP or Ad Hoc node.

Disconnect - No link is established.

SSID - Displays the name of the wireless network that the WLAN card is connecting to.

MAC Address - Indicates the hardware address of the WLAN card. A MAC address is a unique identifier assigned to networking devices. It consists of six groups of two hexadecimal digits (0 through 9 and A through F) separated by colons, e.g. 00:E0:18:F0:05:C0.

Current Channel - Displays the channel of the wireless network.

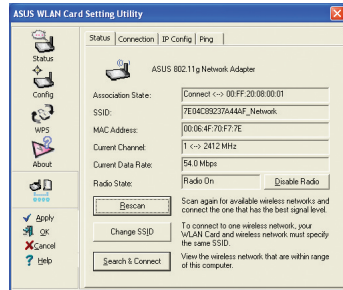
Current Data Rate - Displays the current data transmission rate.

Radio State - Displays the wireless radio status.

Rescan - Rescans for available wireless networks in your location and connects to the one with the best signal.

Change SSID - Set the SSID of the WLAN card.

Search & Connect - Launches the SiteSurvey page that displays the available networks in your location.





Status - Connection

Frame Sent/Received

Transmitted - Displays the number of frames sent from the WLAN card.

Received - Displays the number of frames received by the WLAN card.

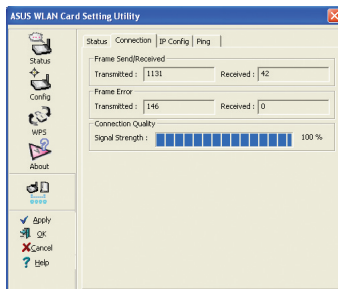
Frame Error

Transmitted - Displays the number of frames that were not successfully sent.

Received - Displays the number of frames that were not successfully received.

Connection Quality

Signal Strength - Indicates the signal level of the AP or the Ad Hoc node the WLAN card is currently connecting to.



Status - IP Config

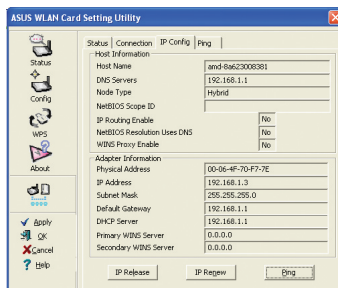
Host Information - Displays the configuration information about the wireless network the WLAN card is currently connecting to.

Adapter Information - Displays TCP/IP settings of the WLAN card.

IP Release - Remove the current IP address of the WLAN card and get an IP address from a DHCP server.

IP Renew - Get a new IP address from a DHCP server.

Ping - Launch the Ping page.



NOTE: The IP Release and IP Renew buttons work only when the WLAN card is connecting to an AP with the DHCP server function.



Status - Ping

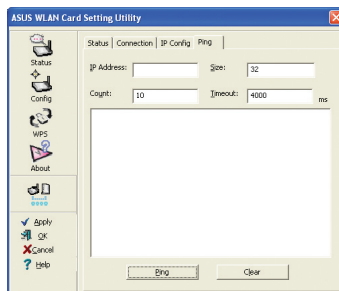
The Ping page allows you to verify the accessibility of a wireless network.

To ping a connection:

1. Key in the IP address of the AP or the Ad Hoc node in the **IP Address** field.
2. Assign the ping packet size, the number of packets to be sent, and the timeout value.
3. Click **Ping**.

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 **Clear** to clear the session field.

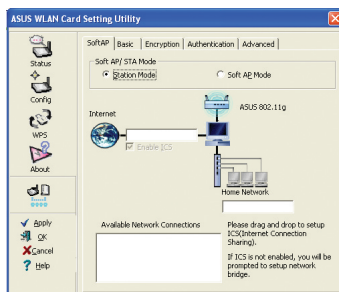


Config - SoftAP

The Soft AP page allows you to switch your WLAN card to the AP mode. Click

Soft AP_Mode to start the configuration.

Refer to **3.3 Soft AP mode (Windows® XP/Vista)** for details.



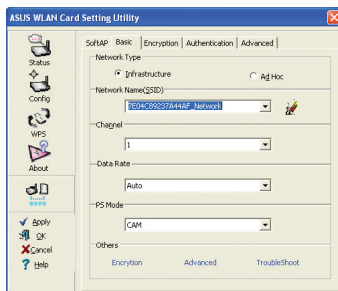


Config - Basic

Network Type

Infrastructure - Select the Infrastructure mode to establish a connection with an AP.

Ad Hoc - Select the Ad Hoc mode to communicate with a station. An Ad Hoc network is formed quickly and easily without pre-planning. For example, you can share meeting notes among networked computers in a meeting room.



Network Name (SSID) - Key in or select from the dropdown list the SSID of an AP or station you are trying to connect to. An SSID must be valid characters and have a maximum of 32 case sensitive characters, such as Wireless LAN.



NOTE: Set the SSID to a null string if you want to allow your WLAN card to connect to any AP it can find. You cannot use a null string in the Ad Hoc mode.

Channel - Select a radio channel for your WLAN card. In the Infrastructure mode, your WLAN card automatically selects the correct channel required to communicate with an AP and this field shows **Auto**. In the Ad Hoc mode, you are allowed to select a channel for your WLAN Card. WLAN cards in the same network can communicate with each other if they have the same channel setting.

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

Data Rate - Select the data transmission rate. Options are:

Auto: The WLAN card adjusts to the most suitable transmission rate automatically.

11g: The data transmission rate is fixed to: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54Mbps.

11b: The data transmission rate is fixed to: 1, 2, 5.5, or 11Mbps.

Others

Encryption - Launches the Encryption page.

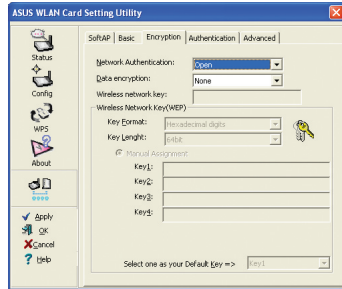
Advanced - Launches the Advanced page. In most cases, you do not need to change the default values.

Troubleshooting - Displays the troubleshooting solutions.



Config - Encryption

The Encryption page allows you to set up the encryption settings for your WLAN card. 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. WEP uses keys to encrypt data packets sent and decrypt data packets received. The encryption process can scramble frame bits to avoid disclosure to others. Wi-Fi Protected Access (WPA) is an improved security system for 802.11 that encrypts data sent over radio waves. WPA is developed to overcome the weakness of the WEP protocol.



Network Authentication - Set up authentication for your WLAN card. Options are:

Open - Sets the network operating in the Open System mode that disables authentication protection for the network or use the WEP encryption for the network.

Shared - Sets the network operating in the Shared Key mode that uses the WEP encryption for your network.

WPA-PSK/WPA2-PSK - Use the WPA Pre-Shared Key/WPA2 Pre-Shared Key in the Infrastructure mode for authentication.

WPA/WPA2 - Enables the IEEE 802.1x authentication mode. This mode is for environments with Remote Access Dial-in User Service (Radius). In a RADIUS environment, various Extensible Authentication Protocol (EAP) are supported, including PEAP, TLS/Smart Card.

Data Encryption - In the Open and Shared authentication modes, options are: None and WEP.

None - Disables the encryption protection for your WLAN card.

WEP - Encrypts the data before it is transmitted over the air. You can communicate with wireless devices that use the same WEP keys.

In the WPA-PSK/WPA2-PSK and WPA/WPA2 authentication modes, options are: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

TKIP - Dynamically generates unique keys to encrypt data packet.

AES - Offers stronger protection and increases the complexity of wireless encryption. It is a symmetric 128-bit block encryption method that works simultaneously on multiple network layers.



Wireless Network Key - This option becomes configurable when you select WPA-PSK/WPA2-PSK in the Network Authentication field. Key in 8 to 64 characters in this field.

Wireless Network Key (WEP) - This option becomes configurable when you select WEP in the Data encryption field. 64-bit WEP key uses 5 ASCII characters (10 hexadecimal digits). 128-bit WEP key uses 13 ASCII (26 hexadecimal digits).

Key Format - Allows you to select the key format.

Key Length - Allows you to select the key length. For 64bits encryption, each key consists of 10 hexadecimal digits or 5 ASCII characters. For 128bits encryption, each key consists of 26 hexadecimal digits or 13 ASCII characters.

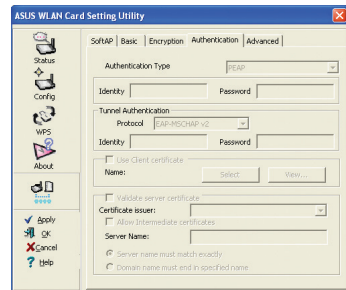
Manual Assignment - Allows you to assign WEP Keys manually.

Select one as your Default Key - Allows you to select one of the four WEP Keys as the default key.

Config - Authentication

The Authentication page allows you to configure security settings to match those on the wireless network you are trying to connect to. The fields in this page become configurable only when you have set the **Network Authentication** item in the Encryption page to **WPA** or **WPA2**.

Authentication Type - Select the authentication type. Options are:



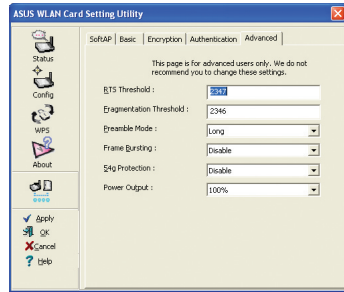
PEAP - Stands for Protected Extensible Authentication Protocol. PEAP is a version of Extensible Authentication Protocol (EAP). EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.

TLS/Smart Card - Stands for Transport Layer Security. TLS is used to create an encrypted tunnel and achieve server-side authentication in a manner similar to web server authentication using the Secure Sockets Layer (SSL) protocol. TLS uses digital certificates to verify the identity of a client and server.



Config - Advanced

This Advanced page is intended for experienced users to set up additional parameters for the WLAN card. We recommend that you keep the default values.



RTS Threshold (0-2347) - The Request to Send/Clear to Send (RTS/CTS) 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 - Select the preamble mode. The default value is Long.

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

54g Protection - Extended Rate PHY (ERP) protection mechanism of 802.11g definition. Options are:

Enable - Always send frame with protection.

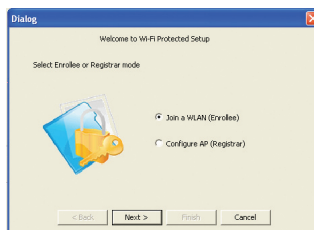
Disable - Always send frame without protection.

Power Output - Indicates the power level. Options are: 100%, 75%, 50%, and 25%.



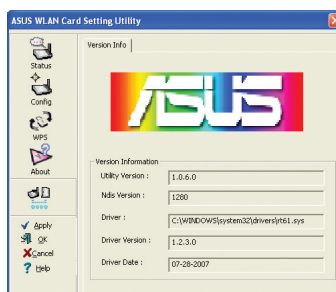
WPS (WiFi Protected Setup)

Click the WPS tab to launch the WPS wizard.
Refer to **3.2 Connecting to a wireless network using WPS** for details.



About - Version Info

The Version Info page displays information about the utility and driver versions of the ASUS PCI-G31 WLAN Card.

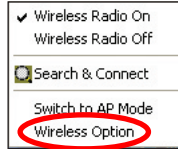




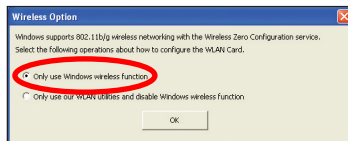
5. Configuring PCI-G31 using Windows® WZC service

To connect your PCI-G31 to a wireless network using Windows® WZC service:

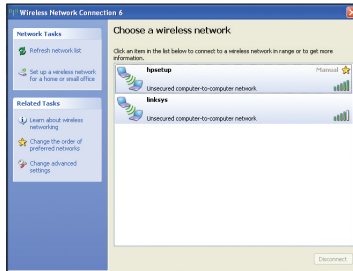
1. Left-click the ASUS WLAN Control Center system tray icon, then select **Wireless Option**.



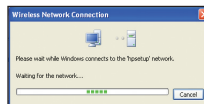
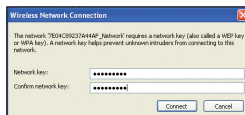
2. Select **Only use Windows wireless function** to enable the Windows wireless utility.



3. Double-click the Wireless Network Connection icon in the system tray to view the available wireless networks in your location. Select the network you want to connect to, then click **Connect**.

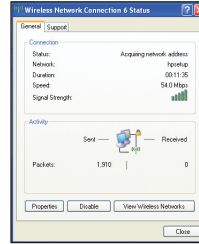


4. Key in the same network key on the network you are trying to connect to, then click **Connect**.





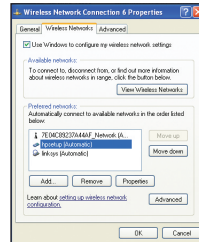
Click the Wireless Network Connection icon in the system tray to display the **Wireless Network Connection Status** window where you are given information on the wireless connection such as the status, speed, and signal strength.



You can save your favorite networks on your computer.

To save networks on your computer:

1. Click **Properties** from the Wireless Network Connection Status window, then select the **Wireless Networks** tab.
2. Click **Add** to add your favorite networks.
3. Set the connection preference order with the **Move up** and **Move down** buttons. Your computer will automatically connect to available networks in the order you set.





6. Troubleshooting

This chapter provides solutions to problems which you may encounter when installing or using the ASUS PCI-G31 WLAN card. Contact a qualified service technician for assistance if the problem still exists after you have performed the troubleshooting solutions.

How do I verify that my WLAN card is installed properly?

1. Right-click **My Computer** from the **Start** menu, then select **Properties**.
2. Select the **Hardware** tab, then click **Device Manager**.
3. Double-click **Network adapters**.
4. Double-click **Ralink Turbo Wireless LAN Card**. A **Ralink Turbo Wireless LAN Card Properties** window appears.
5. Check **Device status** to see if the WLAN Card is working properly.

There is a yellow exclamation mark or a yellow question mark over the icon of Ralink Turbo Wireless LAN Card in the Device Manager window.

In this case, you have to update/reinstall the WLAN card driver.

1. On the **Ralink Turbo Wireless LAN Card Properties** window, select the **Driver** tab.
2. Click **Update Driver**.
3. A **Hardware Update Wizard** window appears. Follow the onscreen instructions to complete the installation of the WLAN card driver.

My WLAN card cannot connect to any Access Points.

- Check if **Network Type** is set to the **Infrastructure** mode.
- Check if the **SSID** of your WLAN card is the same as that of the access point you want to connect to.
- Check if the **Encryption** settings of your WLAN card are the same as those of the access point you want to connect to.



My WLAN card cannot connect to a station or WLAN card.

- Check if **Network Type** is set to the **Ad Hoc** mode.
- Check if the **SSID** of your WLAN card is the same as that of the station or the WLAN card you want to connect to.
- Check if the **Channel** of your WLAN card is the same as that of the station or the WLAN card you want to connect to.
- Check if the **Encryption** settings of your WLAN card are the same as those of the station or the WLAN card you want to connect to.

The connection quality is bad and the signal strength is weak.

- Keep your WLAN card away from microwave ovens and large metal objects to avoid radio interference. Adjust the WLAN card antenna.
- Move your WLAN card closer to the access point, station, or WLAN card you want to connect to.

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

This occurs when your PC 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.



7. Glossary

Access Point (AP)

A 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 lowerspeed subcarriers, which are then transmitted in parallel. Each high-speed carrier is 20MHz wide and is broken up into 52 subchannels, each approximately 300KHz 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 300KHz wide. At the low end of the speed gradient, BPSK (binary phase shift keying) is used to encode 125Kbps of data per channel, resulting in a 6,000Kbps, or 6Mbps, data rate. Using quadrature phase shift keying, you can double the amount of data encoded to 250Kbps per channel, yielding a 12Mbps data rate. And by using 16-level quadrature amplitude modulation encoding 4bits per hertz, you can achieve a data rate of 24Mbps. 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 24Mbps. 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.



ICS

ICS is used to share one computer's Internet connection with the rest of the computers on your network. When this computer is connected to the Internet, all the communications to and from the Internet on your network are sent through this computer which is called the host computer. The rest of the computers can send and receive e-mail messages and access the web as if it were connected directly to the Internet.

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 (54Mbps/sec)

Compared with 802.11b: The 802.11b standard was designed to operate in the 2.4GHz 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 5GHz spectrum from 2.4GHz 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 5GHz band.

IEEE 802.11b (11Mbps/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 11Mbps for direct sequence spread spectrum devices. Under 802.11b, direct sequence devices can operate at 11Mbps, 5.5Mbps, 2Mbps, or 1Mbps. This provides interoperability with existing 802.11 direct sequence devices that operate only at 2Mbps.

Direct sequence spread spectrum devices spread a radio signal over a range of frequencies. The IEEE 802.11b specification allocates the 2.4GHz 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 902MHz, 2.400GHz, and 5.7GHz.

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 60Hz, the AM broadcast radio frequency band is 0.55-1.6MHz, the FM broadcast radio frequency band is 88-108MHz, and wireless 802.11 LANs operate at 2.4GHz.

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 prod WPA (Wi-Fi Protected Access)



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.

Manufacturer:	ASUSTeK Computer Inc. Tel: +886-2-2894-3447 Address: No. 150, LI-DE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised representative in Europe:	ASUS Computer GmbH Address: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY
Authorised distributors in Turkey:	BOGAZICI BIL GISAYAR SAN. VE TIC. A.S. Tel: +90 212 3311000 Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10 AYAZAGA/ISTANBUL
	INDEX BILGISAYAR SISTEMLERI MUHENDISLIK SAN. VE TIC. A.S. Tel: +90 212 3312121 Address: AYAZAGA MAH: CENDERE YOLU NO:9 AYAZAGA/ISTANBUL