ZyAIR G-160

802.11g Wireless Cardbus Card

User's Guide

Version 2.0
June 2004

ZyXEL
Unleash Networking Power

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patents' rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to one (1) year from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

NOTE

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization (RMA) number. Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register online at www.zyxel.com.for free future product updates and information.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operation and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

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 Industry.

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

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

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 commercial environment. 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.

If this equipment does cause harmful interference to radio/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:

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

Notice 1

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

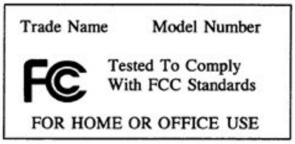
This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Caution

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Certifications

Refer to the product page at www.zyxel.com.



Trade Name Model Number

FC Tested To Comply
With FCC Standards

FOR HOME OR OFFICE USE

Customer Support

When contacting your Customer Support Representative, please have the following information ready:

- Product model and serial number.
- Warranty Information.
- Date you received your product.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway

[1] "+" is the (prefix) number you enter to make an international telephone call.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on the purchase of your new ZyAIR G-160 802.11g Wireless Cardbus Card!

About This User's Guide

This guide provides information about the ZyAIR G-160 Wireless LAN Utility that you use to configure your ZyAIR.

Syntax Conventions

- "Type" or "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- Window and command choices are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font.
- The ZyXEL ZyAIR G-160 802.11g Wireless Cardbus Card is referred to as the ZyAIR in this guide.
- The ZyAIR G-160 Wireless LAN Utility may be referred to as the ZyAIR Utility in this guide.

Related Documentation

- ➢ Support Disk

  Refer to the included CD for support documents and device drivers.

- ➢ Quick Installation Guide

  Our Quick Installation Guide is designed to help you get your ZyAIR up and running right away. It contains a detailed easy-to-follow connection diagram and information on installing your ZyAIR.

- ➢ ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you! E-mail all User's Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Chapter 1
Getting Started

This chapter prepares you to using the ZyAIR Utility.

1.1 About Your ZyAIR

The ZyAIR is an IEEE 802.11g compliant wireless LAN adapter. With the ZyAIR, you can enjoy the wireless mobility within the coverage area.

The following lists the main features of your ZyAIR.

- Your ZyAIR can communicate with other IEEE 802.11b/g compliant wireless devices.
- Automatic rate selection.
- Data transmission rates up to 54 Mbps.
- Offers 64-bit, 128-bit and 256-bit WEP (Wired Equivalent Privacy) data encryption for network security.
- Supports IEEE802.1x and WPA (Wi-Fi Protected Access).
- Low CPU utilization allowing more computer system resources for other programs.
- A built-in antenna
- Driver support for Windows XP/2000/Me/98 SE

1.2 ZyAIR Hardware and Utility Installation

Follow the instructions in the *Quick Installation Guide* to install the ZyAIR Utility and driver and make hardware connections.

1.3 Disable Windows XP Wireless LAN Configuration Tool

Windows XP includes a configuration tool (also known as Zero Configuration) for wireless LAN devices.

DO NOT use the Windows XP configuration tool and the ZyAIR Utility at the same time. It is recommended you use the ZyAIR Utility to configure the ZyAIR.

There are two methods to disable the configuration tool in Windows XP after you install the ZyAIR Utility:

- in the ZyAIR Utility **Main** screen (refer to the instruction in *Table 2-1*)
- in the **Connect to Wireless Network** screen (refer to *Section 1.3.1*).

1.3.1 The Connect to Wireless Network Screen

Follow the steps below to disable the configuration tool in Windows XP in the **Connect to Wireless Network** screen.

Step 1. Double-click on the network icon for the wireless connection in the system tray. If the icon is not present, proceed to *Step 2*. Otherwise skip to *Step 5*.

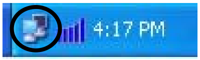
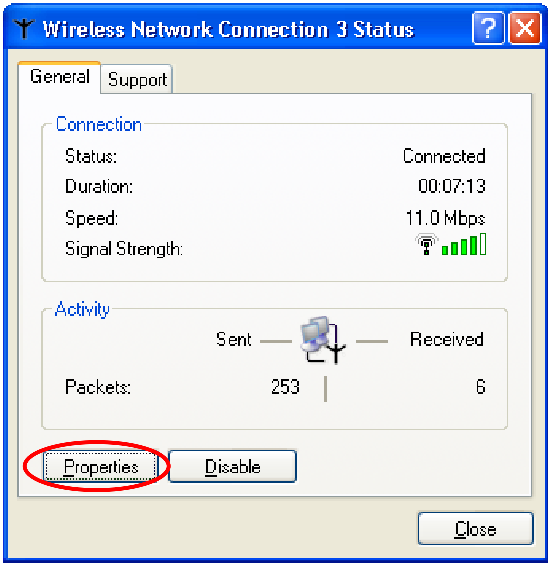


Figure 1-1 Windows XP: System Tray Icon

Step 2. If the icon for the wireless network connection is not in the system tray, click **Start**, **Control Panel** and double-click on **Network Connections**.

Step 3. Double-click on the icon for wireless network connection to display a status window as shown next.



Wireless Network Connection 3 Status

Connection

Status: Connected

Duration: 00:07:13

Speed: 11.0 Mbps

Signal Strength:

Activity

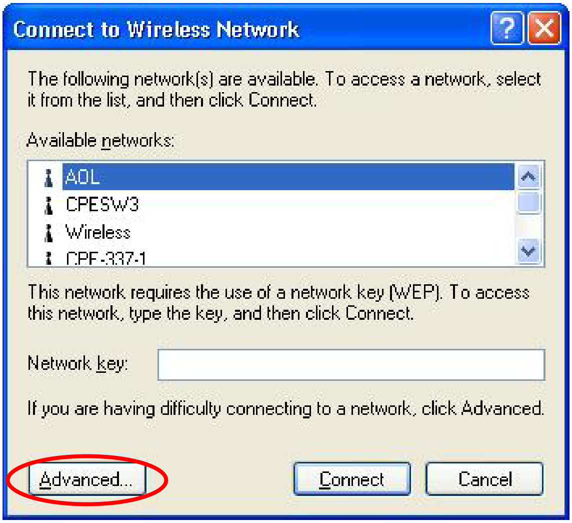
Sent — Received

Packets: 253 | 6

Figure 1-2 Windows XP: Wireless Network Connection Status

Step 4. Click **Properties** and click the **Wireless Networks** tab. Then skip to *Step 6*.

Step 5. When a **Connect to Wireless Network** window displays, click **Advanced…**.



Connect to Wireless Network

The following network(s) are available. To access a network, select it from the list, and then click Connect.

Available networks:

- AOL
- CPESW3
- Wireless
- CPE-337-1

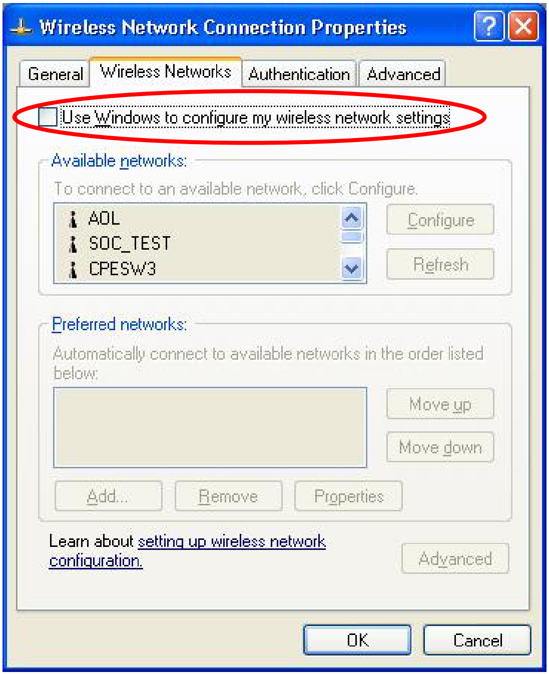
This network requires the use of a network key (WEP). To access this network, type the key, and then click Connect.

Network key:

If you are having difficulty connecting to a network, click Advanced.

Figure 1-3 Windows XP: Connect to Wireless Network

Step 6. In the **Wireless Network Connection Properties** window, make sure the **Use Windows to configure my wireless network settings** check box is *not* selected. Click **OK**.



Wireless Network Connection Properties

□ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

AOL
SOC_TEST
CPESW3

Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

Figure 1-4 Windows XP: Wireless Network Connection Properties

1.4 Accessing the ZyAIR Utility

After you installed the ZyAIR Utility and reboot your computer, the ZyAIR Utility automatically starts and an icon for the ZyAIR Utility appears in the system tray.

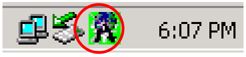


Figure 1-5 ZyAIR Utility: System Tray Icon

The color of the ZyAIR Utility system tray icon indicates the status of the ZyAIR. Refer to the following table for details.

Table 1-1 ZyAIR Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The radio is disabled if your computer provides the radio disable feature and you turn it on.
Green	The ZyAIR is connected to a wireless network.
Yellow	The ZyAIR is in the process of connecting to a wireless network.
Back and White	The ZyAIR is not inserted or the driver is not installed.

The ZyAIR Utility screens are similar in all Microsoft Windows versions. Screens for Windows 2000 are shown.

1.5 Common Screen Command Buttons

The following table shows common command buttons found on many screens.

Table 1-2 Common Screen Command Buttons

BUTTON	DESCRIPTION
_	Click the minimize button to minimize the ZyAIR Utility. Click on the ZyAIR Utility program in the task bar to open the ZyAIR Utility again.
X	Click the close button to close the ZyAIR Utility.
OK	Click **OK** to preserve the changes and minimize the ZyAIR Utility. Click on the ZyAIR Utility icon in the system tray to open the ZyAIR Utility again.
Cancel	Click **Cancel** to discard all changes and click it again to minimize the ZyAIR Utility. Click on the ZyAIR Utility icon in the system tray to open the ZyAIR Utility again.
Apply	Click **Apply** to save the changes to the ZyAIR.

Chapter 2
Using the ZyAIR Utility

This chapter shows you how to configure the ZyAIR using the ZyAIR Utility.

2.1 About Wireless LAN Network

This section describes each wireless LAN parameter.

2.1.1 Channel

The range of radio frequencies used by IEEE 802.11 wireless devices is called a "channel". The number of available channels depends on your geographical area. You may have a choice of channels (for your region) so adjacent APs (access points) should use different channels to reduce crosstalk. Crosstalk occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, the AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

2.1.2 SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

2.1.3 Transmission Rate (Tx Rate)

Your ZyAIR automatically adjusts the transmission rate to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the ZyAIR automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the ZyAIR gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

2.1.4 Wireless Network Application

Wireless LAN works in either of the two modes: ad-hoc and infrastructure.

To connect to a wired network within a coverage area using Access Points (APs), set the ZyAIR operation mode to **Infrastructure**. An AP acts as a bridge between the wireless stations and the wired network. In case you do not wish to connect to a wired network, but prefer to set up a small independent wireless workgroup without an AP, use the **Ad-hoc** mode.

Ad-Hoc (IBSS)

Ad-hoc mode does not require an AP or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

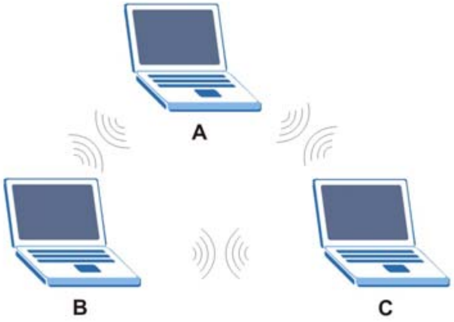


Figure 2-1 Ad-hoc Network Example

To set up an ad-hoc network, configure all wireless stations in ad-hoc network type and use the same SSID and channel.

Infrastructure

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

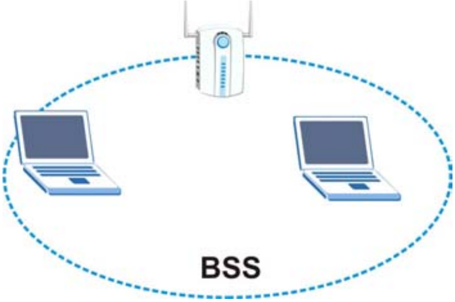


Figure 2-2 BSS Example

A series of overlapping BSS and a network medium, such as an Ethernet forms an Extended Service Set (ESS) or infrastructure network. All communication is done through the AP, which relays data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resource, such as the printer, on the wired network.

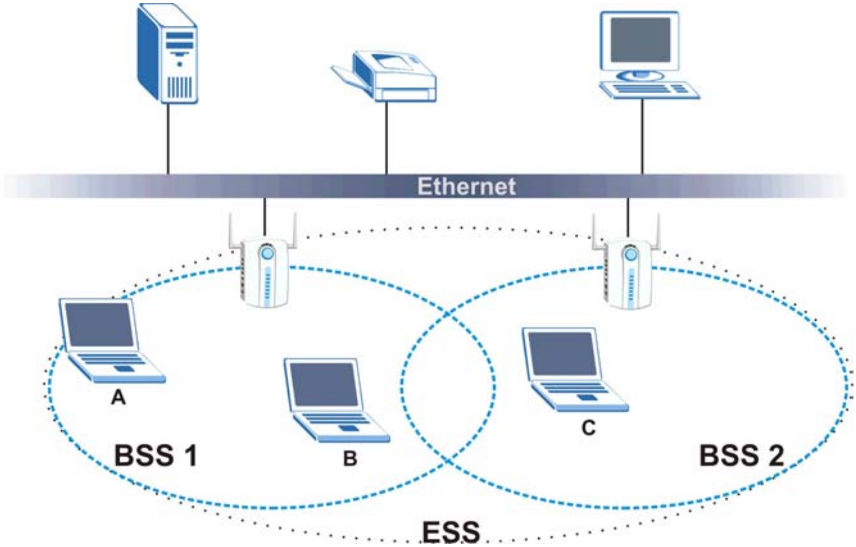


Figure 2-3 Infrastructure Network Example

2.1.5 Roaming

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization or other factors.

The following figure depicts a roaming example. When Wireless Station **B** moves to position **X**, the ZyAIR in wireless station **B** automatically switches the channel to the one used by access point **2** in order to stay connected to the network.

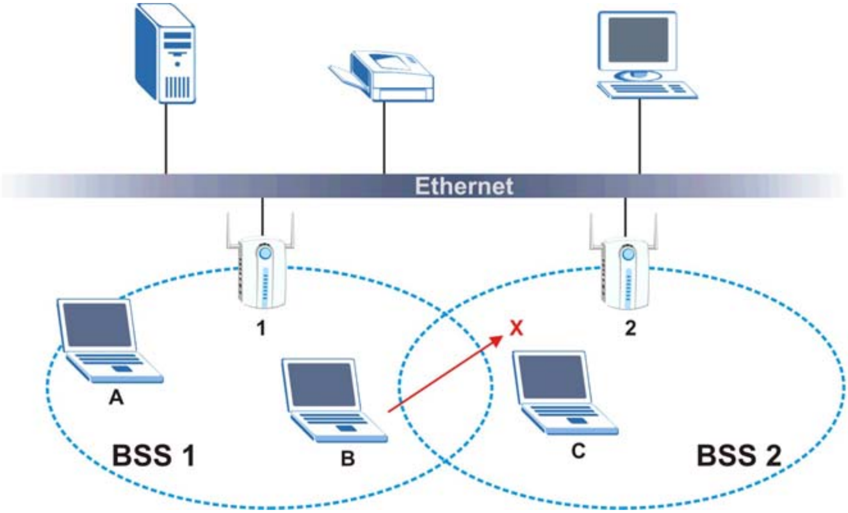


Figure 2-4 Roaming Example

2.1.6 Profile

The **Profile** function allows you to save or delete the wireless network settings and use one of the pre-configured network profiles.

2.1.7 Threshold Controls

Fragmentation Threshold

A fragmentation threshold is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyAIR will fragment the packet into smaller data frames.

A large fragmentation threshold is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the fragmentation threshold value is smaller than the **RTS Threshold** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS Threshold** size.

RTS Threshold

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

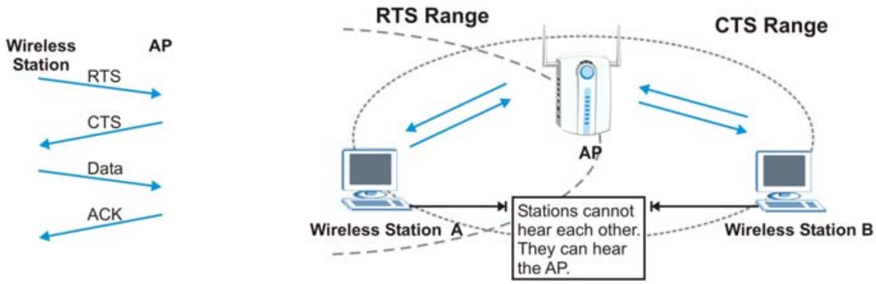


Figure 2-5 RTS Threshold

When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS Threshold is designed to prevent collisions due to hidden nodes. An **RTS Threshold** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS Threshold** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS Threshold** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS Threshold** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS Threshold** value is greater than the **Fragmentation Threshold** value, then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS Threshold** size.

2.1.8 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communication between wireless stations and the wired network.

The figure below shows the possible wireless security levels on your ZyAIR. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

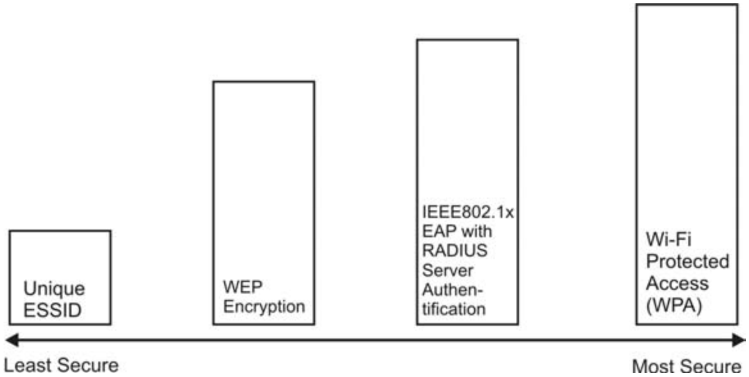

Unique ESSID
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tification
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

Figure 2-6 Wireless LAN Security Levels

Configure the wireless LAN security using the **Privacy** screen. If you do not enable any wireless security on your ZyAIR, communication between the ZyAIR and the wired network is accessible to any wireless networking device that is in the coverage area.

Make sure the security settings are the same on the ZyAIR and the intermediary AP and/or your network security server device.

2.1.9 Data Encryption with WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the ZyAIR and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

Your ZyAIR allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be used at any one time.

2.1.10 Authentication Mode

The IEEE 802.11b standard describes a simple authentication method between the wireless stations and AP. Three authentication modes are defined: **Auto Switch**, **Open System** and **Shared Key**.

Open System mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP do *not* share a secret key. Thus the wireless stations can associate with any AP and listen to any data transmitted plaintext.

Shared Key mode involves a shared secret key to authenticate the wireless station to the AP. This requires you to enable the WEP encryption and specify a WEP key on both the wireless station and the AP.

Auto Switch mode allows the ZyAIR to switch between the open and shared key authentication modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations.

2.1.11 Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long Preamble** and **Short Preamble**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long Preamble** if you have a 'noisy' network or are unsure of what preamble mode the access point or the other wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the ZyAIR and the access point/wireless stations and to provide more reliable communication in 'noisy' networks.

The ZyAIR and the access point MUST use the same preamble mode in order to communicate.

2.1.12 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE802.1x. The ZyAIR supports EAP-TLS, EAP-TTLS, EAP-PEAP and LEAP. Refer to the *Types of EAP Authentication* appendix for descriptions.

For EAP-TLS and EAP-TTLS authentication types, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

2.1.13 WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless station. As long as the passwords match, a station will be granted access to a WLAN.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

2.1.14 WPA-PSK Application Example

A WPA-PSK application looks as follows.

Step 1. First enter identical passwords into the AP and all wireless stations. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

Step 2. The AP checks each station's password and (only) allows it to join the network if it matches its password.

Step 3. The AP derives and distributes keys to the wireless stations.

Step 4. The AP and wireless stations use the TKIP encryption process to encrypt data exchanged between them.

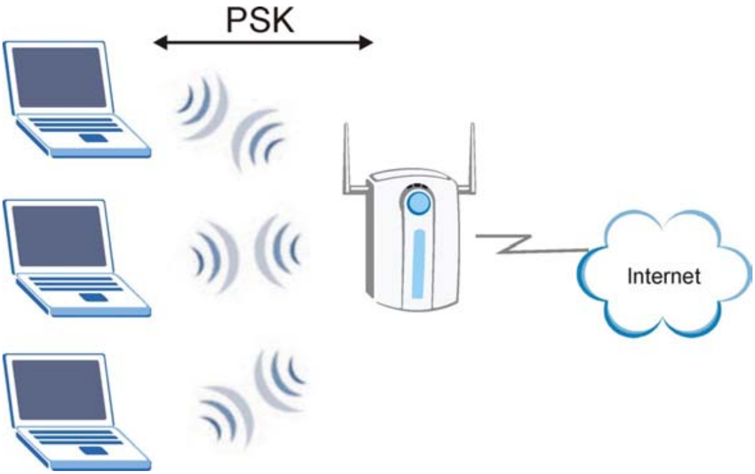


Figure 2-7 WPA - PSK Authentication

2.1.15 WPA with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. “A” is the RADIUS server. “DS” is the distribution system.

Step 1. The AP passes the wireless station’s authentication request to the RADIUS server.

Step 2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

Step 3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations.

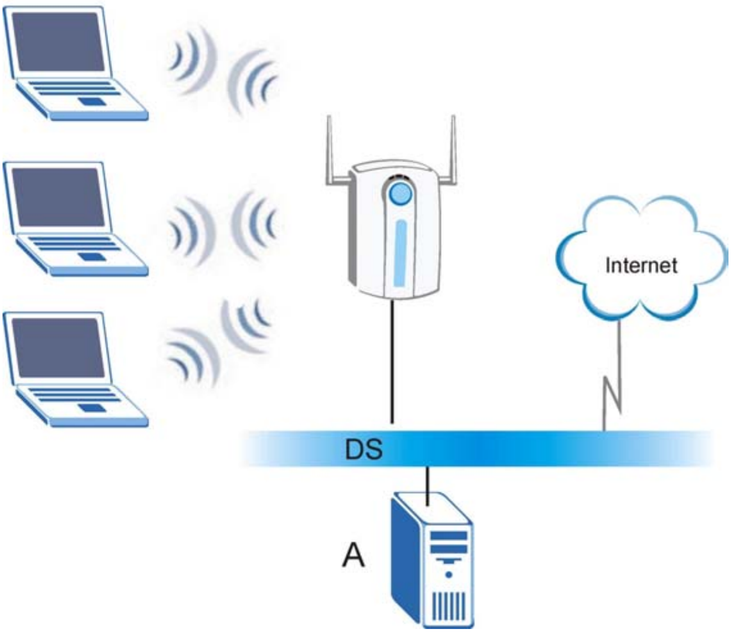
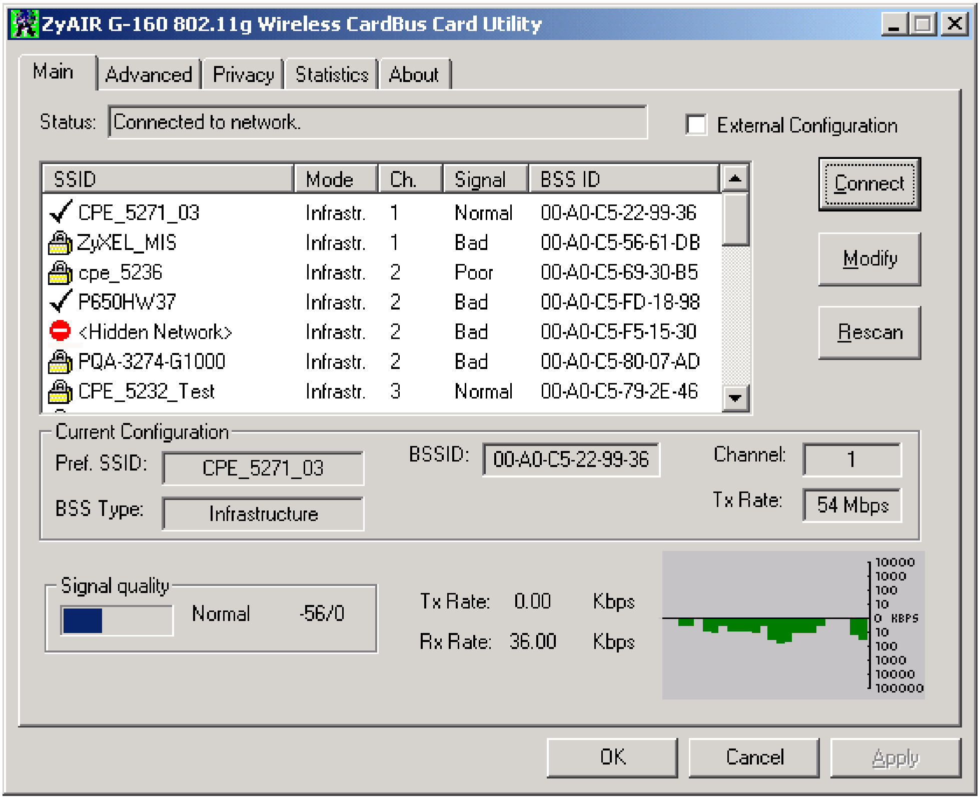


Figure 2-8 WPA with RADIUS Application Example

2.2 The Main Screen

Click the **Main** tab to display the screen as shown next.



Status: Connected to network.

□ External Configuration

SSID	Mode	Ch.	Signal	BSS ID
✓ CPE_5271_03	Infrastr.	1	Normal	00-A0-C5-22-99-36
🔒 ZyXEL_MIS	Infrastr.	1	Bad	00-A0-C5-56-61-DB
🔒 cpe_5236	Infrastr.	2	Poor	00-A0-C5-69-30-B5
✓ P650HW37	Infrastr.	2	Bad	00-A0-C5-FD-18-98
⛔ <Hidden Network>	Infrastr.	2	Bad	00-A0-C5-F5-15-30
🔒 PQA-3274-G1000	Infrastr.	2	Bad	00-A0-C5-80-07-AD
🔒 CPE_5232_Test	Infrastr.	3	Normal	00-A0-C5-79-2E-46

Current Configuration

Pref. SSID: CPE_5271_03

BSS Type: Infrastructure

BSSID: 00-A0-C5-22-99-36

Channel: 1

Tx Rate: 54 Mbps

Signal quality

Normal -56/0

Tx Rate: 0.00 Kbps

Rx Rate: 36.00 Kbps

Figure 2-9 Main

The following table describes the labels in this screen.

Table 2-1 Main

LABEL	DESCRIPTION
Status	This field displays the connection status.
External Configuration	Select this option and click **Apply** if you activate and use another configuration tool (such as the Windows XP Zero Configuration tool) to configure the ZyAIR. You cannot use the ZyAIR Utility to configure the ZyAIR. Clear this checkbox and click **Apply** if you wish to use the ZyAIR Utility to configure the ZyAIR. Other configuration utility will not be able to configure the ZyAIR.

Table 2-1 Main

LABEL	DESCRIPTION
SSID	This field displays the SSID (or name) of each wireless device. ✓ Indicates that the wireless network does not require security setting to access it. 🔒 indicates that the wireless security is activated on this network. ⛔ indicates a hidden network. You must know this network's SSID to access it.
Mode	This field displays the wireless network type (**Infrastr.** or **Ad Hoc**) of the wireless device. **Infrastr.** denotes the infrastructure mode.
Ch.	This field displays the channel number used by each wireless device.
Signal	This field displays the signal strength (**Best**, **Good**, **Normal**, **Poor** or **Bad**) of each wireless device.
BSS ID	This field displays the MAC address of the wireless device.
Connect	Click **Connect** to associate to the selected wireless device.
Modify	Click **Modify** to change the settings of the current connection or create a new profile. Refer to *section 2.2.1*.
Rescan	Click **Rescan** to scan for available wireless device(s) within transmission range.
Current Configuration	
Pref. SSID	This field displays the name of the wireless device to which the ZyAIR is connected.
BSS Type	This field displays the network type of the wireless device to which the ZyAIR is connected.
BSSID	This field displays the MAC address of the wireless device to which the ZyAIR is connected.
Channel	This field displays the radio channel the ZyAIR is currently using.
Tx Rate	This field displays the current transmission rate of the ZyAIR in megabits per second.
Signal Quality	The status bar, signal quality level and the value in dB (from -82 to -10, -82 is the worst) show the quality of the signal.
TX Rate	This field displays the number of data frames transmitted in Kbps.
RX Rate	This field displays the number of data frames received in Kbps.

2.2.1 Connecting to a Network

Follow the steps below to connect to a network using the **Main** screen.

Step 1. Click **Rescan** to scan for all available wireless networks within range.

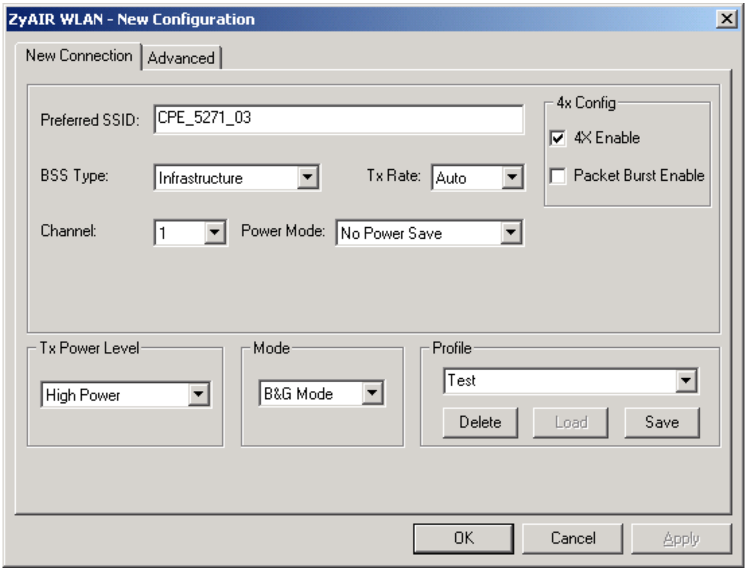
Step 2. To join a wireless network, either click an entry in the table to select a wireless network and then click **Connect** or double-click an entry.

Step 3. If the ZyAIR and the selected wireless network don't use the same security settings, the ZyAIR automatically connect to an accessible network. Refer to *Section 2.4* for more information.

Step 4. Verify that you have successfully connected to the selected network and check the network information on the bottom of the **Main** screen.

2.2.2 The New Connection screen

In the **Main** screen, click **Modify** to display the pop-up screen as shown.



Preferred SSID: CPE_5271_03

BSS Type: Infrastructure

Tx Rate: Auto

Channel: 1

Power Mode: No Power Save

4x Config

☑ 4X Enable

□ Packet Burst Enable

Tx Power Level: High Power

Mode: B&G Mode

Profile: Test

Figure 2-10 Main: New Connection

The following table describes the labels in this screen.

Table 2-2 Main: New Connection

LABEL	DESCRIPTION
Preferred SSID	Enter the SSID (Service Set IDentifier) of the AP or the peer ad-hoc computer-to which you want to associate. To associate to an ad-hoc network, you must enter the same SSID as the peer ad-hoc computer. Leave this field blank to associate to or roam between any infrastructure wireless networks.

Table 2-2 Main: New Connection

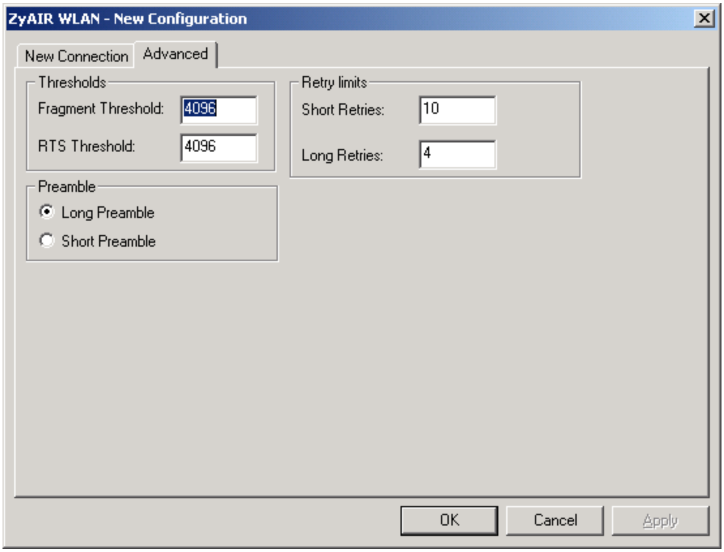
LABEL	DESCRIPTION
BSS Type	Select **Infrastructure** or **802.11 Ad-Hoc** from the drop-down list box. Select **Infrastructure** to associate to an AP. Select **802.11 Ad-Hoc** to associate to a peer ad-hoc computer. Refer to *Section 2.1.4* for more information.
Tx Rate	Select a transmission rate from the drop-down list box. Choose from **Auto** (default), **1Mbps**, **2Mbps**, **5.5Mbps**, **6Mbps**, **9Mbps**, **11Mbps**, **12Mbps**, **18Mbps**, **22Mbps**, **24Mbps**, **36Mbps**, **48Mbps** and **54Mbps**. The transmission rate varies depending the BSS type and the wireless standard you selected.
Channel	Select the channel number from the drop-down list box. To associate to a peer ad-hoc computer, you must use the same channel as the peer ad-hoc computer.
Power Mode	Select **Max Power Save** to reduce power consumption (especially for laptop computers). This turns off the receiver and transmitter on the ZyAIR when it is not transmitting data. Otherwise, select **No Power Save**. **This only works if the wireless device to which the ZyAIR is connected also supports this feature.**
4x Config **4x** is a proprietary technology used to improve throughput in IEEE 802.11 WLAN networks.	
4x Enable	Select this check box to enable **4x**. To use **4x**, you must have this feature and activate it on both the AP and the wireless stations or every peer device in Ad-Hoc mode.
Packet Burst Enable	Select this check box to enable packet bursting. Enable packet bursting to increase the number of data frame transmitted during a transmission period by reducing the interframe space period during which no other WLAN device can transmit data.
Tx Power Level	Select the power level of data transmission from the drop-down list box. Options are **High Power**, **Medium-High Power**, **Medium-Power**, **Medium-Low Power** and **Low Power**.

Table 2-2 Main: New Connection

LABEL	DESCRIPTION
Mode	From the drop-sown list, select the wireless standard (802.11b or 802.11g) of the wireless device. Select **B-Only Mode** to allow the ZyAIR to associate with only IEEE 802.11b compliant WLAN devices. Select **B-Plus Mode** to allow the ZyAIR to associate with IEEE 802.11b compliant WLAN devices or the device with proprietary transmission rate of **22Mbps**. Select **B&G Mode** to allow the ZyAIR to associate with both IEEE 802.11b and IEEE 802.11g compliant WLAN devices. Select **G-Only Mode** to allow the ZyAIR to associate with only IEEE 802.11g compliant WLAN devices.
Profile	This field displays the name of a predefined profile. To use a previously saved network profile, select the profile file name from the drop-down list box. Once you activate a profile, the ZyAIR Utility will use that profile the next time it is started. If you do not activate a profile, the ZyAIR Utility reverts to use the default profile.
Delete	Select a profile from the drop-down list box and click **Delete** to remove the selected profile.
Load	Select an existing profile from the drop-down list box and click **Load** to activate this profile.
Save	Accept the automatically generated name or enter a descriptive name in the **Profile** field and click **Save** to save the current configuration settings in this screen.

2.2.3 The Advanced Screen

In the **Main** screen, click **Modify** and the **Advanced** tab to display the pop-up screen as shown.



Thresholds

Fragment Threshold: 4096

RTS Threshold: 4096

Retry limits

Short Retries: 10

Long Retries: 4

Preamble

● Long Preamble

○ Short Preamble

Figure 2-11 Main: Advanced

The following table describes the labels in this screen.

Table 2-3 Main: Advanced

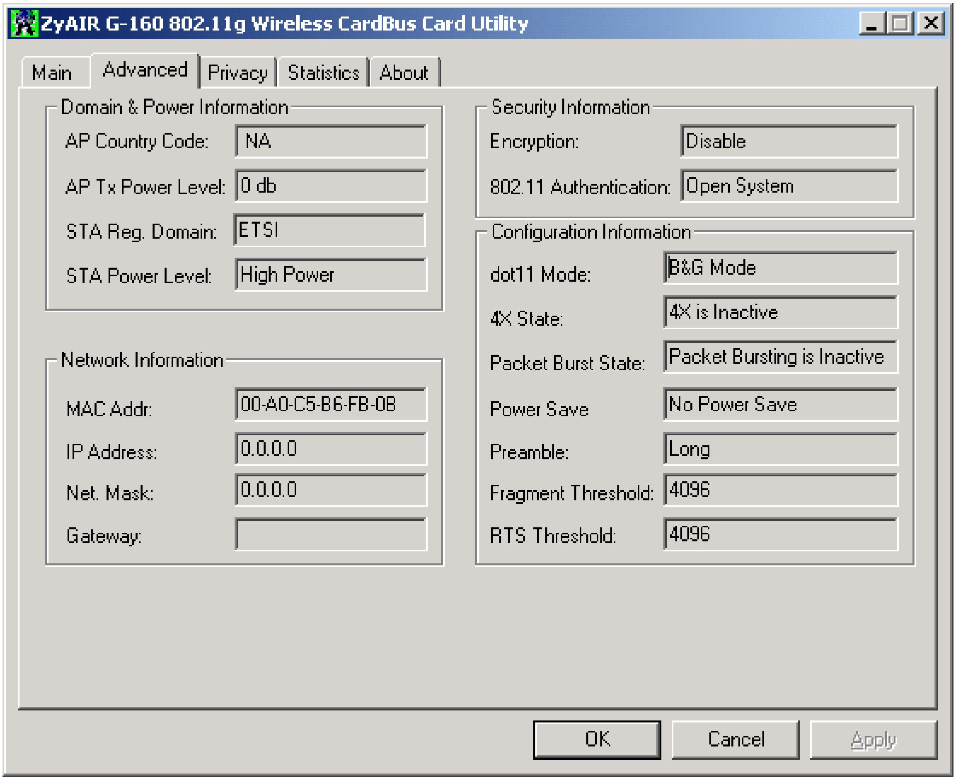
LABEL	DESCRIPTION
Thresholds	
Fragment Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number from 256 to 4096.
RTS Threshold	Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. This value must be greater than 0.
Retry Limits	
Short Retries	Enter the number of times the ZyAIR may attempt to send the data packets without RTS frame.
Long Retries	Enter the number of times the ZyAIR may attempt to send the data packets with RTS frame.

Table 2-3 Main: Advanced

LABEL	DESCRIPTION
Preamble	Use the radio button to select the preamble type. Refer to *Section 2.1.11* for more information.

2.3 The Advanced Screen

Click the **Advanced** tab to display the read-only screen as shown next.



ZyAIR G-160 802.11g Wireless CardBus Card Utility

Domain & Power Information

AP Country Code: NA

AP Tx Power Level: 0 db

STA Reg. Domain: ETSI

STA Power Level: High Power

Network Information

MAC Addr: 00-A0-C5-B6-FB-0B

IP Address: 0.0.0.0

Net. Mask: 0.0.0.0

Gateway:

Security Information

Encryption: Disable

802.11 Authentication: Open System

Configuration Information

dot11 Mode: B&G Mode

4X State: 4X is Inactive

Packet Burst State: Packet Bursting is Inactive

Power Save: No Power Save

Preamble: Long

Fragment Threshold: 4096

RTS Threshold: 4096

Figure 2-12 Advanced

The following table describes the labels in this screen.

Table 2-4 Advanced

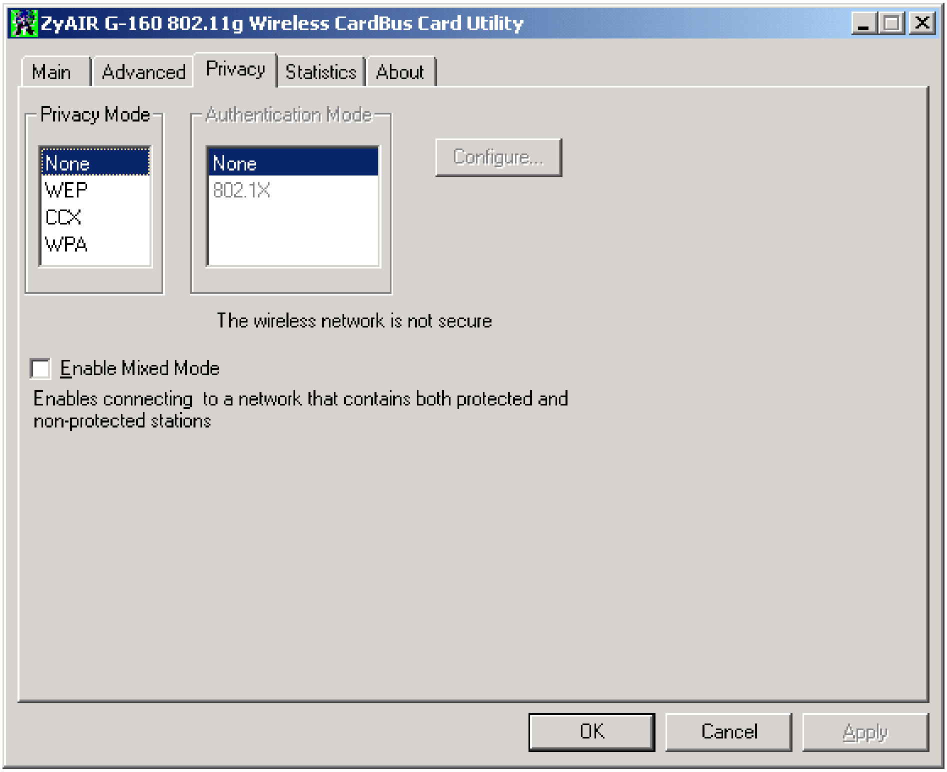
LABEL	DESCRIPTION
Domain & Power Information	
AP Country Code	This field displays the AP's country code of up to three characters.
AP Tx Power Level	This field displays the current transmission power in db (decibel).
STA Reg. Domain	This field displays the ZyAIR's regional code. For 2.4 GHz networks, this field displays **FCC** (North America), **ETSI** (Europe), **MKK** (Japan) or **Unknown**.
STA Power Level	This field displays the power level of data transmission on the ZyAIR.
Network Information	
MAC Addr	This field displays the MAC address of the ZyAIR.
IP Address	This field displays the IP address of the ZyAIR.
Net. Mask	This field displays the subnet mask of the ZyAIR.
Gateway	This field displays the gateway IP address of the ZyAIR.
Security Information	
Encryption	This field shows whether WEP encryption is activated or not.
802.11 Authentication	This field displays the authentication mode.
Configuration Information	
dot11 Mode	This field displays the IEEE 802.11 operating mode.
4X State	This field shows whether or not 4x is enabled.
Packet Burst State	This field shows whether or not packet bursting is activated.
Power Save	This field shows whether or not power saving is activated.
Preamble	This field displays the preamble type.
Fragment Threshold	This field displays the fragment threshold.
RTS Threshold	This field displays the RTS threshold.

2.4 The Privacy Screen

Click the **Privacy** tab to display the screen as shown next.

The screen varies depending on what you select in the **Privacy Mode** and the **Authentication Mode** field.

You see the next screen when you select **None** in the **Privacy Mode** field.



The wireless network is not secure

□ Enable Mixed Mode

Enables connecting to a network that contains both protected and non-protected stations

Figure 2-13 Privacy

The following table describes the labels in this screen.

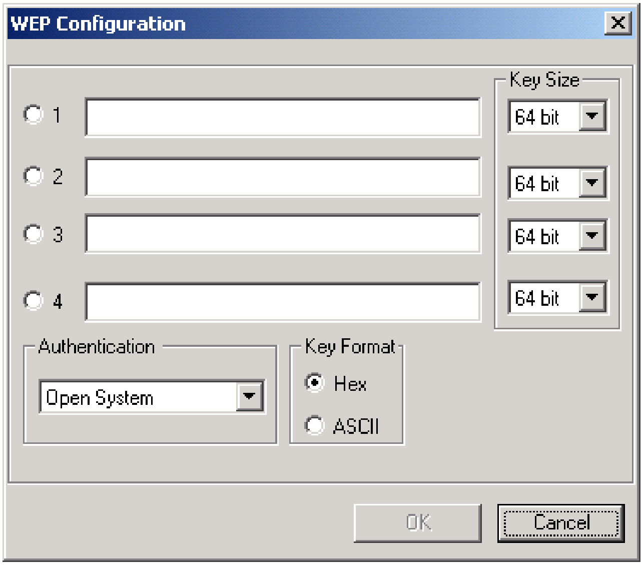
Table 2-5 Privacy

LABEL	DESCRIPTION
Privacy Mode	Select **None** to have no wireless LAN security configured. Select **WEP** to enable WEP data encryption. Select **CCX** (Cisco Compatible Extensions) to allow for instant communication with Cisco networks. Select **WPA** to configure Wi-Fi Protected Access settings.
Authentication Mode	Select **None** to configure WEP keys or a pre-shared key. Select **802.1X** to configure 802.1x authentication.
Configure…	Click this button to display the next screen.
Enable Mixed Mode	This field is not available when you select **WPA** in the **Privacy Mode** field or **802.1X** in the **Authentication Mode** field. Select the check box to have the ZyAIR connect to a network containing both protected and non-protected wireless stations.

2.4.1 WEP Configuration

The WEP keys are used to encrypt communication before it is transmitted. The values for the keys must be set up exactly the same on the APs or other peer ad-hoc wireless computers as they are on the ZyAIR.

In the **Privacy** screen, select **WEP** or **CCX** in the **Privacy Mode** field, set **Authentication Mode** to **None** and click **Configure** to display the **WEP Configuration** screen as shown next.



Authentication: Open System

Key Format: ● Hex ○ ASCII

Figure 2-14 WEP Configuration

The following table describes the labels in this screen.

Table 2-6 WEP Configuration

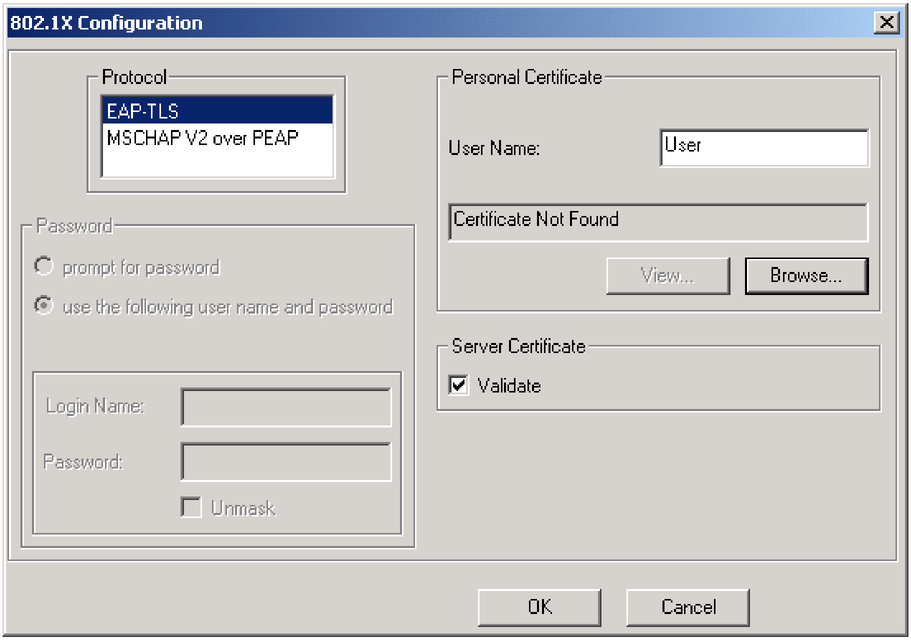
LABEL	DESCRIPTION
1 - 4	Select a WEP key to use for data encryption. Enter the WEP keys in the fields provided. If you select **64 bit** in the **Key Size** field. • Enter either 10 hexadecimal characters in the range of “A-F”, “a-f” and “0-9” (e.g. 11AA22BB33) for hexadecimal key type or • Enter 5 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (e.g. MyKey) for ASCII key type. If you select **128 bit** in the **Key Size** field, • Enter either 26 hexadecimal characters in the range of “A-F”, “a-f” and “0-9” (for example, 00112233445566778899AABBCC) for hexadecimal key type or • Enter 13 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for ASCII key type. If you select **256 bit** in the **Key Size** field, • Enter either 58 hexadecimal characters in the range of “A-F”, “a-f” and “0-9” (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for hexadecimal key type or • Enter 29 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey11112222333344445555678) for ASCII key type. **The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN.** **ASCII WEP key is case sensitive.**
Key Size	Select **64 bit**, **128 bit** or **256 bit** from the drop-down list box to activate WEP encryption and then fill in the related fields.
Authentication	Select an option from the drop-down list box to authenticate the access point. Refer to *Section 2.1.10* for more information.

Table 2-6 WEP Configuration

LABEL	DESCRIPTION
Key Format	Select **Hex** to enter the WEP keys as hexadecimal characters. Select **ASCII** to enter WEP keys as ASCII characters.
OK	Click **OK** to save the changes and close the screen.
Cancel	Click **Cancel** to leave this screen without saving.

2.4.2 802.1x Configuration

In the **Privacy** screen, select **WEP**, **CCX** or **WPA** in the **Privacy Mode** field, set authentication method to **802.1X** and click **Configure** to display the **802.1X Configuration** screen as shown next.



802.1X Configuration

Protocol: EAP-TLS (selected), MSCHAP V2 over PEAP

Password: ○ prompt for password ● use the following user name and password

Login Name:

Password:

□ Unmask

Personal Certificate

User Name: User

Certificate Not Found

Server Certificate

☑ Validate

Figure 2-15 802.1X Configuration

The following table describes the labels in this screen.

Table 2-7 802.1X Configuration

LABEL	DESCRIPTION
Protocol	Select an authentication protocol (**EAP-TLS**, **MSCHAP V2 over PEAP** or **LEAP**) in the text box. The options vary based on what you select in the **Privacy Mode** field in the **Privacy** screen.
Password	This field is only available when you select **MSCHAP V2 over PEAP** or **LEAP** in the **Protocol** field. If you want the ZyAIR Utility to prompt you to enter the password each time the ZyAIR tries to connect to a network, select **prompt for password**. If you want to enter the password now, select **use the following user name and password** and configure the following fields.
Login Name	Enter a user name. This is the user name that you or an administrator set up on the RADIUS server.
Password	Enter the password associated with the user name above.
Unmask	Note that as you type a passphrase, the screen displays an asterisk (*) for each character you type. Select this check box if you want to view the passphrase you entered.
Personal Certificate	This field is only available when you select **EAP-TLS** in the **Protocol** field. **You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.**
User Name	Enter the user name that is assigned to the certificate.
View	Click **View** to check the certificate information of the selected certificate.
Browse	Click **Browse** to display the **Select Certificate** screen. Select a certificate and click **OK** or click **View** to check the certificate information of the selected certificate.
Server Certificate	This field is only available when you select **EAP-TLS** in the **Protocol** field.
Validate	Select the check box to check the certificate of the authentication server.
OK	Click **OK** to save the changes and close the screen.
Cancel	Click **Cancel** to leave this screen without saving.

2.4.3 WPA-PSK Configuration

In the **Privacy** screen, select **WPA** in the **Privacy Mode** field, select **None** in the **Authentication Mode** field and click **Configure** to display the **PSK Configuration** screen as shown next.

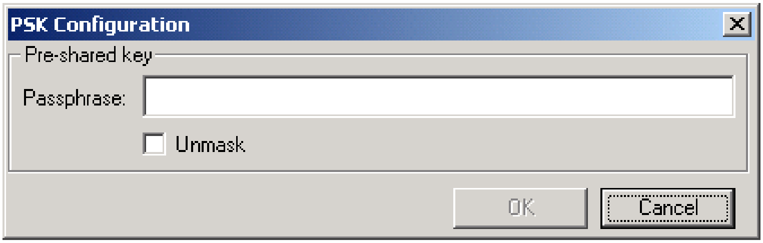


Figure 2-16 PSK Configuration

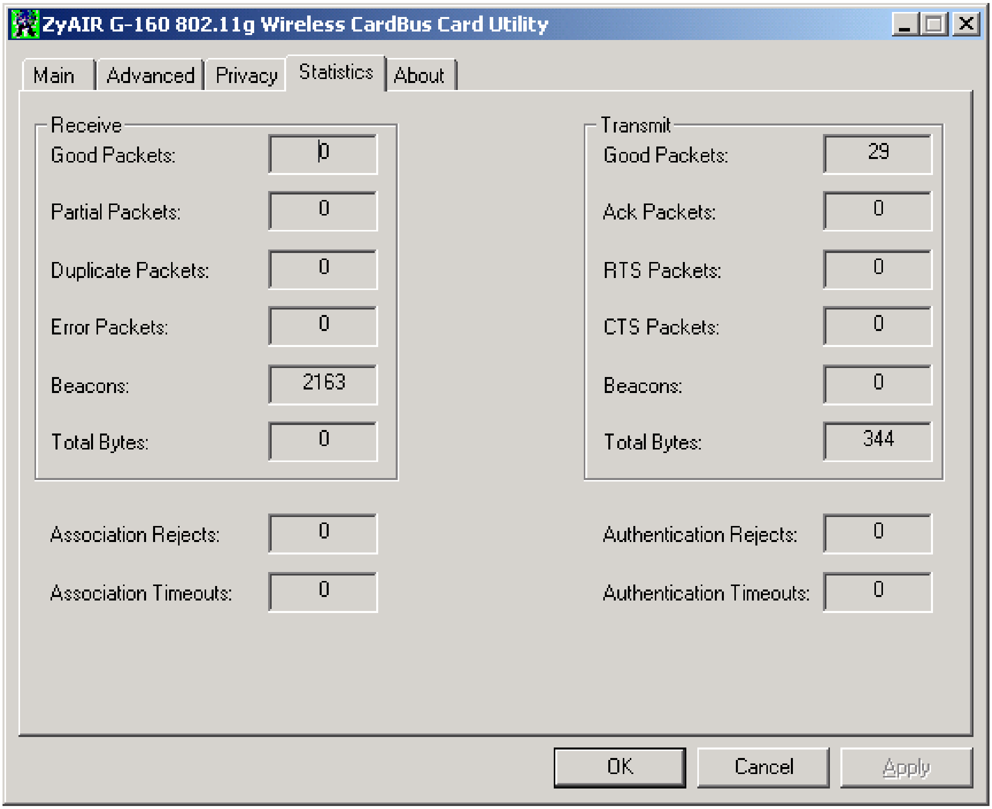
The following table describes the labels in this screen.

Table 2-8 PSK Configuration

LABEL	DESCRIPTION
Pre-shared key	
Passphrase	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. A "password phrase" is called a passphrase. Type a passphrase from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Unmask	Note that as you type a passphrase, the screen displays an asterisk (*) for each character you type. Select this check box if you want to view the passphrase you entered.
OK	Click **OK** to save the changes and close the screen.
Cancel	Click **Cancel** to leave this screen without saving.

2.5 The Statistics Screen

Use the **Statistics** screen to view the read-only information of packet specific statistics.



Receive

Good Packets: 0

Partial Packets: 0

Duplicate Packets: 0

Error Packets: 0

Beacons: 2163

Total Bytes: 0

Transmit

Good Packets: 29

Ack Packets: 0

RTS Packets: 0

CTS Packets: 0

Beacons: 0

Total Bytes: 344

Association Rejects: 0

Association Timeouts: 0

Authentication Rejects: 0

Authentication Timeouts: 0

Figure 2-17 Statistics

The following table describes the labels in the table.

Table 2-9 Statistics

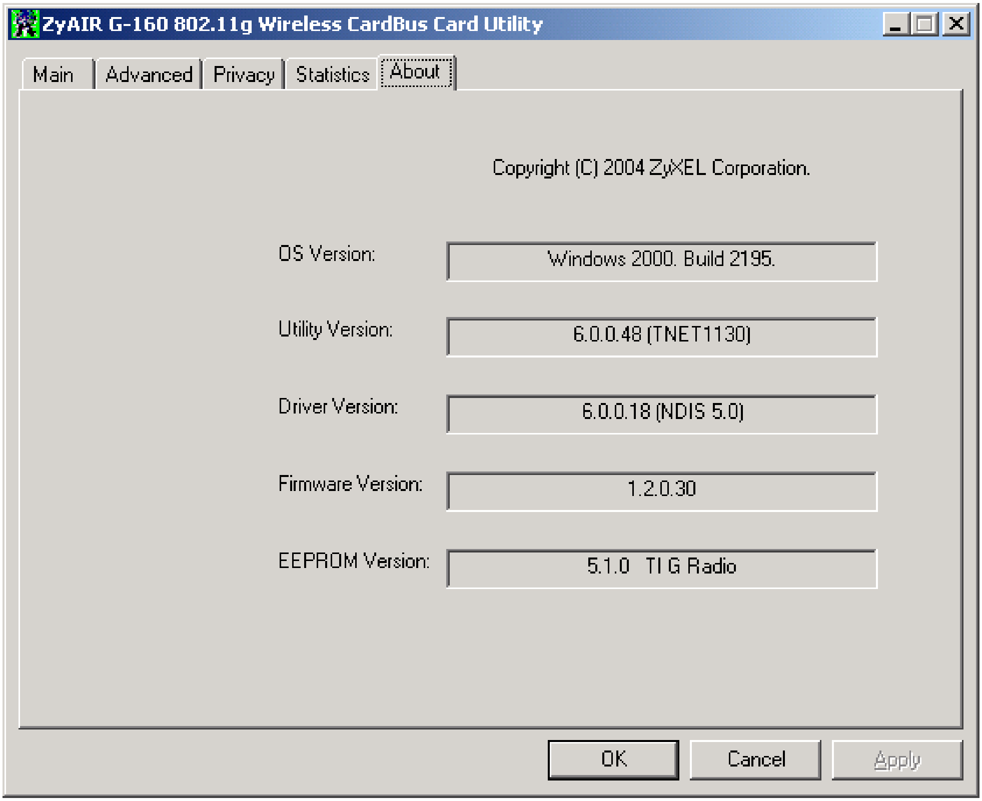
LABEL	DESCRIPTION
Receive	
Good Packets	This is the total number of packets that the ZyAIR receives without errors.
Partial Packets	This is the total number of partial packets that the ZyAIR receives.
Duplicate Packets	This is the total number of the same duplicate packets that the ZyAIR receives.

Table 2-9 Statistics

LABEL	DESCRIPTION
Error Packets	This is the total number of packets that the ZyAIR receives with errors.
Beacons	This is the total number of beacons that the ZyAIR receives from other WLAN devices for probing.
Total Bytes	This is the total number of bytes that the ZyAIR receives.
Transmit	
Good Packets	This is the total number of packets that the ZyAIR sends out without errors.
Ack Packets	This is the total number of packets that the ZyAIR sends out for acknowledge.
RTS Packets	This is the total number of RTS packets.
CTS Packets	This is the total number of CTS packets.
Beacons	This is the total number of beacons that the ZyAIR sends out for probing.
Total Bytes	This is the total number of bytes that the ZyAIR sends out.
Association Rejects	This is the total number of association rejections.
Association Timeouts	This is the total number of association request that have timed out.
Authentication Rejects	This is the total number of authentication request failed.
Authentication Timeouts	This is the total number authentication request that have timed out.

2.6 The About Screen

The **About** screen displays related version numbers of the ZyAIR.



Copyright (C) 2004 ZyXEL Corporation.

OS Version: Windows 2000. Build 2195.

Utility Version: 6.0.0.48 (TNET1130)

Driver Version: 6.0.0.18 (NDIS 5.0)

Firmware Version: 1.2.0.30

EEPROM Version: 5.1.0 TI G Radio

Figure 2-18 About

The following table describes the read-only fields in this screen.

Table 2-10 About

FIELD	DESCRIPTION
Utility Version	This field displays the version number and release date of the ZyAIR Utility.
Network Driver Version	This field displays the version number and release date of the Windows driver for the ZyAIR.
Firmware Version	This field displays the firmware version of the ZyAIR.
EEPROM Version	This field displays the EEPROM (Electrically Erasable Programmable Read-only Memory) version of the ZyAIR.

Chapter 3
Maintenance

This chapter describes how to uninstall or upgrade the ZyAIR Utility.

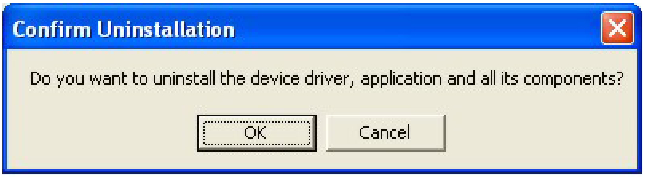
3.1 Removing the ZyAIR Utility

Follow the steps below to remove (or uninstall) the ZyAIR Utility from your computer.

Step 1. Close and exit the ZyAIR Utility.

Step 2. Click **Start**, **(all) Programs**, **IEEE802.11g Wireless LAN Utility**, **Uninstall ZyAIR G-160 802.11g Wireless CardBus Card Utility**.

Step 3. When prompted, click **OK** to remove the driver and the utility software.



Confirm Uninstallation

Do you want to uninstall the device driver, application and all its components?

Figure 3-1 Confirm Uninstallation

Step 4. Click **Finish** and restart the computer when prompted.

3.2 Upgrading the ZyAIR Utility

To perform the upgrade, follow the steps below.

Step 1. Download the latest version of the utility from the ZyXEL web site and save the file on your computer.

Step 2. Follow the steps in *Section 3.1* to remove the current ZyAIR Utility from your computer.

Step 3. Restart the computer when prompted.

Step 4. After restarting, refer to the procedure in the *Quick Installation Guide* to install the new utility software.

Step 5. Check the version numbers in the **About** screen to make sure the new utility is installed properly.

Chapter 4
Troubleshooting

This chapter covers potential problems and the possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

4.1 Problems Starting the ZyAIR Utility Program

Table 4-1 Troubleshooting Starting ZyAIR Utility Program

Cannot start the ZyAIR Wireless LAN Utility	Make sure the ZyAIR is properly inserted and the LED is on. Refer to the *Quick Installation Guide* for the LED descriptions.
	Use the **Device Manager** to check for possible hardware conflicts. Click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and **Device Manager**. Verify the status of the ZyAIR under **Network Adapter**. (Steps may vary depending on the version of Windows).
	Install the ZyAIR in another computer.
	If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.

4.2 Problems Communicating With Other Computers

Table 4-2 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The ZyAIR computer cannot communicate with the other computer.	Make sure you are connected to the wireless network.
A. Infrastructure	Make sure that the AP and the associated computers are turned on and working properly. Make sure the ZyAIR and the associated AP use the same SSID. Configure the AP to use another radio channel if interference is high. Make sure that the computer and the AP share the same wireless security settings. Verify the settings in the **Privacy** screens.

Table 4-2 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
B. Ad-Hoc	Verify that the peer computer(s) is turned on. Make sure the ZyAIR and the peer computer(s) are using the same SSID and channel. Use another radio channel if interference is high. Make sure that the computer and the AP share the same wireless security settings. Verify the settings in the **Privacy** screens.

4.3 Problem with the Link Status

Table 4-3 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	Search and connect to another WLAN device with a better link quality using the **Main** screen. Move your computer closer to the AP or the peer computer(s) within the transmission range. There is too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.

Appendix A Product Specifications

Product Specifications

Product Name	ZyAIR G-160 802.11g Wireless Cardbus Card
Interface	32-bit Cardbus, Type II PCMCIA Card
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Frequencies	2.412-2.483GHz
Operating Channels	IEEE 802.11b: 11 Channels (North America) IEEE 802.11g: 11 Channels (North America) IEEE 802.11b: 13 Channels (Europe) IEEE 802.11g: 13 Channels (Europe)
Data Rate	IEEE 802.11b: 22, 11, 5.5, 2, 1Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps Proprietary: 100 Mbps (4x) for G standard, 22 Mbps for B standard
Modulation	IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK) IEEE 802311b: Direct Spread Spectrum (CCK, DQPSK, DBOSK).
Security	64/128/256 bit WEP, WPA, WPA-PSK, 802.1x
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 60 degrees Centigrade
Operating Humidity	20 ~ 95% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Power Consumption (maximum)	IEEE802.11b: TX: 500mA RX: 450mA IEEE802.11g: TX: 650mA RX: 450mA
Voltage	3.3V±5%
Weight	<50g

Product Specifications

Dimension	117.6mm(L)*54.1mm(W)*7mm(H)

Appendix B
Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**. The type of authentication you use depends on the RADIUS server. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of five authentication types.

Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

Index