ZyAIR G-100

802.11g Wireless CardBus Card

User's Guide

Version 1.1
November 2004

ZyXEL
Unleash Networking Power

Copyright

Copyright ©2004 by ZyXEL Communications Corporation

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

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 your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

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.

Caution

1. The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d) (2).
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.
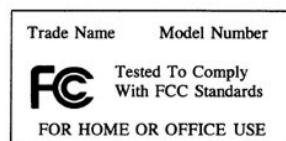
Customer Support

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 1°, 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
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

●

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on the purchase of your new ZyAIR G-100 802.11g Wireless CardBus Card!

About This User's Guide

This guide provides information about the ZyAIR G-100 802.11g Wireless CardBus 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-100 802.11g Wireless CardBus Card is referred to as the ZyAIR in this guide.

- The ZyAIR G-100 802.11g Wireless CardBus 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 ZyAIR Hardware and Utility Installation

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

1.2 Disable Windows XP Wireless LAN Configuration Tool

Windows XP includes a configuration tool 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.

From ZyAIR Utility

Right-click on the ZyAIR Utility system tray icon and click **Turn off zero configuration**.
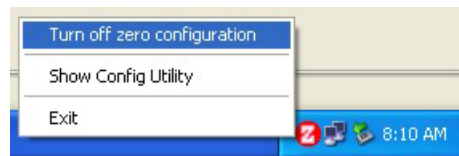
Figure 1-1 Windows XP: System Tray Icon

From the Wireless Network Connection Status Screen

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 1-2 Windows XP: System Tray Icon

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**.

3. Double-click on the icon for wireless network connection to display a status window as shown next.
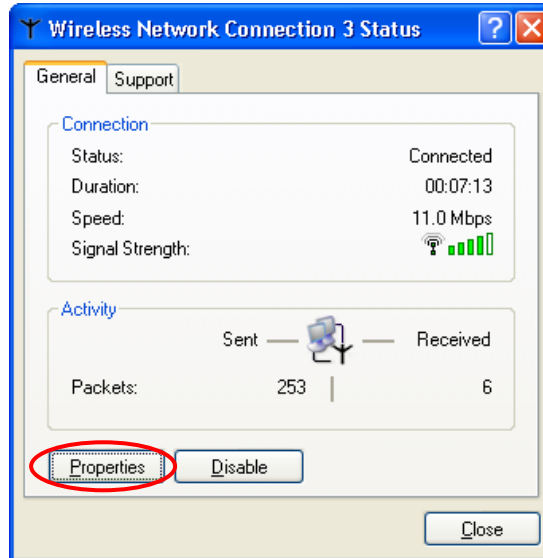
Figure 1-3 Windows XP: Wireless Network Connection Status

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

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

Figure 1-4 Windows XP: Connect to Wireless Network

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**.
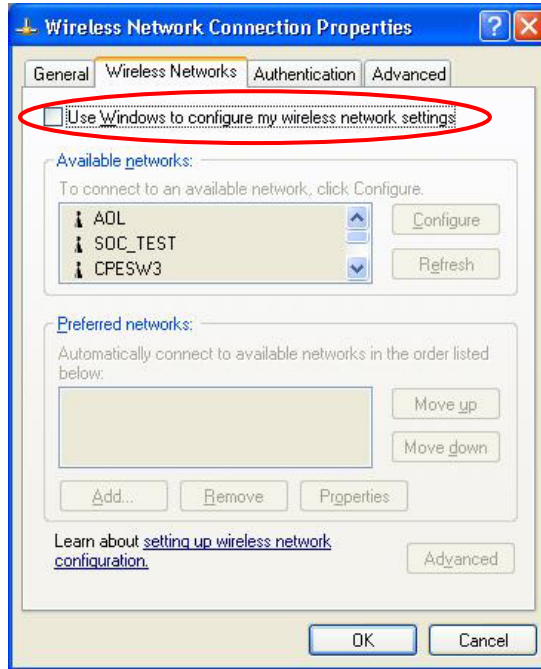
Figure 1-5 Windows XP: Wireless Network Connection Properties

1.3   Accessing the ZyAIR Utility

After you installed the ZyAIR Utility, an icon for the ZyAIR Utility appears in the system tray.

☞ **When the ZyAIR Utility system tray icon displays, the ZyAIR is installed properly.**

Figure 1-6 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 ZyAIR is working properly but is not connected to any AP or wireless station.
Green	The ZyAIR is connected to a wireless network.

Double click on the ZyAIR Utility icon in the system tray to open the ZyAIR Utility.

Chapter 2
Using the ZyAIR Utility

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

2.1 About Your ZyAIR

The ZyAIR is an IEEE 802.11g compliant wireless LAN PC card that fits into any 32-bit CardBus slot. With the ZyAIR, you can enjoy wireless mobility within the coverage area. The IEEE 802.11g technology provides greater range and offers transmission rate at up to 54 Mbps.

The following lists the main features of your ZyAIR.

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

2.2 Benefits of a Wireless LAN

Wireless Local Area Network (WLAN) systems offer a number of advantages over traditional wired systems. WLANs are flexible, easy to set up and manage. They are also more economical than wired LAN systems.

- Access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
- Doctors and nurses can access a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
- It allows flexible workgroups a lower total cost of ownership for networks that are frequently reconfigured.
- Conference room users can access the network as they move from meeting to meeting-accessing up-to-date information that facilitates the ability to communicate decisions "on the fly".
- It provides campus-wide networking coverage, allowing enterprises the roaming capability to set up easy-to-use wireless networks that transparently covers an entire campus.

2.3 Notes on Wireless LAN Setup

When setting up a wireless LAN, be sure to note the following points:

Optimize the performance of the WLAN by ensuring that the distance between access points is not too far. In most buildings, most WLAN adapters operate within a range of 100 ~ 300 feet, depending on the thickness and structure of the walls.

Radio waves can pass through walls and glass but not metal. If there is interference in transmitting through a wall, it may be that the wall has reinforcing metal in its structure. Install another access point to circumvent this problem.

Floors usually have metal girders and metal reinforcing struts that interfere with WLAN transmission.

2.4   About Wireless LAN Network

This section describes the wireless LAN network terms and applications.

2.4.1   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.

2.4.2   Channel

A range of radio frequencies used by IEEE 802.11b wireless devices is called a channel.

2.4.3   Transmission 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.

2.4.4   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 (BSS)**. 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 (IBSS)** (Independent Basic Service Set) mode.

Ad-Hoc (IBSS)

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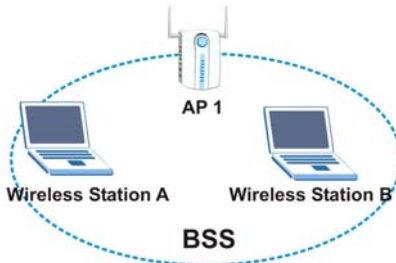

Figure 2-1 Ad-hoc Network Example

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

Infrastructure

When a number of wireless clients 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 clients or devices connected to the wired network. Wireless clients can then access resource, such as the printer, on the wired network.
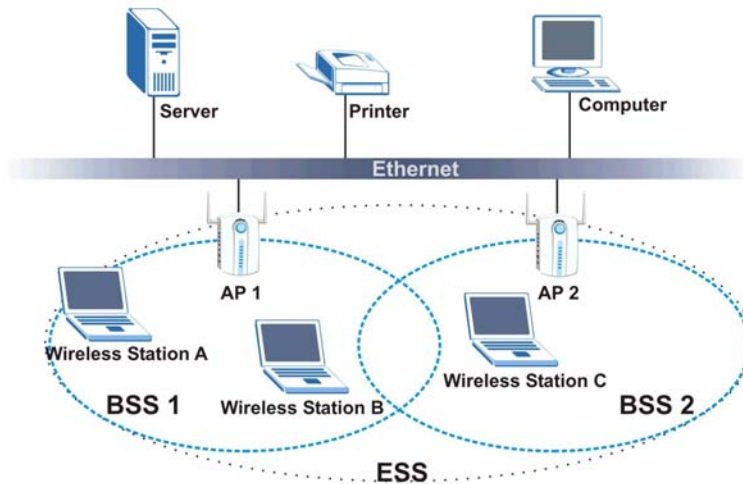
Figure 2-3 Infrastructure Network Example

2.4.5 Roaming

Roaming is where in an infrastructure network, wireless clients are able to switch from one BSS to another as they move between coverage areas. During this period, the wireless client maintains uninterrupted connection to the network. As the wireless client moves from place to place, it scans for the most appropriate AP depending on the signal strength, network utilization or other factors.

The following figure depicts a roaming example. When **Wireless Client B** moves to position **X**, the ZyAIR in **Wireless Client 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

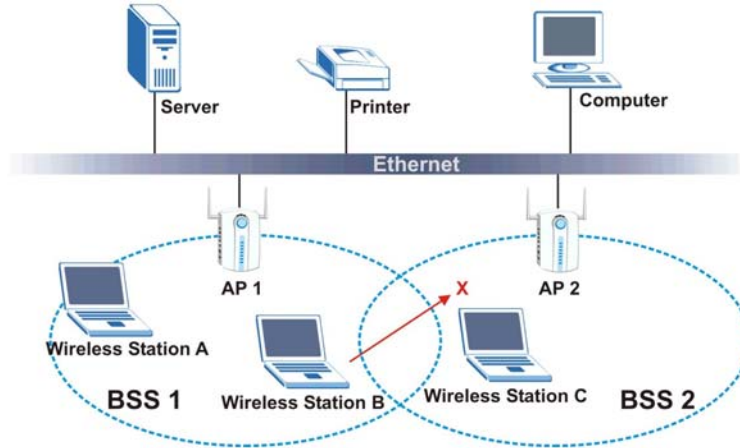## 2.5   ZyAIR Driver and Wireless Utility Installation

Refer to the *Quick Installation Guide* to install the ZyAIR driver and wireless utility program.

2.6   The Link Info Screen

When the ZyAIR Utility starts, the **Link Info** screen displays, showing the current configuration of your ZyAIR.
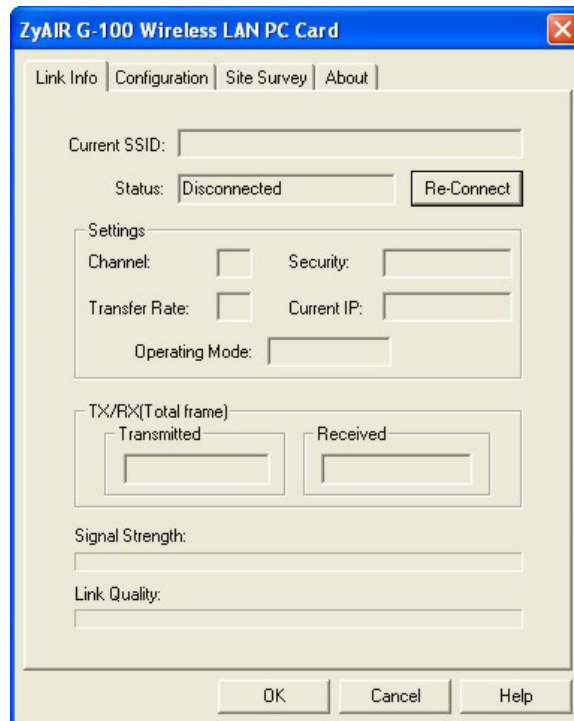

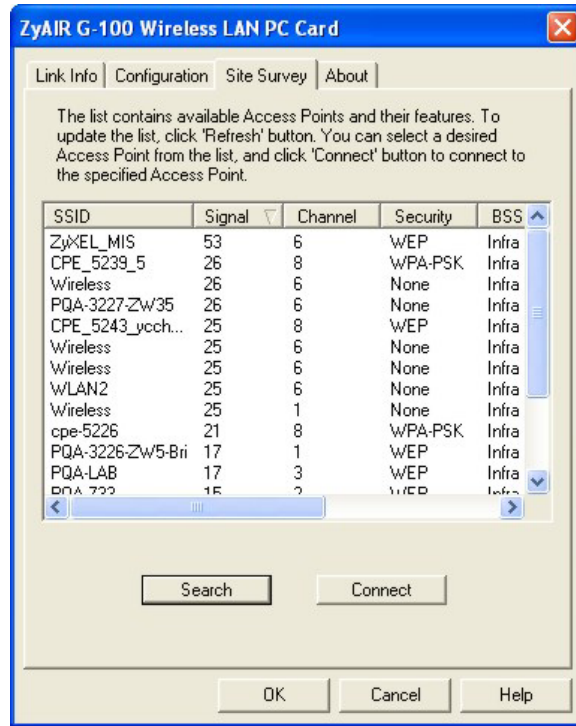**Figure 2-5 ZyAIR Utility: Link Info**

The following table describes the fields in this screen.

Table 2-1 ZyAIR Utility: Link Info

LABEL	DESCRIPTION
Current SSID	This field displays the name of the wireless LAN network to which the ZyAIR is associated.
Status	This field displays the connection status of the ZyAIR. This field is blank if there is no device associated with the ZyAIR.
Re-Connect	Click **Re-Connect** to re-establish the connection to the wireless network whose SSID is shown in the **Current SSID** field.
Channel	This field displays the radio channel the ZyAIR is currently using.
Transfer Rate	This field displays the current transmission rate of the ZyAIR in megabits per second.
Security	This field displays the security level configured as either **None**, **WEP**, **WPA-PSK**, **WPA** or **802.1x** for the wireless device.
Current IP	This field displays your computers IP address.
Operating Mode	This field displays the operating mode of the ZyAIR. **Infrastructure:** the ZyAIR associates to an AP. **Ad-Hoc:** the ZyAIR associates to a peer ad-hoc computer.
TX/RX (Total Frame)	
Transmitted	This field displays the number of data frames transmitted.
Received	This field displays the number of data frames received.
Signal Strength	The status bar and the percentage number or a number in dBm show the strength of the signal.
Link Quality	The status bar and the percentage number show the quality of the signal.
OK	Click **OK** to apply the changes and close the screen.
Cancel	Click **Cancel** to discard all changes and close the screen.
Help	Click **Help** to display on-line help screen.

2.7   The Site Survey Screen

Use the **Site Survey** screen to scan for and connect to a wireless network automatically.

ZyAIR G-100 Wireless LAN PC Card
Link Info
Configuration
Site Survey
About
Search
Connect
OK
Cancel
Help

The list contains available Access Points and their features. To update the list, click 'Refresh' button. You can select a desired Access Point from the list, and click 'Connect' button to connect to the specified Access Point.

SSID	Signal	Channel	Security	BSS
ZyXEL_MIS	53	6	WEP	Infra
CPE_5239_5	26	8	WPA-PSK	Infra
Wireless	26	6	None	Infra
PQA-3227-ZW35	26	6	None	Infra
CPE_5243_ycch...	25	8	WEP	Infra
Wireless	25	6	None	Infra
Wireless	25	6	None	Infra
WLAN2	25	6	None	Infra
Wireless	25	1	None	Infra
cpe-5226	21	8	WPA-PSK	Infra
PQA-3226-ZW5-Bri	17	1	WEP	Infra
PQA-LAB	17	3	WEP	Infra

Figure 2-6 Site Survey

The following table describes the fields in the table.

Table 2-2 Site Survey

FIELD	DESCRIPTION
SSID	This field displays the SSID (or name) of each wireless device.
Signal	This field displays the signal strength of each wireless device.
Channel	This field displays the channel number used by each wireless device.
Security	This field shows whether the wireless security is activated (**WEP**, **WPA-PSK**, **WPA** or **802.1x**) or inactive (**None**).
BSSType	This field displays the wireless network type as **Infrastructure** or **Ad Hoc** of each wireless device. **Infrastructure:** the ZyAIR associates to an AP. **Ad-Hoc:** the ZyAIR associates to a peer ad-hoc computer.
Mode	This field displays the wireless standard (802.11b or 802.11g) of the wireless device.
BSSID	This field displays the MAC address of the wireless device.
Search	Click **Search** to scan for available wireless device within transmission range.
Connect	Click **Connect** to associate to the selected wireless device.
OK	Click **OK** to apply the changes and close the screen.
Cancel	Click **Cancel** to discard all changes and close the screen.
Help	Click **Help** to display on-line help screen.

2.7.1 Connecting to a Wireless Network

Follow the steps below to connect to a network.

1. Click **Search** to scan for all available wireless networks within range.
2. To join a network, either click an entry in the table to select a wireless network and then click **Connect** or double-click an entry.
3. If the **WEP** field is **Yes** for the selected wireless network, you must also set up WEP keys in the **Security Configuration** screen. Refer to *Section 2.10* for more information.
4. To verify that you have successfully connected to the selected network, check the network information in the **Link Info** screen. When you click **Connect**, you are automatically taken to the **Link Info** screen.

2.8 The Configuration Screen

Click **Configuration** in the ZyAIR Utility program to display the **Configuration** screen as shown next.

Figure 2-7 Configuration

The following table describes the labels in this screen.

Table 2-3 Configuration

FIELD	DESCRIPTION
Profile	The **Profile** function allows you to:
	Create a new profile. Enter a descriptive name in the drop-down list box and click **OK** in the **Configuration** screen to save the new profile settings.
	Use one of the pre-configured network profiles.
Remove	To delete an existing wireless network configuration, select a profile from the drop-down list box and click **Remove**.
Activate	To use a previously saved network profile, select the profile file name from the drop-down list box and click **Activate**.

Table 2-3 Configuration

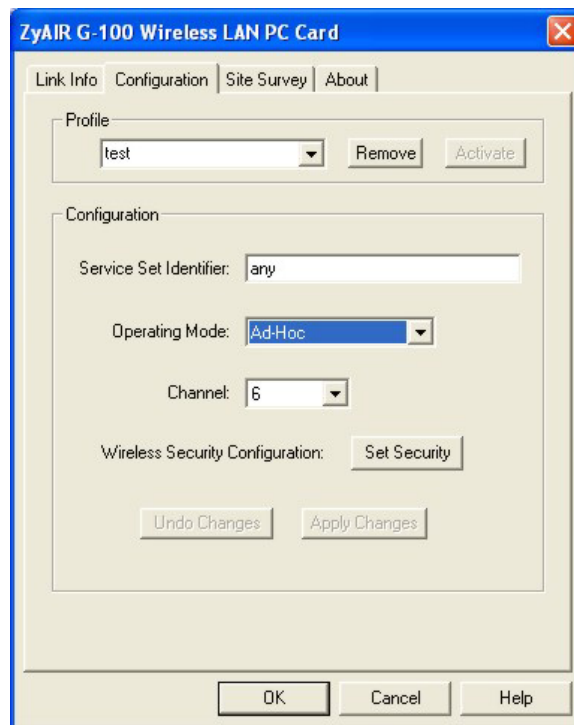| FIELD	DESCRIPTION
Configuration	
Service Set Identifier	Enter the SSID (Service Set Identifier) of the AP or the peer ad-hoc computer to which you want to associate in this field. To associate to an ad-hoc network or a particular AP in an infrastructure network, you must enter the same SSID as the peer ad-hoc computer. Enter **any** to associate to or roam between any infrastructure wireless networks. This is the default setting.
Operating Mode	Select **Infrastructure** or **Ad-Hoc** from the drop-down list box. Select **Infrastructure** to associate to an AP. Select **Ad-Hoc** to associate to a peer ad-hoc computer. Refer to *Section 2.4.4* for more information.
Channel	This field is activated if you select **Ad-Hoc** in the **Operation Mode** field. 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.
Set Security	Click **Set Security** to display the **Security Configuration** screen. Configure your ZyAIR with wireless LAN security in this screen.
Undo Changes	Click **Undo Changes** to start configuring the fields again.
Apply Changes	Click **Apply Changes** to save the changes back to ZyAIR.
Ok	Click **OK** to apply the changes and close the screen.
Cancel	Click **Cancel** to discard all changes and close the screen.
Help	Click **Help** to display on-line help screen.

2.9   Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communication between wireless clients 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
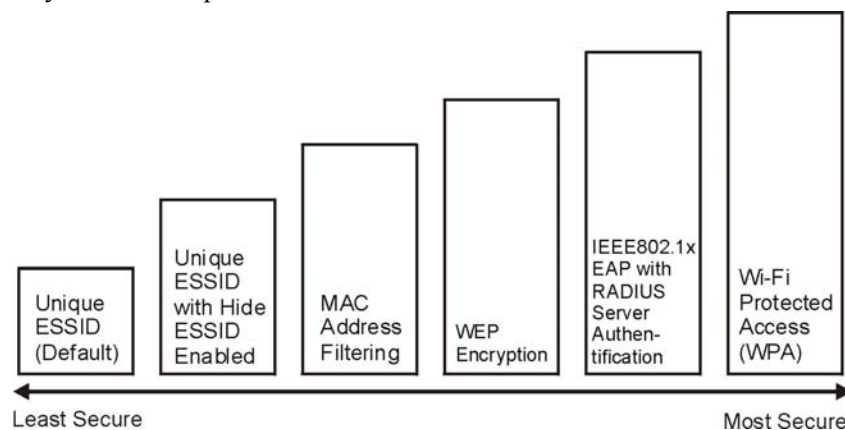
Figure 2-8 ZyAIR Wireless Security Levels

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.

2.10 The Security Configuration Screen

Configure the wireless LAN security by clicking the **Set Security** button in the **Configuration** screen.

There are five data authentication options available from the **Authentication** drop-down list box, when you select **Infrastucture** as the **Operating Mode** in the previous screen:

- ♦ None
- ♦ WEP
- ♦ WPA-PSK
- ♦ WPA
- ♦ 802.1x

There are three data authentication options available from the **Authentication** drop-down list box, when you select **Ad-Hoc** as the **Operating Mode** in the previous screen:

- ♦ None
- ♦ WEP
- ♦ WPA-PSK

2.10.1 Data Encryption with WEP

Select **WEP** from the **Authentication** drop-down list box to view the security configuration options.

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

There are two ways to create WEP keys in your ZyAIR.

- ♦ Automatic WEP key generation based on a "password phrase" called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
- ♦ Enter the WEP keys manually.

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

Authentication Type

Two different methods can be used to authenticate wireless stations to the network: **Open System** and **Shared Key**. The following figure illustrates the steps involved.
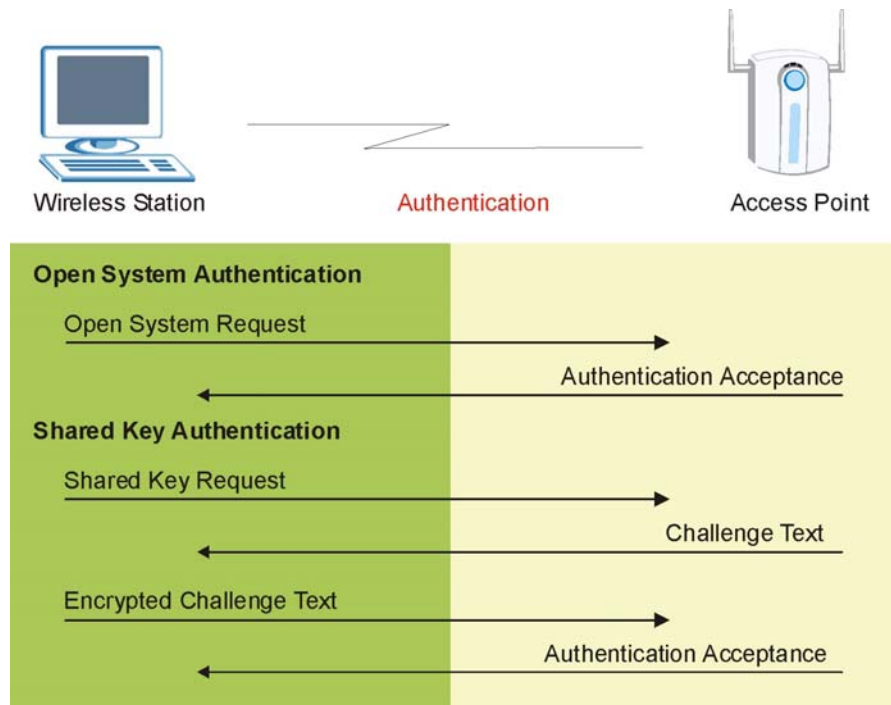
Figure 2-9 WEP Authentication Steps

Open System authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

**Shared Key** authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your ZyAIR's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the ZyAIR will accept either type of authentication request and the ZyAIR will fall back to use open authentication if the shared key does not match.
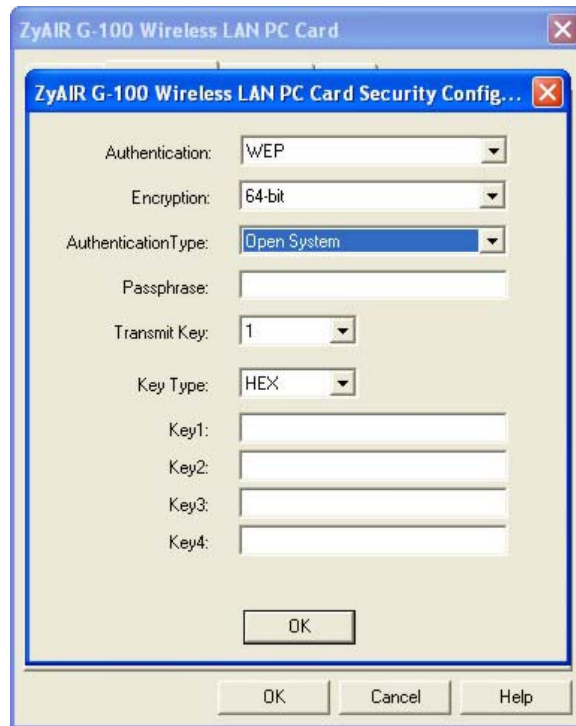
Figure 2-10 WEP Authentication

Follow the instructions in the table to configure the WEP encryptions.

Table 2-4 WEP Authentication

FIELD	DESCRIPTION
Authentication	Select **WEP** from the drop-down list box to activate **WEP Authentication**.
Encryption	Select either **64 Bits** or **128 Bits** from the drop-down list box to activate WEP encryption and then fill in the related fields. Select **Disabled** to deactivate the WEP encryption.
☞	**WEP Key Entry: The WEP keys are used to encrypt communication before transmitting. 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.**
Authentication Type	Select **Open System** or **Shared Key** from the drop-down list box. See the section on **Authentication Type** for further descriptions of these. Select **Open System** to allow any station to gain access to the network. Select **Shared Key** if you want the ZyAIR to automatically generate four different WEP keys based on the passphrase specified in the **Passphrase** field.
Passphrase	Type a Passphrase. As you enter the Passphrase, the ZyAIR automatically generates four different WEP keys and displays them in the key fields below. Write down the automatically generated WEP keys and use them to manually set the WEP keys in other WLAN adapters. Passphrase is case-sensitive. If you select ASCII characters as the Key Type, the Passphrase screen will be grayed out. For more information on Passphrase, see *section 2.10.1.*

Table 2-4 WEP Authentication

FIELD	DESCRIPTION
Transmit Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyAIR and the wireless stations to communicate.
Key Type	Select ASCII to enter the WEP keys as ASCII characters. Select this option if you want to manually enter the WEP keys. Select HEX to have the WEP keys as hexadecimal characters. Select this option if you want the ZyAIR to automatically generate four different WEP keys based on the passphrase specified in the Passphrase field.
Key 1 … 4	Enter the WEP keys in the fields provided. If you select **64 Bits** in the **Encryption (WEP)** field. ◆ Enter either 10 hexadecimal digits 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 Bits** in the **Encryption (WEP)** field, ◆ Enter either 26 hexadecimal digits 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. ☞ **You *must* configure all four WEP keys the first time you use the ZyAIR.** ☞ **ASCII WEP keys are case sensitive.**
OK	Click **OK** to apply the changes and close the screen.

2.10.2 Data Encryption with WPA

Select **WPA** from the **Authentication** drop-down list box to view the security configuration options.

Introduction to 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 clients using an external RADIUS database. See later in this *User's Guide* for more information on IEEE 802.1x and EAP.

WPA-PSK (WPA -Pre-Shared Key), only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client 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 clients. 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.

Figure 2-11 WPA Authentication

Follow the instructions in the table to configure WPA security.

Table 2-5 WPA Authentication

| FIELD	DESCRIPTION
Authentication	Select **WPA** from the drop-down list box.
Encryption Status	All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Authentication** is selected. See the section on Encryption for details about Temporal Key Integrity Protocol (**TKIP**).
EAP Type	Select an **EAP Type** from the drop-down list box. See *Types of EAP Authentication* in the *Appendix* of this *User's Guide* for information on the fields listed below. The choices are: **EAP-TLS** **EAP-TTLS** **EAP-MD5** **EAP-PEAP** **LEAP**
Login Name	If you want all wireless stations to have to enter user names before access to the wired network is allowed, type a Login Name.
Password	If you want all wireless stations to have to enter passwords before access to the wired network is allowed, type a **Password**.
Certificate	This field is only available when you select **EAP-TLS** in the **EAP Type** 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.**
Validate Server Certificate	This field is not available when you select **EAP-MD5** or **LEAP** from the **EAP Type** list. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. Select the check box to have your server validate this certificate.
TTLS Protocol/ PEAP Protocol	Select a protocol from the drop-down list box. The choices are: **EAP-TTLS** PAP CHAP MS CHAP MS CHAP v2 **EAP-PEAP** MD5 Challenge EAP-GTC MS CHAP v2 See the *Types of EAP Authentication* in the appendix for details.
OK	Click **OK** to apply the changes and close the screen.

2.10.3 Data Encryption with WPA-PSK

Select **WPA-PSK** from the **Authentication** drop-down list box to view the security configuration options.

WPA-PSK Application Example

A WPA-PSK application looks as follows.

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

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

3. The AP derives and distributes keys to the wireless clients.

4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.
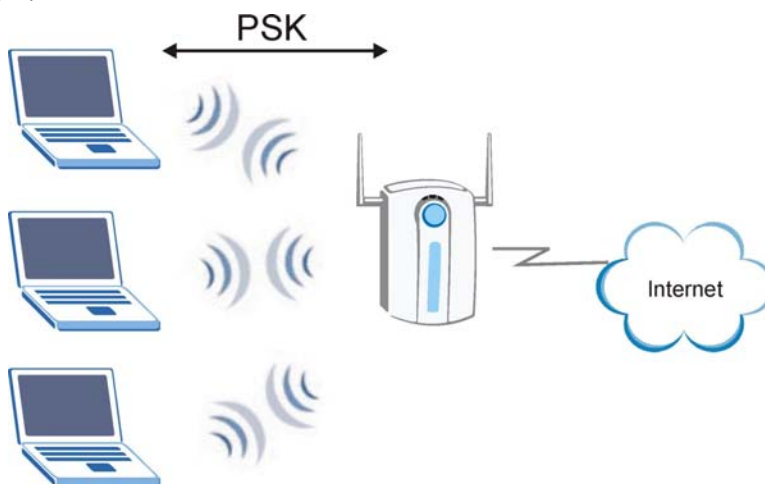
Figure 2-12 WPA - PSK Authentication

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.

1. The AP passes the wireless client's authentication request to the RADIUS server.

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

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 clients.
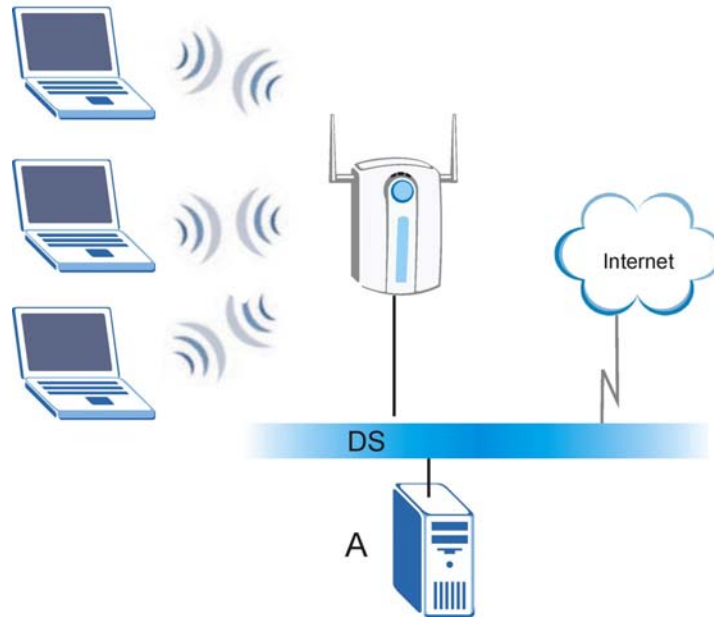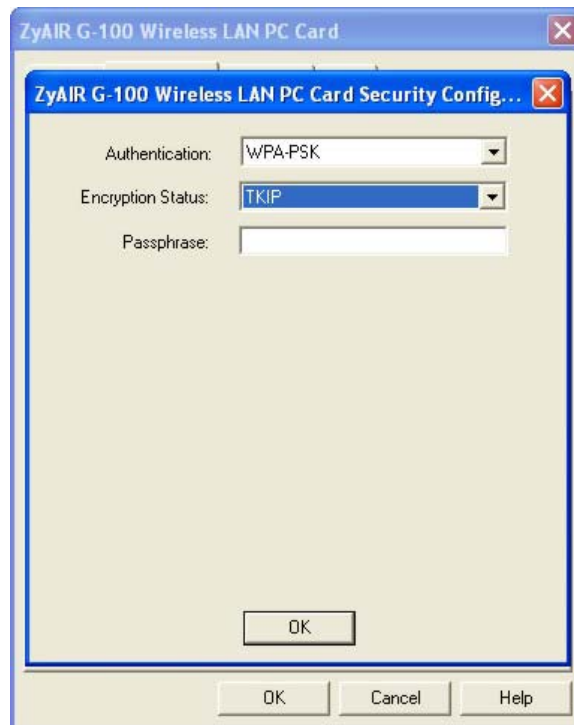
Figure 2-13 WPA with RADIUS Application Example

Figure 2-14 WPA-PSK Authentication

Follow the instructions in the table to configure the WEP encryptions.

Table 2-6 WPA-PSK Authentication

FIELD	DESCRIPTION
Authentication	Select **WPA-PSK** from the drop-down list box.

Table 2-6 WPA-PSK Authentication

FIELD	DESCRIPTION
Encryption Status	All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Authentication** is selected. See the section on Encryption for details about Temporal Key Integrity Protocol (**TKIP**).
Passphrase	Type a Passphrase from 8 to 63 ASCII characters long. The Passphrase is case-sensitive. You must use the same Passphrase for all wireless LAN adapters with this feature in the same WLAN. For more information on Passphrase, see *section 2.10.1.*
OK	Click **OK** to apply the changes and close the screen.

2.10.4 Data Encryption with 802.1x

Select **802.1x** from the **Authentication** drop-down list box to view the security configuration options.

802.1x Overview

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 for an unlimited number of users.

EAP Authentication Overview

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, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The ZyAIR supports EAP-TLS, EAP-TTLS, LEAP and PEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the different types.

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the *IEEE 802.1x appendix*.

- ♦ The wireless station sends a "start" message to the AP.
- ♦ The AP sends a "request identity" message to the wireless station for identity information.
- ♦ The wireless station replies with identity information, including username and password.
- ♦ The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

Figure 2-15 802.1x Authentication

Follow the instructions in the table to configure 802.1x authentication.

Table 2-7 802.1x Authentication

FIELD	DESCRIPTION
Authentication	Select **802.1x** from the drop-down list box.
EAP Type	Select an EAP Type from the drop-down list box. See *Types of EAP Authentication* in the *Appendix* of this *User's Guide* for information on the fields listed below: **EAP-TLS** **EAP-TTLS** **EAP-MD5** **EAP-PEAP** **LEAP**
Login Name	Enter a user name. This is the user name that you or an administrator set up on the RADIUS server.
Password	If you want all wireless stations to have to enter passwords before access to the wired network is allowed, type a **Password**.
Certificate	This field is only available when you select **EAP-TLS** in the **EAP Type** 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.**

Table 2-7 802.1x Authentication

FIELD	DESCRIPTION
Validate Server Certificate	This field is not available when you select **EAP-MD5** or **LEAP** from the **EAP Type** list. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. Select the check box to have your server validate this certificate.
TTLS Protocol/ PEAP Protocol	Select a protocol from the drop-down list box. The choices are: **EAP-TTLS** PAP CHAP MS CHAP MS CHAP v2 **EAP-PEAP** MD5 Challenge EAP-GTC MS CHAP v2 See the *Types of EAP Authentication* in the appendix for details.
OK	Click **OK** to apply the changes and close the screen.

2.11 The About Screen

The **About** screen displays related version numbers of the ZyAIR.
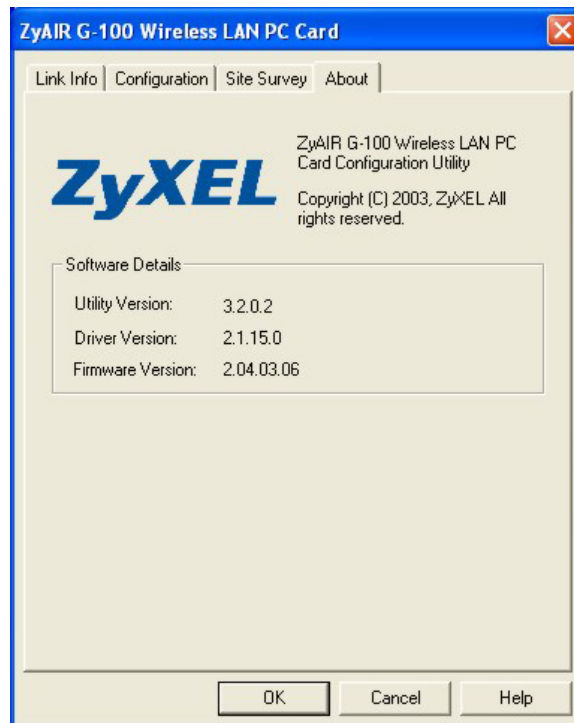
Figure 2-16 About

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

Table 2-8 About

| FIELD	DESCRIPTION
Utility Version	This field displays the version number of the ZyAIR Utility.
Driver Version	This field displays the version number of the ZyAIR wireless card driver.
Firmware	This field displays the version of the firmware of the ZyAIR card.
OK	Click **OK** to apply the changes and close the screen.
Cancel	Click **Cancel** to discard all changes and close the screen.
Help	Click **Help** to display on-line help screen.

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.

1. Click Start, Programs, ZyAIR G-200 Wireless LAN USB Adapter, Uninstall.

2. A **Confirm Uninstallation** window displays. Click **OK** to remove the driver and the utility software.
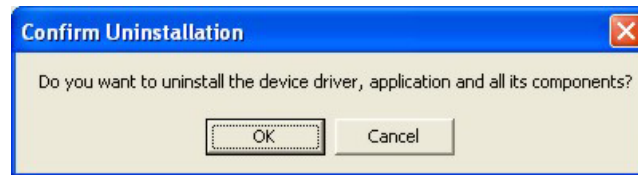
Figure 3-1 Confirm Uninstallation

3. Restart your computer when prompted.

3.2 Upgrading the ZyAIR Utility

To perform the upgrade, follow the steps below.

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

2. Follow the steps in the *Removing the ZyAIR Utility* section to remove the current ZyAIR Utility from your computer.

3. Restart the computer when prompted.

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

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

3.3 Disconnecting the ZyAIR

☞ **To avoid losing data, DO NOT disconnect the ZyAIR while data transmission is taking place.**

After you exit from the ZyAIR Utility program, you may disconnect the ZyAIR from your computer.

You do not have to turn off the computer before removing the ZyAIR - you can insert or remove the ZyAIR while the computer is turned on. However, it is recommended that you stop the operation of the ZyAIR first.

Follow the steps below to disable the ZyAIR in Windows. Screen shots may vary depending on the version of Windows.
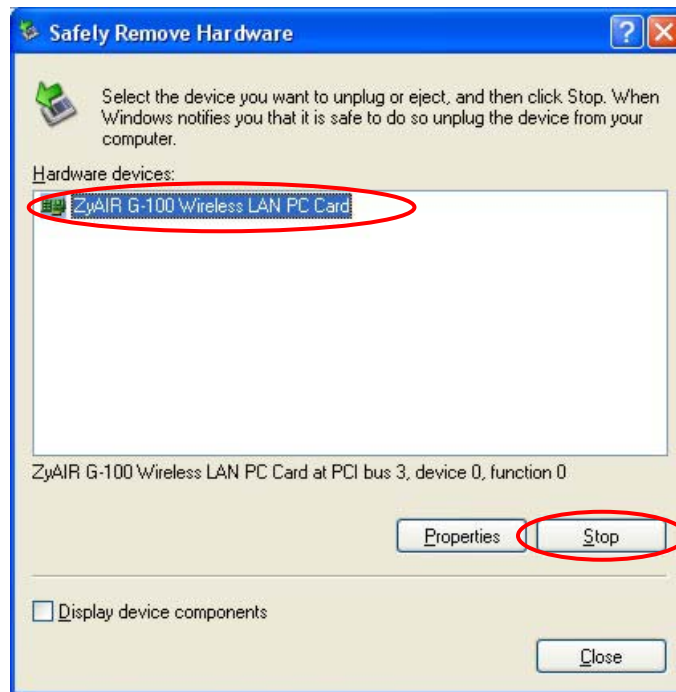
1. Close and exit the ZyAIR Utility.
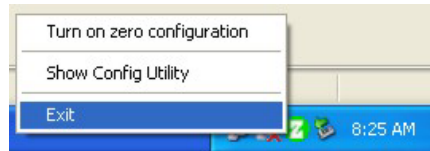
Figure 3-2 ZyAIR Utility: Exit

2. Double-click the removable device icon in the system tray.

Figure 3-3 Removable Device System Tray Icon: Windows XP

3. When a **Safely Remove Hardware** window displays, select the ZyAIR device in the **Hardware devices** list and click **Stop**.

Figure 3-4 Safely Remove Hardware: Windows XP

4. If you do not close and exit the ZyAIR Utility, a warning window displays. Click **OK** and then close and exit the ZyAIR Utility.

5. Click **OK** in the **Stop a Hardware device** window to stop the ZyAIR.

Figure 3-5 Stop a Hardware device: Windows XP

6. After the following notice window displays in the system tray, you can safely disconnect the ZyAIR from your computer.

Figure 3-6 Safe To Remove Hardware Message: Windows XP

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

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyAIR Utility	Make sure the ZyAIR is properly inserted and the **PWR** 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.
The ZyAIR Utility displays only three tabs.	When the ZyAIR Utility displays only three tabs, you are using the Windows XP wireless configuration tool at the same time. Refer to *Section 1.2* to disable the Windows XP wireless configuration tool.

4.2 Problems Communicating With Other Computers

Table 4-2 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The **Connect** button is disabled in the **Site Survey** screen	You are using the Windows XP wireless configuration tool and the ZyAIR Utility at the same time. Refer to *Section 1.2* to disable the Windows XP wireless configuration tool.
The computer connected to the ZyAIR cannot communicate with the other computer.	
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. Change the AP and the associated wireless clients to use another radio channel if interference is high. Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Security Configuration** screen.

Table 4-2 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
B. **Ad-Hoc (IBSS)**	Verify that the peer computer(s) is turned on.
	Make sure the ZyAIR and the peer computer(s) are using the same SS ID and channel.
	Make sure that the ZyAIR and the peer computer(s) share the same security option and key.
	Change the wireless clients to use another radio channel if interference is high.
	Make sure that the ZyAIR and the peer computer(s) share the same security option and key. Verify the settings in the **Security Configuration** screen.

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 AP with a better link quality using the **Site Survey** 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.

4.4   The ZyAIR Does Not Respond

Table 4-4 Troubleshooting the ZyAIR

PROBLEM	CORRECTIVE ACTION
The ZyAIR connected to a computer does not respond after resuming the computer from sleep mode.	When you resume your computer from sleep/standby/suspend mode, the ZyAIR may not work or immediately respond.
	If this happens, disconnect and connect the ZyAIR.

Appendix A
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.
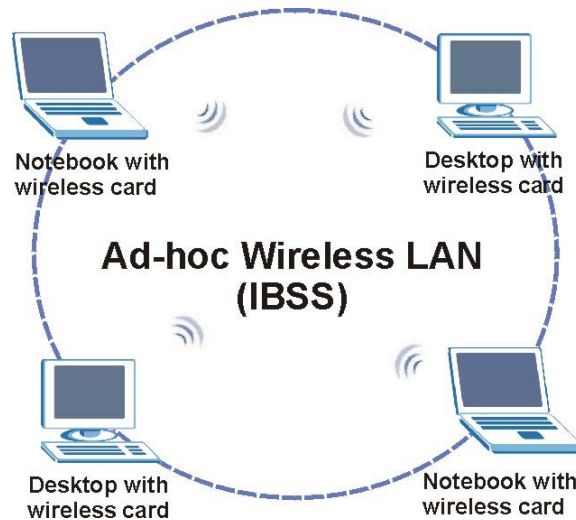
Diagram 4-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.
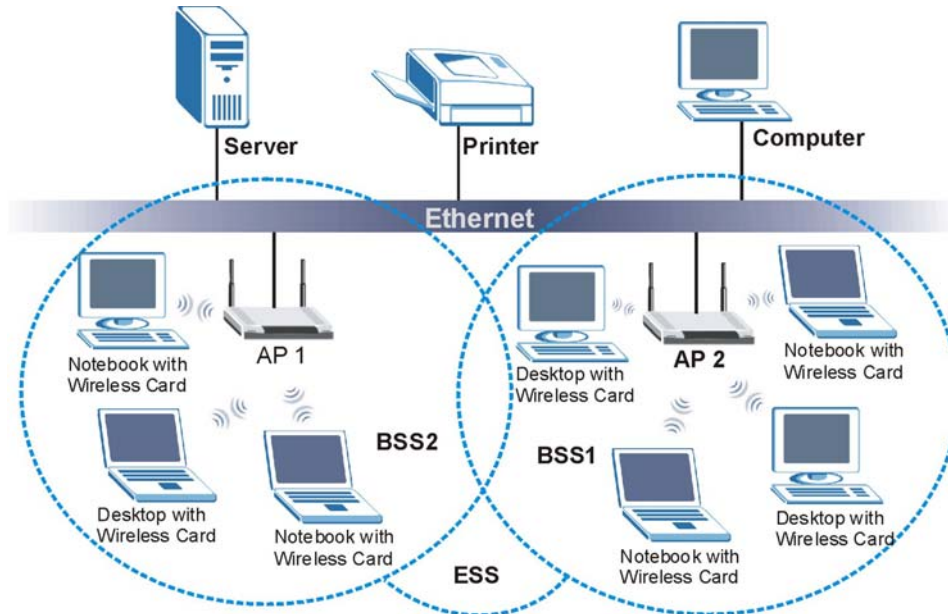
Diagram 4-2 ESS Provides Campus-Wide Coverage

Appendix B
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

Advantages of the IEEE 802.1x

- ♦ User based identification that allows for roaming.
- ♦ Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- ♦ Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

<u>RADIUS Server Authentication Sequence</u>

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).
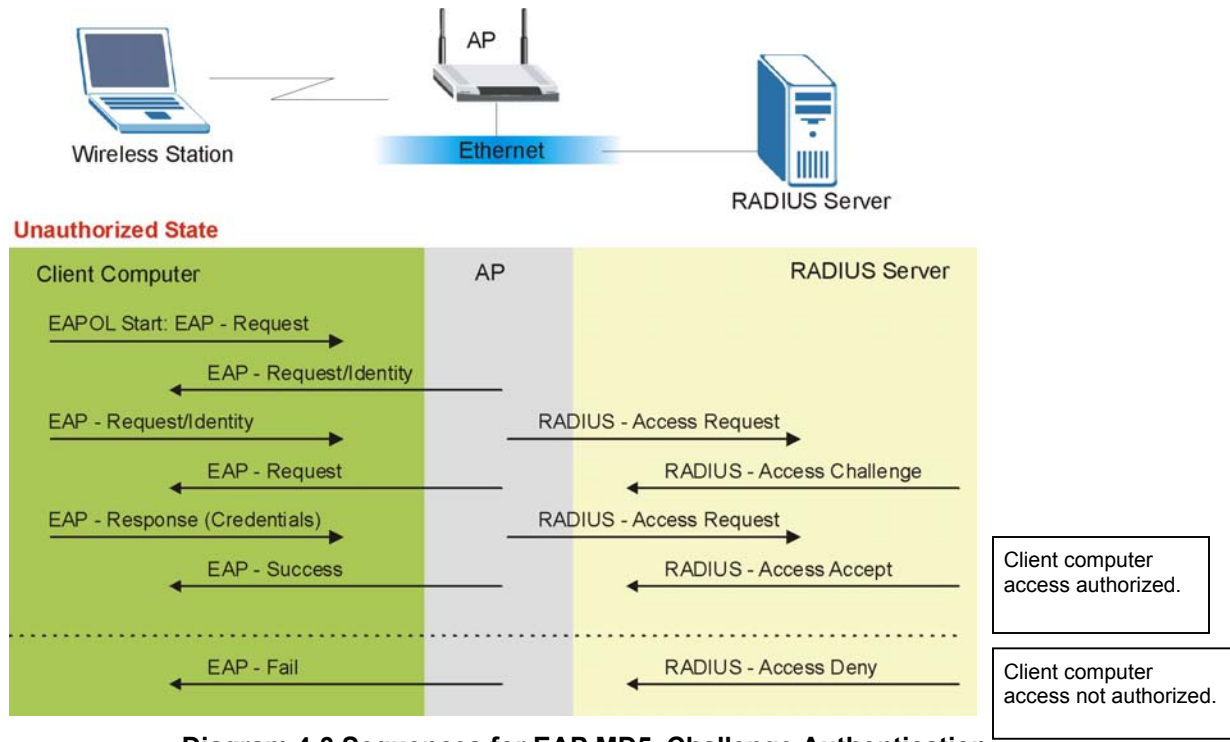
Diagram 4-3 Sequences for EAP MD5–Challenge Authentication

Appendix C
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 (Light 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 Security	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Wireless Security	Poor	Best	Good	Good	Good
Client Identity Protection	No	No	Yes	Yes	No

Appendix D
Product Specifications

PHYSICAL SPECIFICATIONS	
Product Name	ZyAIR G-100 802.11g Wireless CardBus Card
Type	3.3V 32-bit CardBus
Standards	IEEE 802.11b IEEE 802.11g
Antenna	Internal PCB antenna

RADIO SPECIFICATIONS	
Media Access Protocol	IEEE802.11
Frequency	2.412-2.497GHz
Channels	11 Channels (USA, Canada) 13 Channels (Europe) 14 Channels (Japan)
Data Rate	802.11b: 11, 5.5, 2, 1Mbps 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	802.11g: OFDM with BPSK, QPSK and 16/64-QAM sub-carrier modulations 802.11b: DBPSK, DQPSK, CCK
Output Power	17 dBm (typical) at 11Mbps CCK 13 dBm (typical) at 54Mbps OFDM
RX Sensitivity	802.11g (OFDM): 54 Mbps: -71 dBm 48 Mbps: -72 dBm 36 Mbps: -76 dBm 24 Mbps: -80 dBm 18 Mbps: -83 dBm 12 Mbps: -85 dBm 9 Mbps: -87 dBm 6 Mbps: -88 dBm 802.11b (CCK/DSS): 11 Mbps: -85 dBm 5.5 Mbps: -88 dBm 2 Mbps: -91 dBm 1 Mbps: -94 dBm

SOFTWARE SPECIFICATIONS	
Device Drivers	Windows 2000, Windows XP. [2]
Roaming	802.11 compliant
WEP	Supports 64-bit and 128-bit encryption

●

[2] At the time of writing.

ENVIRONMENTAL SPECIFICATIONS	
Temperature	Operating: 0° ~ 50° C Storage: -20° ~ 75° C
Relative Humidity	5% to 95% (non-condensing)

Index