

ZyAIR G-110

802.11g Wireless CardBus Card

User's Guide

Version 1.10

May 2004



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 two (2) years 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.

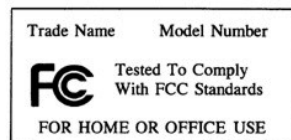
Caution

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

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

Certifications

1. Go to www.zyxel.com.
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.



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	TELEPHONE ¹	WEB SITE	REGULAR MAIL
	SALES E-MAIL	FAX ¹	FTP SITE	
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 Niils Hansens vei 13 0667 Oslo Norway

¹ “+” is the (prefix) number you enter to make an international telephone call.

ZyAIR G-110 User's Guide

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

Copyright.....	ii
ZyXEL Limited Warranty	iii
Information for Canadian Users.....	iv
Federal Communications Commission (FCC) Interference Statement.....	v
Customer Support.....	vii
List of Figures.....	xi
List of Tables	xii
Preface.....	xiii
Chapter 1 Getting Started.....	1-1
1.1 About Your ZyAIR	1-1
1.2 ZyAIR Hardware and Utility Installation.....	1-1
1.3 Disable Windows XP Wireless LAN Configuration Tool.....	1-1
1.4 Accessing the ZyAIR Utility.....	1-4
Chapter 2 Using the ZyAIR Utility.....	2-1
2.1 About Wireless LAN Network.....	2-1
2.1.1 Channel	2-1
2.1.2 SSID	2-1
2.1.3 Transfer Rate.....	2-1
2.2 Wireless Network Application.....	2-1
2.2.1 Ad-Hoc (IBSS).....	2-2
2.2.2 Infrastructure.....	2-2
2.3 Roaming.....	2-3
2.4 Viewing Current Configuration	2-4
2.4.1 Common Screen Command Buttons	2-6
2.5 Configuring the ZyAIR Wireless Parameters.....	2-6
2.6 Network Configuration Profile Setting.....	2-9
2.6.1 Saving the Current Setting to a Profile.....	2-9
2.6.2 Using a Pre-configured Profile.....	2-9
2.6.3 Deleting a Profile	2-10
2.7 The Site Survey Screen.....	2-10
2.7.1 Connecting to a Network.....	2-11
2.8 About Wireless LAN Security.....	2-11
2.8.1 Data Encryption with WEP	2-12

2.8.2	Authentication Mode	2-13
2.8.3	IEEE 802.1x.....	2-13
2.8.4	WPA	2-13
2.8.5	WPA-PSK Application Example.....	2-14
2.8.6	WPA with RADIUS Application Example.....	2-15
2.9	<i>Configuring Wireless Security on the ZyAIR</i>	2-16
2.9.1	WEP Encryption	2-17
2.9.2	WPA-PSK.....	2-19
2.9.3	WPA	2-20
2.9.4	IEEE802.1x.....	2-22
2.10	<i>The About Screen</i>	2-24
Chapter 3 Maintenance		3-1
3.1	<i>Uninstalling the ZyAIR Utility</i>	3-1
3.2	<i>Upgrading the ZyAIR Utility</i>	3-1
Chapter 4 Troubleshooting		4-1
4.1	<i>Problems Starting the ZyAIR Utility Program</i>	4-1
4.2	<i>Problems Communicating With Other Computers</i>	4-1
4.3	<i>Problem with the Link Status</i>	4-2
Appendix A Types of EAP Authentication		A
Appendix B Product Specifications.....		C
Index		F

List of Figures

Figure 1-1 Windows XP: System Tray Icon.....	1-2
Figure 1-2 Windows XP: System Tray Icon.....	1-2
Figure 1-3 Windows XP: Wireless Network Connection Status	1-2
Figure 1-4 Windows XP: Wireless Network Connection.....	1-3
Figure 1-5 Windows XP: Wireless Network Connection Properties.....	1-4
Figure 1-6 ZyAIR Utility: System Tray Icon	1-4
Figure 2-1 Ad-hoc Network Example	2-2
Figure 2-2 BSS Example.....	2-2
Figure 2-3 Infrastructure Network Example	2-3
Figure 2-4 Roaming Example	2-4
Figure 2-5 ZyAIR Utility: Link Info	2-5
Figure 2-6 ZyAIR Utility: Profile: Configuration.....	2-7
Figure 2-7 Odyssey Client	2-8
Figure 2-8 ZyAIR Utility: Profile	2-9
Figure 2-9 Site Survey	2-10
Figure 2-10 Wireless LAN Security Levels	2-12
Figure 2-11 WPA - PSK Authentication.....	2-15
Figure 2-12 WPA with RADIUS Application Example	2-16
Figure 2-13 ZyAIR Utility: Security Configuration: None.....	2-17
Figure 2-14 ZyAIR Utility: Security Configuration: WEP	2-18
Figure 2-15 ZyAIR Utility: Security Configuration: WPA-PSK	2-20
Figure 2-16 ZyAIR Utility: Security Configuration: WPA	2-21
Figure 2-17 ZyAIR Utility: Security Configuration: 802.1x.....	2-23
Figure 2-18 ZyAIR Utility: About	2-25

List of Tables

Table 1-1 ZyAIR Utility: System Tray Icon	1-5
Table 2-1 ZyAIR Utility: Link Info	2-5
Table 2-2 Common Screen Command Buttons.....	2-6
Table 2-3 ZyAIR Utility: Profile: Configuration	2-7
Table 2-4 Site Survey.....	2-10
Table 2-5 ZyAIR Utility: Security Configuration: WEP	2-18
Table 2-6 ZyAIR Utility: Security Configuration: WPA-PSK.....	2-20
Table 2-7 ZyAIR Utility: Security Configuration: WPA	2-21
Table 2-8 ZyAIR Utility: Security Configuration: 802.1x.....	2-23
Table 2-9 ZyAIR Utility: About.....	2-25
Table 4-1 Troubleshooting Starting ZyAIR Utility Program	4-1
Table 4-2 Troubleshooting Communication Problems	4-1
Table 4-3 Troubleshooting Link Status.....	4-2

Preface

Congratulations on the purchase of your new ZyAIR G-110 802.11g Wireless CardBus Card!

About This User's Guide

This guide provides information about the ZyAIR G-110 Wireless LAN Utility that you use to configure your ZyAIR G-110. Familiarize yourself with the *Syntax Conventions* listed below for better and faster understanding.

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-110 802.11g Wireless CardBus Card is referred to as the ZyAIR in this guide.
- The ZyAIR G-110 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!

Graphics Icons Key

 Wireless Access Point	 Computer	 Notebook computer
 Server	 Modem	 Wireless Signal
 Telephone	 Switch	 Router

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 PC card that fits into any 32-bit CardBus slot. With the ZyAIR, you can enjoy the 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/g/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.
- Supports IEEE802.1x and WPA (Wi-Fi Protected Access).
- Low CPU utilization allowing more computer system resources for other programs.
- A built-in antenna and one external antenna connector (refer to the *Quick Installation Guide*).
- Power and Link LEDs.
- 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 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**.

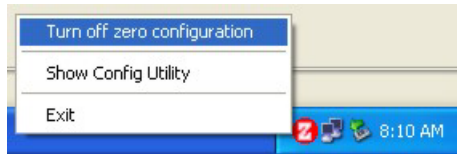


Figure 1-1 Windows XP: System Tray Icon

From the Wireless Network Connection Status Screen

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 1-2 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.

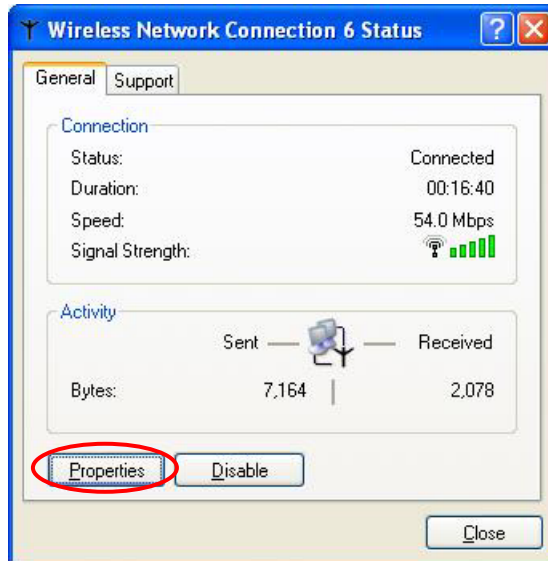


Figure 1-3 Windows XP: Wireless Network Connection Status

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

Step 5. When a **Wireless Network Connection** window displays, click **Advanced...**

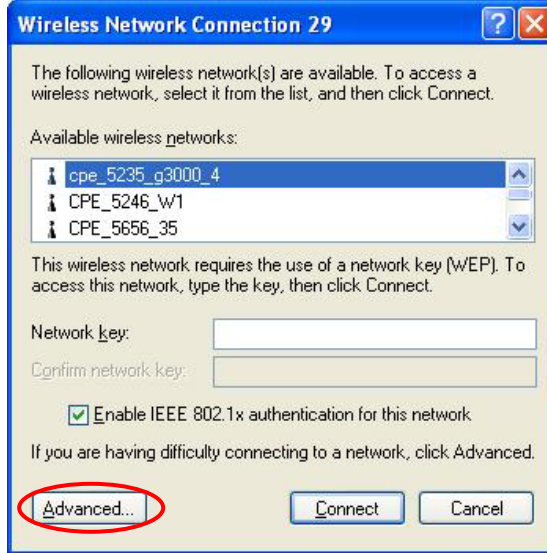


Figure 1-4 Windows XP: Wireless Network Connection

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**.

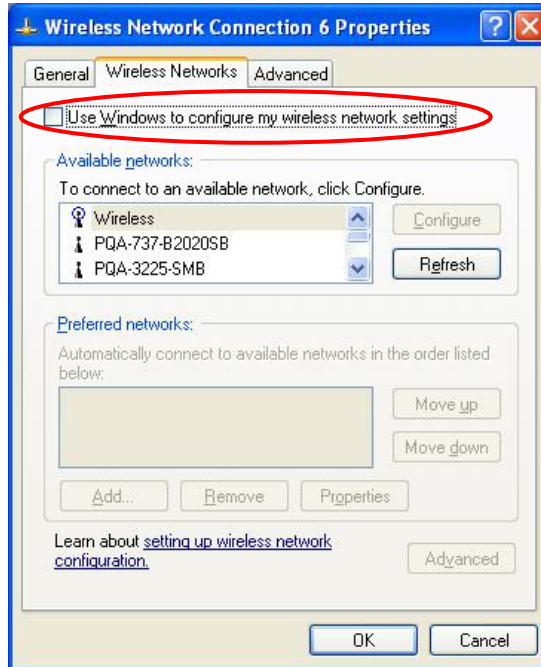


Figure 1-5 Windows XP: Wireless Network Connection Properties

1.4 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 not connected to a wireless network or is searching for an available wireless network.
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 Wireless LAN Network

This section describes each wireless LAN parameter.

2.1.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b wireless devices. 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 Transfer 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.

2.2 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.

2.2.1 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).

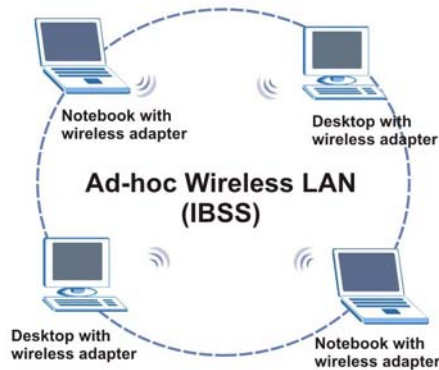


Figure 2-1 Ad-hoc Network Example

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

2.2.2 Infrastructure

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

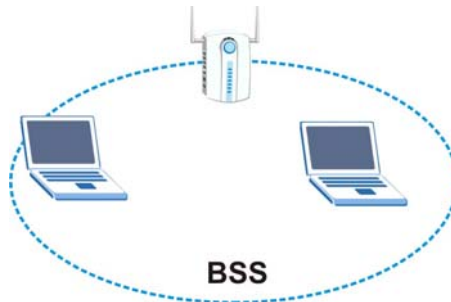


Figure 2-2 BSS Example

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.

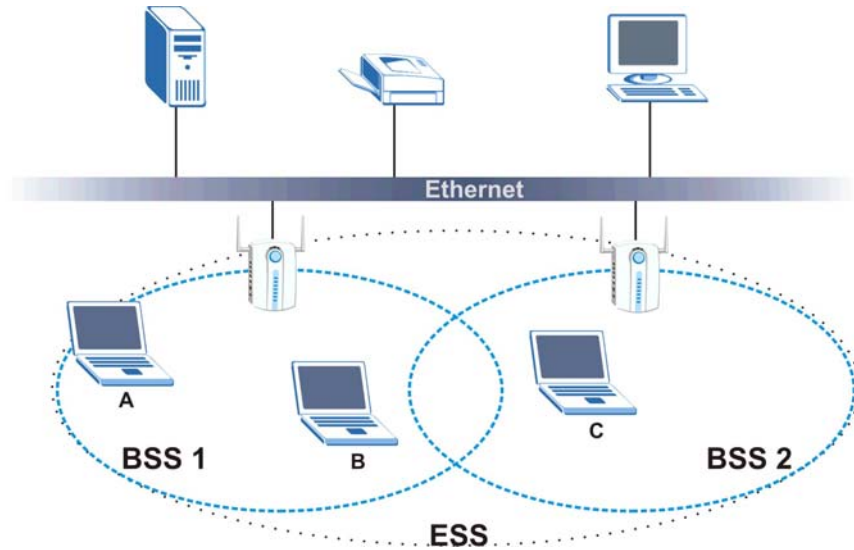


Figure 2-3 Infrastructure Network Example

2.3 Roaming

Roaming in an infrastructure network, wireless stations are able to switch from one BSS to another as they move between coverage areas. During this period, the wireless station maintains uninterrupted connection to the network. As the wireless station 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 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.

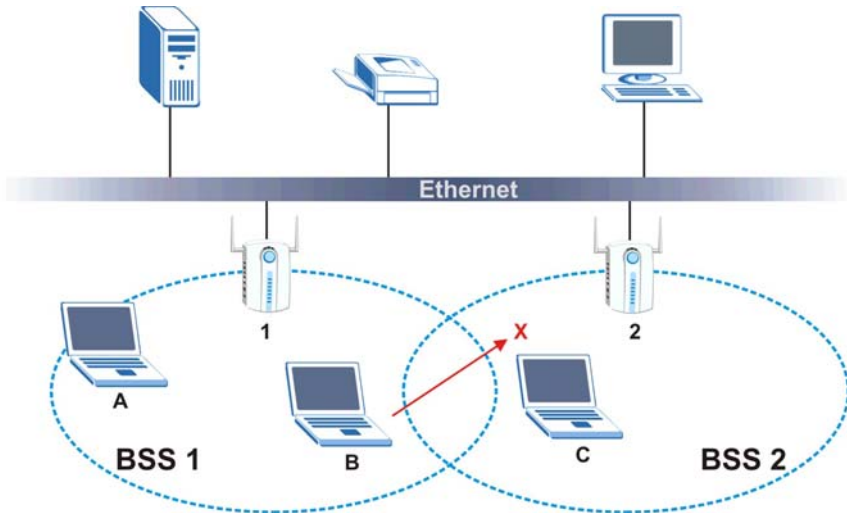


Figure 2-4 Roaming Example

2.4 Viewing Current Configuration

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

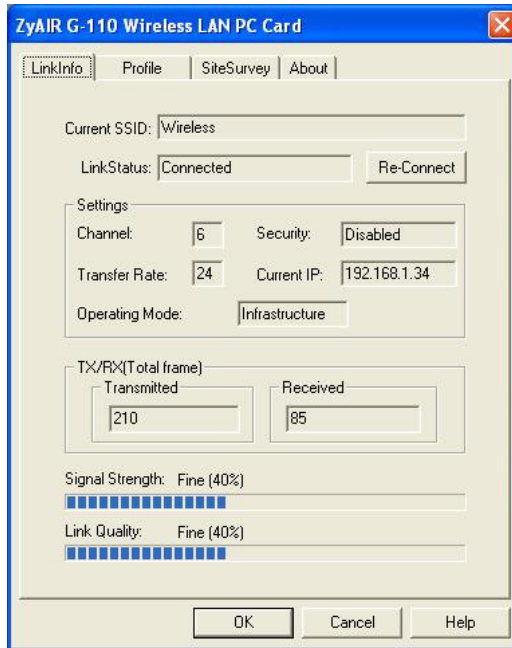


Figure 2-5 ZyAIR Utility: Link Info

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 device/network to which the ZyAIR is associated.
Link Status	This field displays the current connection status of the ZyAIR.
Re-Connect	Click Re-Connect to have the ZyAIR search for and connect to a wireless device with the best signal reception.
Settings	
Channel	This field displays the radio channel the ZyAIR is currently using to connect to a wireless device.
Security	This field displays the wireless security mode you select in the Security Configuration screen.

Table 2-1 ZyAIR Utility: Link Info

LABEL	DESCRIPTION
Transfer Rate	This field displays the current transmission rate of the ZyAIR in megabits per second (Mbps).
Current IP	This field displays the current IP address of the ZyAIR.
Operating Mode	This field displays the network type (Infrastructure or Ad Hoc) of the ZyAIR.
Tx/Rx (Total Frames)	
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 show the strength of the signal.
Link Quality	The status bar and the percentage number show the quality of the link.

2.4.1 Common Screen Command Buttons

The following table describes common command buttons on all ZyAIR Utility screens.

Table 2-2 Common Screen Command Buttons

BUTTON	DESCRIPTION
OK	Click OK to save all changes and close the ZyAIR Utility.
Cancel	Click Cancel to discard changes and close the ZyAIR Utility.
Help	Click Help to display the on-line help window.

2.5 Configuring the ZyAIR Wireless Parameters

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

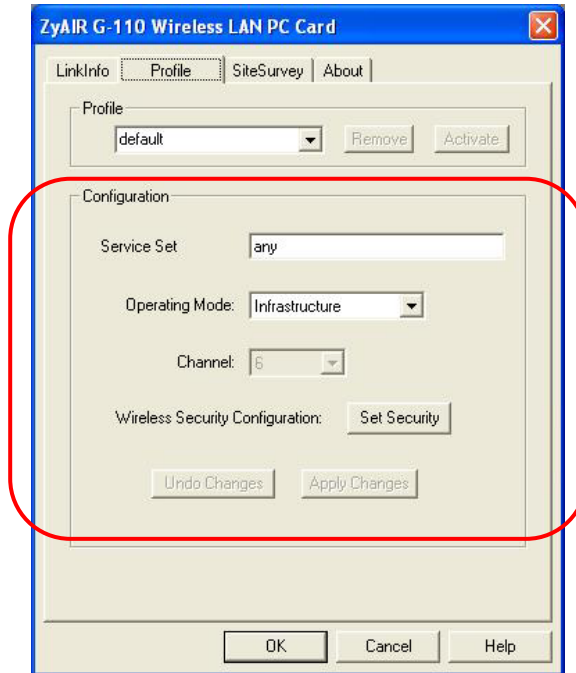


Figure 2-6 ZyAIR Utility: Profile: Configuration

Follow the instructions in the table below to configure the wireless LAN related fields. Refer to the next section for **Profile** field descriptions.

Table 2-3 ZyAIR Utility: Profile: Configuration

FIELD	DESCRIPTION
Configuration	
Server Set	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, you must enter the same SSID as the peer ad-hoc computer. Enter any to associate to or roam between any infrastructure wireless networks.
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 <i>Section 2.2</i> for more information.

Table 2-3 ZyAIR Utility: Profile: Configuration

FIELD	DESCRIPTION
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.
Wireless Security Configuration	Click Set Security to display the Security Configuration screen and configure the security settings for this profile.
Undo Changes	Click Undo Changes to start configuring the fields again.
Apply Changes	Click Apply Changes to save the changes back to ZyAIR.

When you configure the ZyAIR to use a certificate in the **Security Configuration** screen and click **Apply Changes** in the **Profile** screen, the ZyAIR tries to connect to the network and a screen displays as shown.

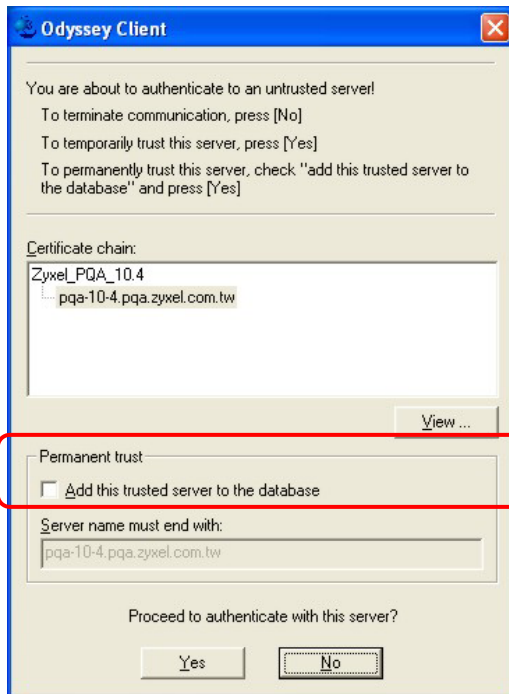


Figure 2-7 Odyssey Client

To trust a server permanently, select **Add this trusted server to the database** and click **Yes**.

To trust a server for this session only, make sure the **Add this trusted server to the database** check box is not selected and click **Yes**.

If you don't want to trust an authentication server, click **No**. The ZyAIR will not connect to the network.

2.6 Network Configuration Profile Setting

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

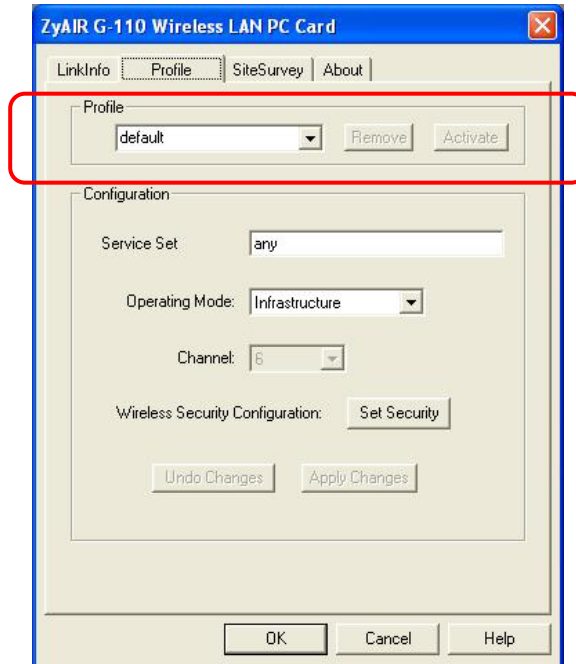


Figure 2-8 ZyAIR Utility: Profile

2.6.1 Saving the Current Setting to a Profile

To save the current settings in the **Profile** screen to a new profile, enter a descriptive name in the **Profile** field and click **Apply Changes**. This also activates the new profile at the same time.

2.6.2 Using a Pre-configured 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 remove a profile, the ZyAIR Utility reverts to use the default profile.

2.6.3 Deleting a Profile

To delete an existing wireless network configuration, select a profile from the drop-down list box and click **Remove**.

2.7 The Site Survey Screen

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

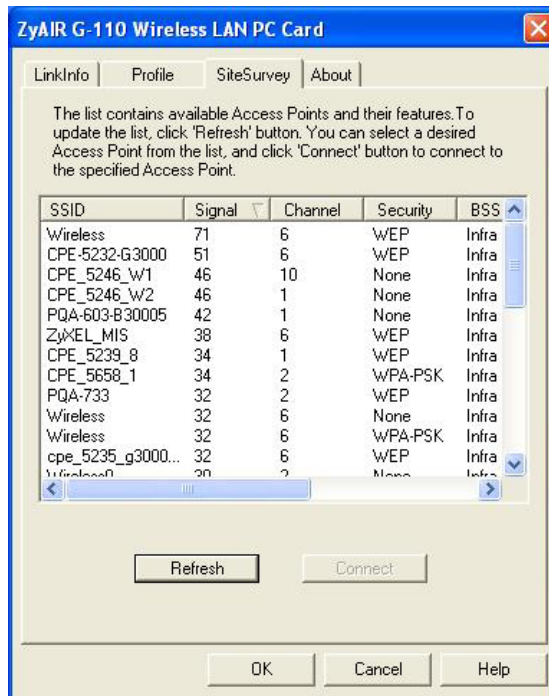


Figure 2-9 Site Survey

The following table describes the fields in the table.

Table 2-4 Site Survey

FIELD	DESCRIPTION
ESSID	This field displays the SSID (or name) of each wireless device.

Table 2-4 Site Survey

FIELD	DESCRIPTION
Signal	This field displays the signal strength of each wireless device in percentage.
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).
BSS Type	This field displays the wireless network type (Infra or Ad Hoc) of the wireless device. Infra denotes the infrastructure mode.
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.
Refresh	Click Refresh to scan for available wireless device(s) within transmission range.
Connect	Click Connect to associate to the selected wireless device.

2.7.1 Connecting to a Network

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

- Step 1.** Click **Search** to scan for all available wireless networks within range.
- Step 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.
- Step 3.** If the **Security** field is activated for the selected wireless network, you must also set the related fields in the **Security Configuration** screen to the same security settings. Refer to *Section 2.9* for more information.
- Step 4.** Verify that you have successfully connected to the selected network and check the network information in the **Link Info** screen.

2.8 About 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.

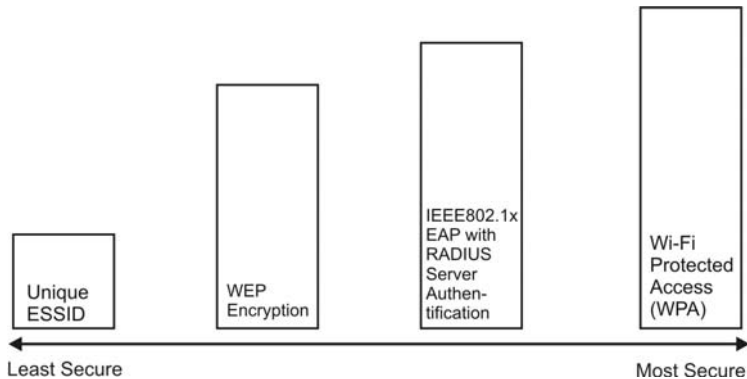


Figure 2-10 Wireless LAN Security Levels

Configure the wireless LAN security using the **Security Configuration** 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.

2.8.1 Data Encryption with WEP

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 stations 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 and only available when you select the **HEX** key type. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN. For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Configuration** screen of the ZyAIR Utility and entering them manually as the WEP keys in the other WLAN adapter(s).
- Enter the WEP keys manually.

Your ZyAIR allows you to configure up to four 64-bit or 128-bit WEP keys. You must enter four keys but only one key is used as the default key at any one time.

2.8.2 Authentication Mode

The IEEE 802.11b standard describes a simple authentication method between the wireless stations and AP. Two authentication modes are defined: Open and Shared.

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

2.8.3 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.

2.8.4 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.

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 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.

2.8.5 WPA-PSK Application Example

A WPA-PSK application looks as follows.

- Step 1.** First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- Step 2.** The AP checks each client'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 clients.
- Step 4.** The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

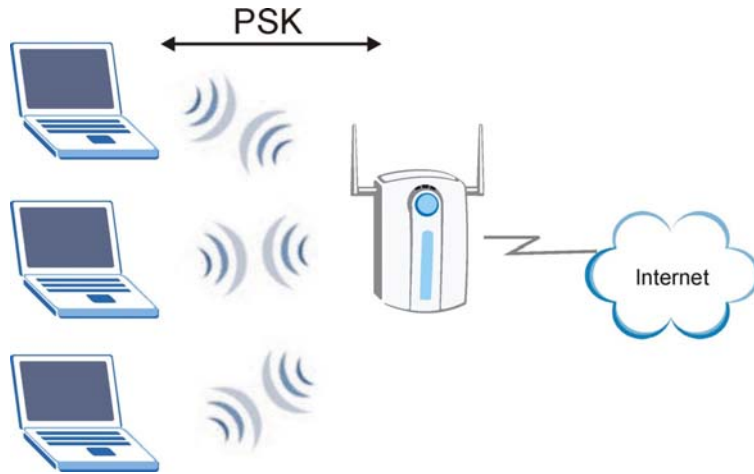


Figure 2-11 WPA - PSK Authentication

2.8.6 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 client'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 clients.

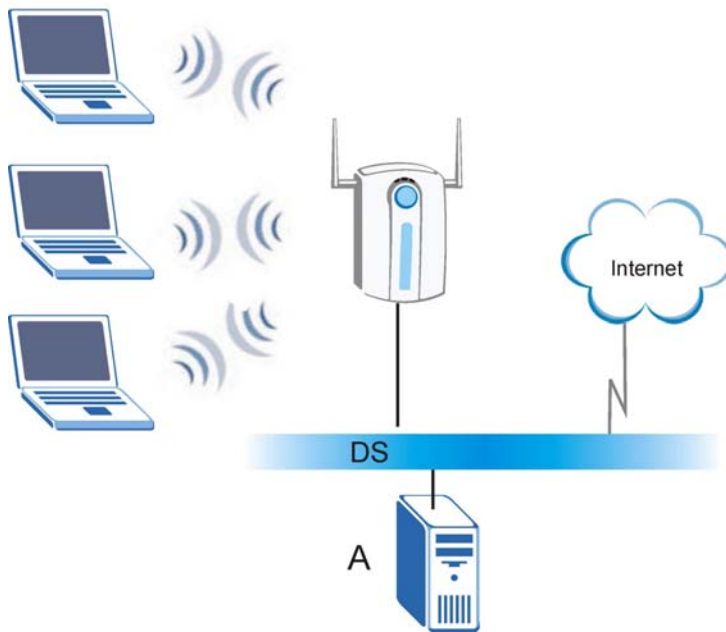


Figure 2-12 WPA with RADIUS Application Example

2.9 Configuring Wireless Security on the ZyAIR

In the **Profile** screen, click **Set Security** to display the **Security Configuration** screen as shown next. The screen varies depending on what you select in the **Authentication** field. You see the next screen when you select **None** in the **Authentication** field.

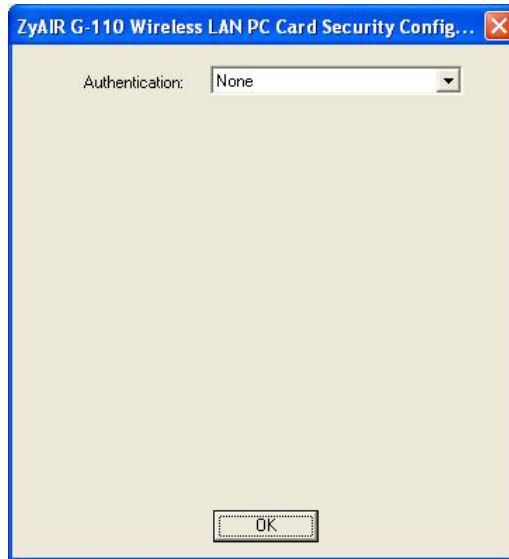


Figure 2-13 ZyAIR Utility: Security Configuration: None

2.9.1 WEP Encryption

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.

Select **WEP** in the **Authentication** field to display the screen as shown next.

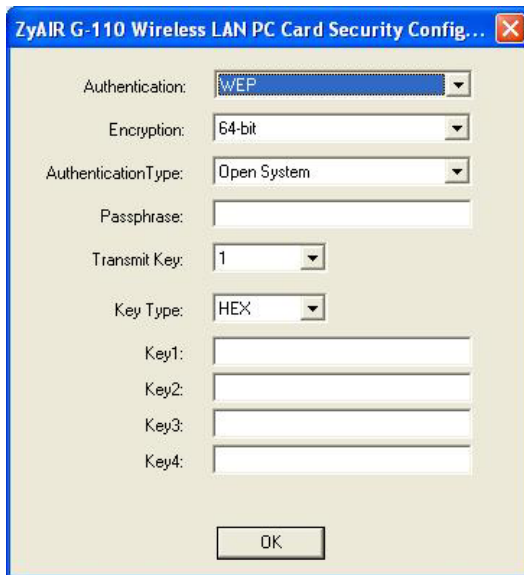


Figure 2-14 ZyAIR Utility: Security Configuration: WEP

The following table describes the labels in this screen.

Table 2-5 ZyAIR Utility: Security Configuration: WEP

FIELD	DESCRIPTION
Authentication	Select WEP from the drop down list.
Encryption	The WEP keys are used to encrypt data 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. Select either 64-bit or 128-bit from the drop-down list box to activate WEP encryption and then fill in the related fields.
Authentication Type	Select Open System or Shared Key from the drop-down list box to authenticate the access point. Refer to <i>Section 2.8.2</i> for more information.

Table 2-5 ZyAIR Utility: Security Configuration: WEP

FIELD	DESCRIPTION
PassPhrase	<p>Enter the passphrase in the field provided. As you enter the passphrase, the ZyAIR automatically generates the WEP keys and displays them in the key fields below. Write down the automatically generated WEP keys in and use them to manually set the WEP keys in other WLAN adapters.</p> <p>Leave this field blank if you want to manually enter the WEP keys.</p> <p>The passphrase is case-sensitive and only available when you select the HEX key type. You must use the same passphrase for all wireless LAN adapters with this feature in the same WLAN.</p>
Key Type	<p>Select ASCII to enter WEP keys as ASCII characters.</p> <p>Select HEX to enter the WEP keys as hexadecimal characters.</p>
Transmit Key	<p>From the drop-down list menu, select a WEP key to use for data encryption.</p>
Key 1 ... 4	<p>Enter the WEP keys in the fields provided.</p> <p>If you select 64-bit in the Encryption field.</p> <ul style="list-style-type: none"> ♦ Enter either 10 hexadecimal characters in the range of "A-F", "a-f" and "0-9" (e.g. 11AA22BB33) for HEX key type <p>or</p> <ul style="list-style-type: none"> ♦ Enter 5 printable ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (e.g. MyKey) for ASCII key type. <p>If you select 128-bit in the Encryption field,</p> <ul style="list-style-type: none"> ♦ Enter either 26 hexadecimal characters in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type <p>or</p> <ul style="list-style-type: none"> ♦ Enter 13 printable ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type. <div style="border: 1px solid black; padding: 5px; text-align: center; margin-top: 10px;"> <p>The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN.</p> <p>ASCII WEP key is case sensitive.</p> </div>
OK	<p>Click OK to save the changes.</p>

2.9.2 WPA-PSK

Select **WPA-PSK** in the **Authentication** field to display the screen as shown next.

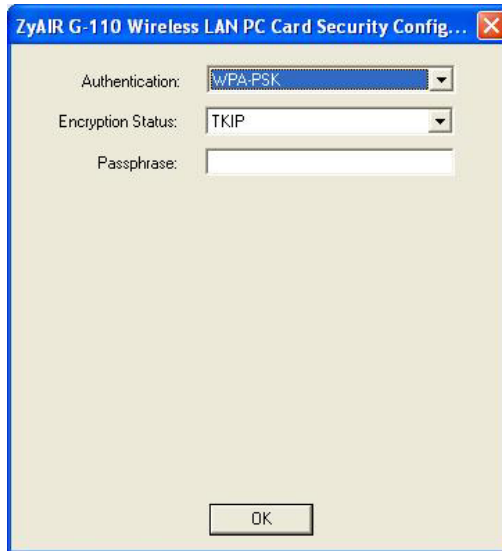


Figure 2-15 ZyAIR Utility: Security Configuration: WPA-PSK

The following table describes the labels in this screen.

Table 2-6 ZyAIR Utility: Security Configuration: WPA-PSK

FIELD	DESCRIPTION
Authentication	Select WPA-PSK from the drop down list.
Encryption Status	WPA uses Temporal Key Integrity Protocol (TKIP) to improve data encryption.
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. Type a passphrase from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
OK	Click OK to save the changes.

2.9.3 WPA

Select **WPA** in the **Authentication** field to display the screen as shown next.

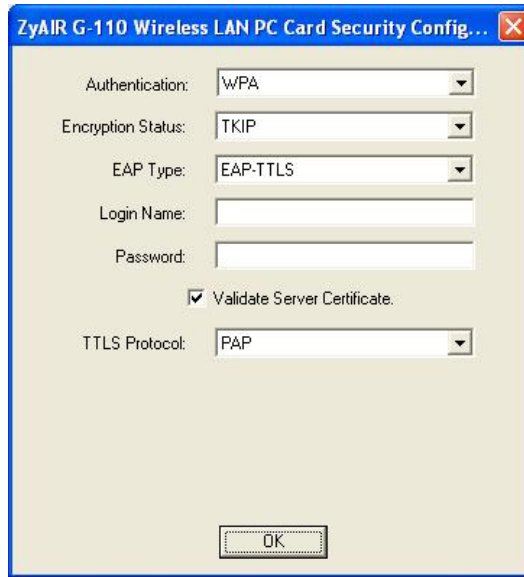


Figure 2-16 ZyAIR Utility: Security Configuration: WPA

The following table describes the labels not previously discussed

Table 2-7 ZyAIR Utility: Security Configuration: WPA

FIELD	DESCRIPTION
Authentication	Select WPA from the drop down list.
Encryption Status	WPA uses Temporal Key Integrity Protocol (TKIP) to improve data encryption.
EAP Type	Select an authentication method from the drop down list. Options are EAP-TLS , EAP-TTLS , EAP-PEAP and LEAP . Select LEAP if the (Cisco) AP you're connecting with uses LEAP to communicate with the RADIUS server.
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. This field is not available when you select EAP-TLS in the EAP Type field.

Table 2-7 ZyAIR Utility: Security Configuration: WPA

FIELD	DESCRIPTION
Certificate	This field is only available when you select EAP-TLS in the EAP Type field. <div style="border: 1px solid black; padding: 5px; background-color: #e0e0e0; margin: 10px auto; width: fit-content;">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.</div>
Validate Server Certificate	This field is not available when you select LEAP in the EAP Type field. Select the check box to check the certificate of the authentication server.
TTLS Protocol	This field is only available when you select EAP-TTLS in the EAP Type field. Use the drop down list box to select a TTLS protocol. Options are PAP , CHAP , MS CHAP and MS CHAP v2 .
PEAP Protocol	This field is only available when you select EAP-PEAP in the EAP Type field. Use the drop down list box to select a PEAP protocol. Options are MD5 Challenge , EAP-GTC and MS CHAP v2 .

2.9.4 IEEE802.1x

The following sections describe how to configure IEEE802.1x security with various authentication methods.

To set the IEEE802.1x WLAN security, select **802.1x** in the **Authentication** field in the **Security Configuration** screen.

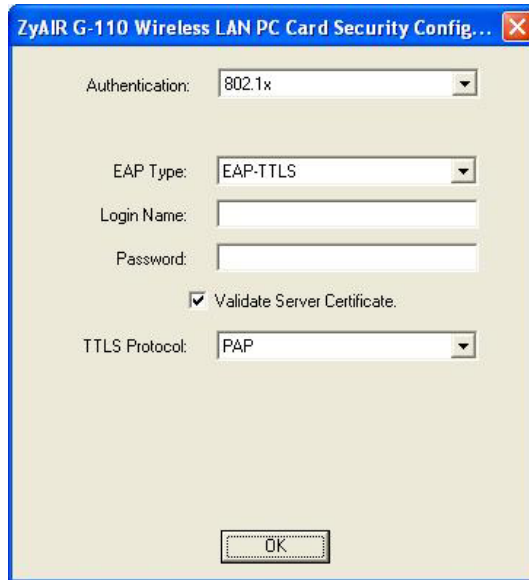


Figure 2-17 ZyAIR Utility: Security Configuration: 802.1x

The following table describes the labels not previously discussed

Table 2-8 ZyAIR Utility: Security Configuration: 802.1x

FIELD	DESCRIPTION
Authentication	Select 802.1x from the drop down list.
EAP Type	Select an authentication method from the drop down list. Options are EAP-TLS , EAP-TTLS , EAP-PEAP and LEAP . Select LEAP if the (Cisco) AP you're connecting with uses LEAP to communicate with the RADIUS server.
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. This field is not available when you select EAP-TLS in the EAP Type field.

Table 2-8 ZyAIR Utility: Security Configuration: 802.1x

FIELD	DESCRIPTION
Certificate	This field is only available when you select EAP-TLS in the EAP Type field. <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0; margin: 10px 0;">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.</div>
Validate Server Certificate	This field is not available when you select LEAP in the EAP Type field. Select the check box to check the certificate of the authentication server.
TTLS Protocol	This field is only available when you select EAP-TTLS in the EAP Type field. Use the drop down list box to select a TTLS protocol. Options are PAP , CHAP , MS CHAP and MS CHAP v2 .
PEAP Protocol	This field is only available when you select EAP-PEAP in the EAP Type field. Use the drop down list box to select a PEAP protocol. Options are MD5 Challenge , EAP-GTC and MS CHAP v2 .

2.10 The About Screen

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

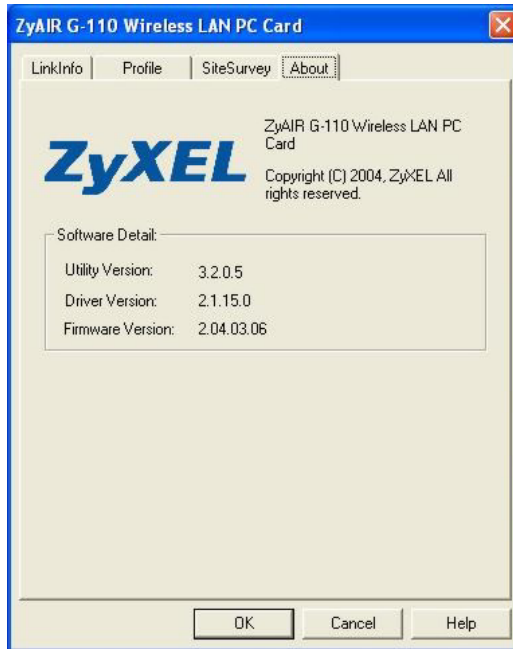


Figure 2-18 ZyAIR Utility: About

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

Table 2-9 ZyAIR Utility: 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 Windows driver.
Firmware Version	This field displays the version of the firmware of the ZyAIR card.

Chapter 3

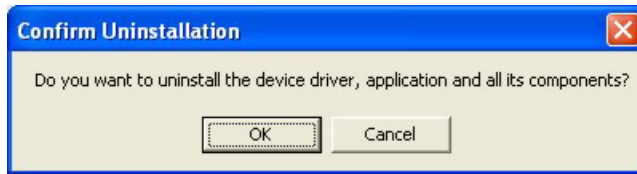
Maintenance

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

3.1 Uninstalling 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, ZyAIR G-110 Wireless LAN PC Card, Uninstall.
- Step 3.** When prompted, click **OK** to remove the driver and the utility software.



- 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 the *Uninstalling the ZyAIR Utility* section 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 <i>Quick Installation Guide</i> 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 network.
A. Infrastructure	<p>Make sure that the AP and the associated computers are turned on and working properly.</p> <p>Make sure the ZyAIR and the associated AP use the same SSID.</p> <p>Configure the AP to use another radio channel if interference is high.</p> <p>Make sure that the computer and the AP shares the same WEP key and authentication mode. Verify the settings in the Security Configuration screens.</p>

Table 4-2 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
B. Ad-Hoc	<p>Verify that the peer computer(s) is turned on.</p> <p>Make sure the ZyAIR and the peer computer(s) are using the same SSID and channel.</p> <p>Use another radio channel if interference is high.</p> <p>Make sure that the ZyAIR and the AP share the same WEP key and authentication mode. Verify the settings in the Security Configuration screens.</p>

4.3 Problem with the Link Status

Table 4-3 Troubleshooting Link Status

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	<p>Move your computer closer to the AP or the peer computer(s) within the transmission range.</p> <p>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.</p>
The Site Survey screen displays all entries with low signal.	<p>Move your computer closer to the AP or peer computer(s) within the transmission range.</p> <p>There is too much radio interference (for example metal structure, microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.</p>

Appendix A

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

Appendix B

Product Specifications

PHYSICAL SPECIFICATIONS	
Product Name	ZyAIR G-110 802.11g Wireless CardBus Card
Type	3.3V 32-bit Cardbus card
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Frequencies	2.412-2.484GHz
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: 11, 5.5, 2, 1Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK) IEEE 802.11b: Direct Spread Spectrum (CCK, DQPSK, DBOSK).
Security	64/128-bit WEP
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 60 degrees Centigrade
Operating Humidity	10 ~ 90% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Power Consumption	TX: 471mA RX: 422mA
Voltage	3.3V±5%
Weight	40g
Dimension	(W) 118mm × (D) 54mm × (H)7.5 mm

RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Frequency	2.4 ~ 2.4835GHz (Industrial Scientific Medical Band)
Channels	1~11 Channels (USA, Canada) 1~13 Channels (Europe)
Data Rate	802.11g (OFDM): 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b: 1, 2, 5.5, 11 Mbps
Modulation	802.11g: OFDM with BPSK, QPSK and 16/64-QAM sub-carrier modulations 802.11b: DBPSK, DQPSK, CCK
Output Power	15 dBm (typical) at 11Mbps CCK 12 dBm (typical) at 54Mbps OFDM
RX Sensitivity	802.11g (OFDM): <ul style="list-style-type: none"> 54 Mbps: -66 dBm 48 Mbps: -71 dBm 36 Mbps: -75 dBm 24 Mbps: -79 dBm 18 Mbps: -81 dBm 12 Mbps: -83 dBm 9 Mbps: -85 dBm 6 Mbps: -88 dBm 802.11b (CCK/DSS): <ul style="list-style-type: none"> 11 Mbps: -83 dBm 5.5 Mbps: -86 dBm 2 Mbps: -89 dBm 1 Mbps: -92 dBm

SOFTWARE SPECIFICATIONS	
Device Drivers	Microsoft Windows 98(SE), Windows 2000, Windows XP, Windows ME
Roaming	802.11 compliant
WEP	Supports 64-bit and 128-bit encryption

ENVIRONMENTAL SPECIFICATIONS

Temperature	Operating: 0° ~ 50° C Storage: -30° ~ 60° C
Relative Humidity	20% to 95% (non-condensing)

Index

A

About 2-24
 Accessing the ZyAIR Utility 1-5
 Authentication Mode 2-13
 Open 2-13
 Shared 2-13
 Automatic WEP key generation 2-12

B

Basic Service Set *See* BSS
 BSS 2-2

C

CA A
 Certificate Authority *See* CA
 Channel 2-8
 Common Screen Command Buttons 2-6
 Communication Problem 4-1
 Ad-hoc (IBSS) 4-2
 Infrastructure 4-2
 Connecting to a Network 2-11
 Copyright ii
 Disclaimer ii
 Trademarks ii
 Create WEP key with passphrase ... 2-19, 2-20, 2-21, 2-23
 Customer Support vii

D

Data encryption 2-12
 Disable Windows XP Wireless Support 1-1

E

EAP Authentication

MD5 A
 PEAP A
 TLS A
 TTLS A
 Encryption 2-14
 ESS 2-3
 Extended Service Set *See* ESS

F

Federal Communications Commission (FCC)
 Interference Statement v

G

Graphics Icons Key xiv

I

IBSS 2-2
 IEEE 802.11g 1-1
 Independent Basic Service Set *See* IBSS
 Information for Canadian Users iv
 Caution iv
 Note iv
 Infrastructure 2-2

L

Link Info 2-4

M

MD5 A
 Message Digest Algorithm 5 *See* MD5
 Message Integrity Check 2-14
 MIC *See* Message Integrity Check

N

Network Configuration Profile	2-9
Deleting.....	2-10
Saving	2-9
Using a pre-configured profile	2-10
Network Type	2-2
Ad-Hoc(IBSS).....	2-2
Infrastructure.....	2-2

O

Online Registration	iii
Open authentication mode.....	2-13
Operating Mode	<i>See</i> Network Type

P

passphrase	2-12
PEAP.....	A
Preface	xiii
problem description.....	4-1
Product specifications	C
Profile.....	2-9
Network Configuration	2-9
Protected EAP	<i>See</i> PEAP

R

Related Documentation.....	xiii
Roaming.....	2-3
Example	2-4

S

Service Set Identity	<i>See</i> SSID
Shared authentication mode	2-13
Site Survey	2-10
SSID.....	2-1, 2-7
Syntax Conventions	xiii

T

Temporal Key Integrity Protocol	2-14
TKIP.....	<i>See</i> Temporal Key Integrity Protocol
TLS	A
Transmission rate	2-1
Transport Layer Security.....	<i>See</i> TLS
Troubleshooting	4-1
Checking Hardware Conflict.....	4-1
Communication problems	4-1
Radio interference	4-2
Site Survey.....	4-2
Starting ZyAIR Utility	4-1
TTLS	A
Tunneled Transport Layer Service	<i>See</i> TTLS

U

Upgrading the ZyAIR Utility	3-1
User Authentication	2-13
Using the ZyAIR Utility.....	2-1

V

Viewing Current Configuration	2-4
-------------------------------------	-----

W

Warranty.....	iii
Note.....	iii
WEP	2-12
WEP Data Encryption	
Configuring	2-16
WEP Data Encryption with.....	2-12
WEP Key.....	2-12
Wired Equivalent Privacy	<i>See</i> WEP
Wireless LAN Parameters	
Channel	2-1
Configuring	2-6
Network Type.....	2-2
SSID.....	2-1
Transmission Rate.....	2-1

Wireless LAN Security
 Data Encryption with WEP..... 2-12
WPA 2-13
WPA with RADIUS Application..... 2-15
WPA-PSK..... 2-13
WPA-PSK Application..... 2-14

Z

ZyAIR Utility 3-1

About 2-25
Before you upgrade..... 3-1
Link Info 2-5
Removing..... 3-1
Site Survey..... 2-10
Upgrading 3-1
WEP Encryption . 2-16, 2-17, 2-18, 2-20, 2-21,
 2-23
ZyAIR Utility system tray icon..... 1-6