

# *ZyAIR G-300*

*Wireless LAN PCI Adapter*

## *User's Guide*

Version 2.00

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

## **NOTE**

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

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

## **Online Registration**

Register online at [www.zyxel.com](http://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

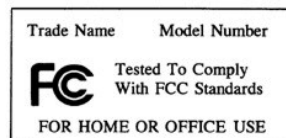
Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Caution

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

## Certifications

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

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

## ZyAIR G-300 User's Guide

---

| METHOD<br>LOCATION | SUPPORT E-MAIL<br>SALES E-MAIL   | TELEPHONE <sup>1</sup><br>FAX <sup>1</sup> | WEB SITE<br>FTP SITE                           | REGULAR MAIL   |
|--------------------|--|--|--|--|
| SWEDEN             | <a href="mailto:support@zyxel.se">support@zyxel.se</a><br><a href="mailto:sales@zyxel.se">sales@zyxel.se</a> | +46 31 744 7700<br>+46 31 744 7701         | <a href="http://www.zyxel.se">www.zyxel.se</a> | ZyXEL Communications A/S<br>Sjöporten 4, 41764 Göteborg<br>Sweden      |
| FINLAND            | <a href="mailto:support@zyxel.fi">support@zyxel.fi</a>   | +358-9-4780-8411                           | <a href="http://www.zyxel.fi">www.zyxel.fi</a> | ZyXEL Communications Oy<br>Malminkaari 10<br>00700 Helsinki<br>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 G-300 .....                                    | 1-1  |
| 1.2 ZyAIR Hardware and Utility Installation.....                    | 1-1  |
| 1.3 Configuration Methods.....                                      | 1-1  |
| 1.4 Windows XP Users Only .....                                     | 1-2  |
| 1.5 Accessing the ZyAIR Utility .....                               | 1-2  |
| 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 Transmission Rate .....                                       | 2-1  |
| 2.1.4 Wireless Network Application .....                            | 2-1  |
| 2.1.5 Roaming.....  | 2-3  |
| 2.1.6 Profile.....  | 2-4  |
| 2.1.7 Threshold Controls.....                                       | 2-4  |
| 2.2 Wireless LAN Security.....                                      | 2-5  |
| 2.2.1 Authentication Mode .....                                     | 2-6  |
| 2.2.2 IEEE 802.1x.....  | 2-6  |
| 2.2.3 WPA.....  | 2-6  |
| 2.2.4 WPA-PSK Application Example.....                              | 2-7  |
| 2.2.5 WPA with RADIUS Application Example .....                     | 2-8  |
| 2.3 The Configuration Screen .....                                  | 2-9  |

|                   |  |             |
|-------------------|--|-------------|
| 2.3.1             | The Advanced Configuration Screen .....                        | 2-12        |
| 2.3.2             | The Security Screen.....                                       | 2-13        |
| 2.3.3             | The Certificate Screen .....                                   | 2-16        |
| <b>2.4</b>        | <b>The Site Survey Screen .....</b>                            | <b>2-18</b> |
| 2.4.1             | Connecting to a Network.....                                   | 2-20        |
| <b>2.5</b>        | <b>The About Screen.....</b>                                   | <b>2-20</b> |
| <b>Chapter 3</b>  | <b>Maintenance .....</b>                                       | <b>3-1</b>  |
| 3.1               | Removing the ZyAIR Utility .....                               | 3-1         |
| 3.2               | Upgrading the ZyAIR Utility .....                              | 3-1         |
| <b>Chapter 4</b>  | <b>Troubleshooting.....</b>                                    | <b>4-1</b>  |
| 4.1               | Problems Starting the ZyAIR Utility Program .....              | 4-1         |
| 4.2               | Problems Communicating With Other Computers .....              | 4-1         |
| 4.3               | Problem with the Link Status.....                              | 4-2         |
| <b>Appendix A</b> | <b>Disable Windows XP Wireless LAN Configuration Tool.....</b> | <b>A</b>    |
| <b>Appendix B</b> | <b>Management with Wireless Zero Configuration .....</b>       | <b>I</b>    |
| <b>Appendix C</b> | <b>Types of EAP Authentication .....</b>                       | <b>Y</b>    |
| <b>Appendix D</b> | <b>Product Specifications.....</b>                             | <b>AA</b>   |
| <b>Index.....</b> |  | <b>CC</b>   |

# List of Figures

|   |      |
|---|------|
| Figure 1-1 ZyAIR Utility: System Tray Icon .....                      | 1-2  |
| 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.....                                       | 2-3  |
| Figure 2-5 RTS Threshold .....  | 2-4  |
| Figure 2-6 Wireless LAN Security Levels.....                          | 2-5  |
| Figure 2-7 WPA-PSK Authentication .....                               | 2-8  |
| Figure 2-8 WPA with RADIUS Application Example.....                   | 2-9  |
| Figure 2-9 Configuration.....   | 2-10 |
| Figure 2-10 Configuration: Advanced.....                              | 2-12 |
| Figure 2-11 Configuration: Privacy Configuration: Security .....      | 2-14 |
| Figure 2-12 Configuration: Privacy Configuration: Certification ..... | 2-17 |
| Figure 2-13 Site Survey.....  | 2-19 |
| Figure 2-14 ZyAIR Utility: About .....                                | 2-21 |
| Figure 3-1 Confirm Uninstallation.....                                | 3-1  |

## List of Tables

|   |      |
|---|------|
| Table 1-1 ZyAIR Utility: System Tray Icon .....                     | 1-2  |
| Table 2-1 Configuration.....  | 2-10 |
| Table 2-2 Configuration: Advanced.....                              | 2-12 |
| Table 2-3 Configuration: Privacy Configuration: Security .....      | 2-14 |
| Table 2-4 Configuration: Privacy Configuration: Certification ..... | 2-17 |
| Table 2-5 Site Survey.....  | 2-19 |
| Table 2-6 ZyAIR Utility: About.....                                 | 2-21 |
| Table 4-1 Troubleshooting Starting ZyAIR Utility Program .....      | 4-1  |
| Table 4-2 Troubleshooting Communication Problems .....              | 4-1  |
| Table 4-3 Troubleshooting Link Quality .....                        | 4-2  |

# Preface

Congratulations on the purchase of your new ZyAIR G-300 Wireless LAN PCI Adapter!

## About This User's Guide

This guide provides information about the ZyAIR G-300 Wireless LAN Utility that you use to configure your ZyAIR.

## Syntax Conventions

- “Type” or “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- Window and command choices are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font.
- The ZyXEL ZyAIR G-300 Wireless LAN PCI adapter is referred to as the ZyAIR in this guide.
- The ZyAIR G-300 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](http://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](mailto: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

|  |   |   |
|--|---|---|
| <br>Wireless Access Point | <br>Computer | <br>Notebook computer |
| <br>Server                | <br>Modem    | <br>Wireless Signal    |
| <br>Telephone             | <br>Switch   | <br>Router            |

# Chapter 1

## Getting Started

*This chapter prepares you to using the ZyAIR Utility.*

### 1.1 About Your ZyAIR G-300

The ZyAIR G-300 is an IEEE 802.11g compliant wireless LAN adapter. With the ZyAIR, you can enjoy the wireless mobility within the coverage area.

The following lists the main features of your ZyAIR.

- Your ZyAIR can communicate with other IEEE 802.11b/g compliant wireless devices.
- Automatic rate selection.
- Offers 64-bit and 128-bit WEP (Wired Equivalent Privacy) data encryption for network security.
- Supports IEEE 802.1x and WPA (Wi-Fi Protected Access)
- Low CPU utilization allowing more computer system resources for other programs.
- A built-in antenna
- Plug-and-play installation for Windows ME, Windows 2000 and Windows XP.
- Driver and utility support for Windows 98 Second Edition, Windows ME, Windows 2000 and Windows XP.

### 1.2 ZyAIR Hardware and Utility Installation

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

### 1.3 Configuration Methods

To configure your ZyAIR, use one of the following applications:

- Wireless Zero Configuration (WZC) (recommended for Windows XP)
- ZyAIR Utility
- Odyssey Client Manager

**DO NOT use the Windows XP configuration tool or the Odyssey Client Manager and the ZyAIR Utility at the same time.**

**The bundled Odyssey Client Manager only works for your ZyAIR. Do NOT use the Odyssey Client Manager to configure non-ZyXEL WLAN adapters.**

Refer to the Odyssey Client Manager documentation for more information.

## 1.4 Windows XP Users Only

You must disable WZC if you want to use the ZyAIR utility. Refer to the appendices on how to deactivate WZC or how to use WZC to manage the ZyAIR.

## 1.5 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 1-1 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   |
|--------|---|
| Blue   | The ZyAIR is connected to a wireless network.                                     |
| Yellow | The ZyAIR has a weak connection to a wireless network.                            |
| Red    | The ZyAIR is working properly but is not connected to any AP or wireless station. |

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 radio frequency used by a wireless device is called a channel.

#### 2.1.2 SSID

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

#### 2.1.3 Transmission Rate

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

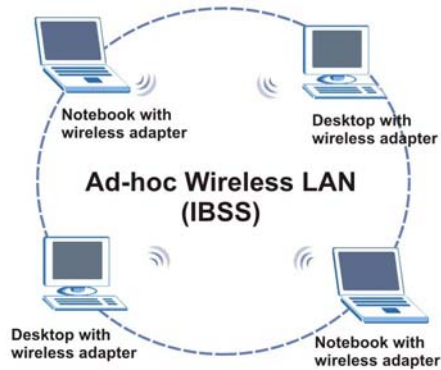
#### 2.1.4 Wireless Network Application

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

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

##### **Ad-Hoc (IBSS)**

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

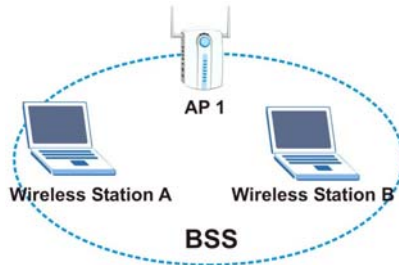


**Figure 2-1 Ad-hoc Network Example**

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

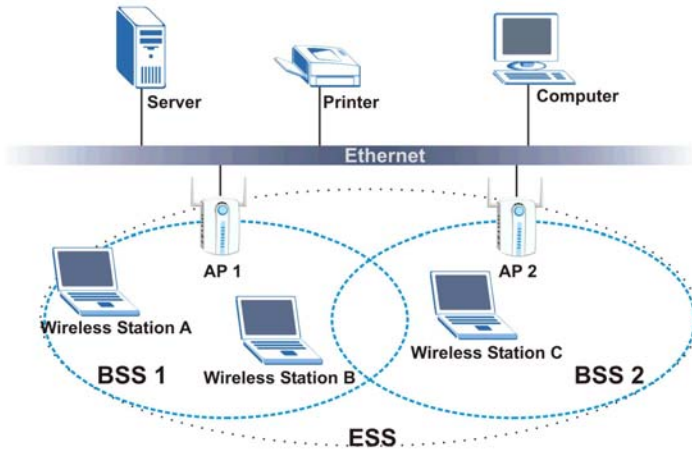
### Infrastructure

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.

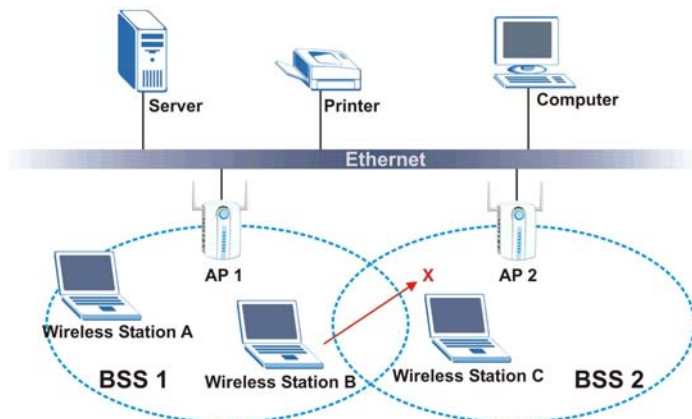


**Figure 2-3 Infrastructure Network Example**

### 2.1.5 Roaming

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

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



**Figure 2-4 Roaming Example**

## 2.1.6 Profile

The Profile function allows you to save the wireless network settings in this screen, use one of the pre-configured network profiles or reset the settings in this screen to the factory default values.

## 2.1.7 Threshold Controls

### Fragmentation Threshold

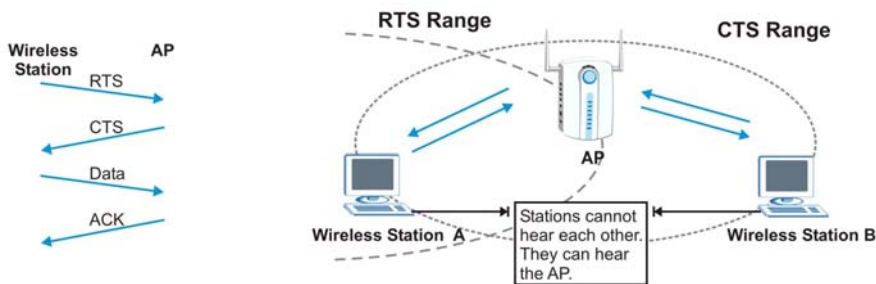
A fragmentation threshold is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyAIR will fragment the packet into smaller data frames.

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

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

### RTS Threshold

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



**Figure 2-5 RTS Threshold**

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

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

When a data frame exceeds the **RTS Threshold** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to

send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

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

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

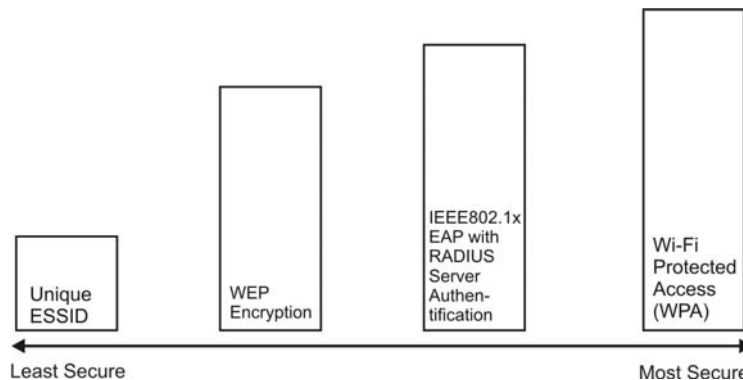
If the **RTS Threshold** value is greater than the **Frag Threshold** value, then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS Threshold** size.

**Enabling the RTS threshold causes redundant network overhead that may affect throughput performance.**

## 2.2 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 2-6 Wireless LAN Security Levels**

Configure the wireless LAN security using the **Profile Security Settings** screen. If you do not enable any wireless security on your ZyAIR, the ZyAIR's wireless communications are accessible to any wireless networking device that is in the coverage area.

## Data Encryption with WEP

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

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

### 2.2.1 Authentication Mode

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

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

### 2.2.2 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 IEEE 802.1x 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-PEAP and LEAP. Refer to the *Types of EAP Authentication* appendix for descriptions.

For EAP-TLS authentication type, 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.

### 2.2.3 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), IEEE 802.1x and Advanced Encryption Standard (AES).

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.

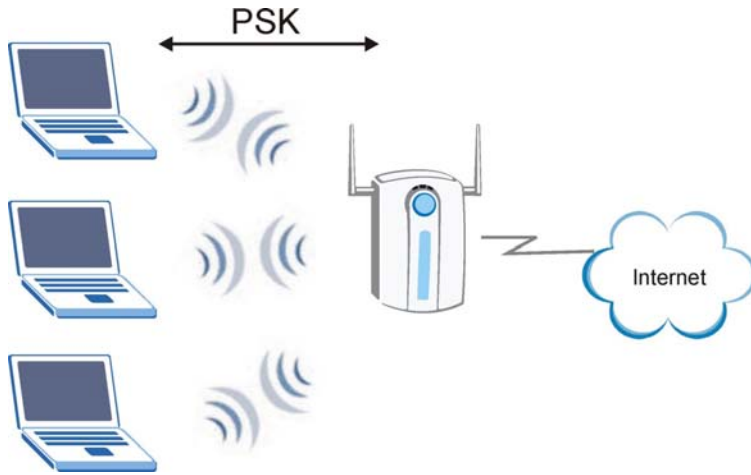
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement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

Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data

### **2.2.4 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) 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 2-7 WPA-PSK Authentication**

### 2.2.5 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.



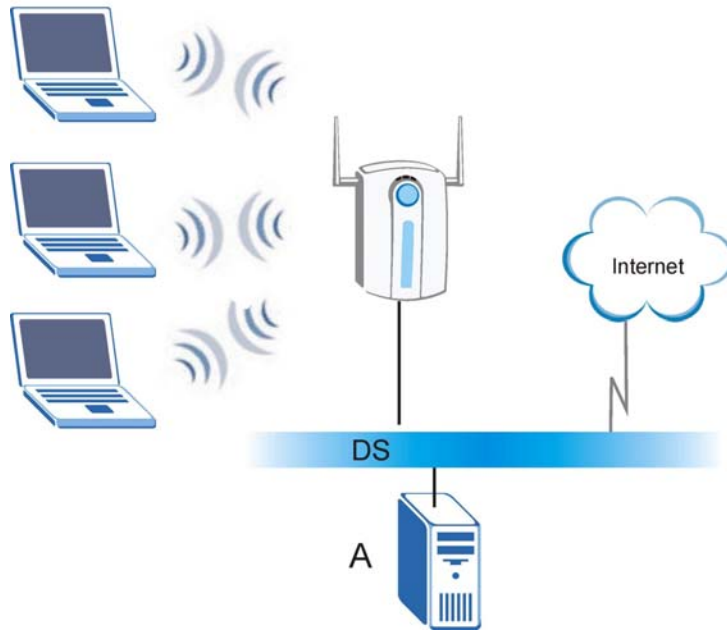
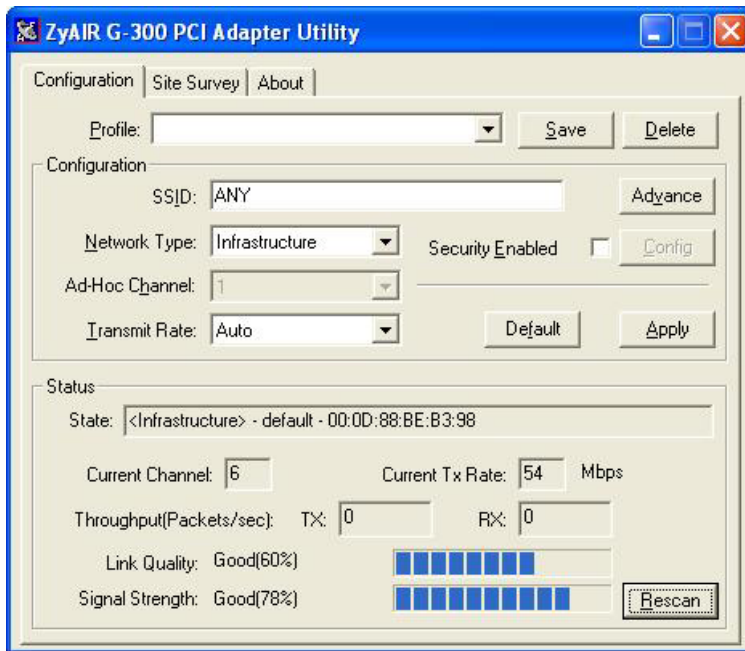


Figure 2-8 WPA with RADIUS Application Example

## 2.3 The Configuration Screen

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



**Figure 2-9 Configuration**

The following table describes the labels in this screen.

**Table 2-1 Configuration**

| LABEL         | DESCRIPTION   |
|---------------|---|
| Profile       | This field displays the name of a predefined profile.<br>To use a previously saved network profile, select the profile file name from the drop-down list box. Once you activate a profile, the ZyAIR Utility will use that profile the next time it is started. If you do not activate a profile, the ZyAIR Utility reverts to use the default profile. |
| Save          | Enter a descriptive name in the <b>Profile</b> field and click <b>Save</b> to save the current configuration settings this screen.  |
| Delete        | Select a profile from the drop-down list box and click <b>Delete</b> to remove the selected profile.  |
| Configuration |   |

Table 2-1 Configuration

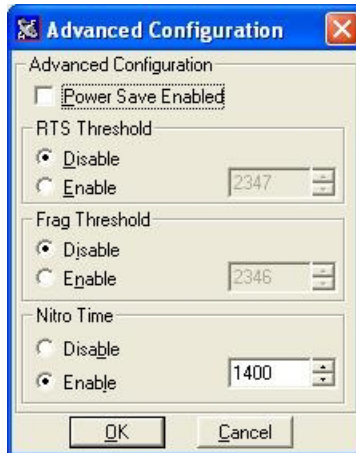
| LABEL                 | DESCRIPTION   |
|-----------------------|---|
| SSID                  | Enter the SSID (Service Set Identifier) of the AP or the peer ad-hoc computer to which you want to associate. To associate to an ad-hoc network, you must enter the same SSID as the peer ad-hoc computer.<br>Enter "any" to associate to or roam between any infrastructure wireless networks. |
| Advanced              | Click <b>Advanced</b> to display the <b>Advanced Configuration</b> screen. Refer to <i>Section 2.3.1</i> .  |
| Network Type          | Select <b>Infrastructure</b> or <b>Ad-Hoc</b> from the drop-down list box.<br>Select <b>Infrastructure</b> to associate to an AP.<br>Select <b>Ad-Hoc</b> to associate to a peer ad-hoc computer.<br>Refer to <i>Section 2.1.4</i> for more information.  |
| WEP Enabled           | The WEP keys are used to encrypt data before transmitting.<br>Select this check box to activate WEP encryption. Refer to <i>Section 2.2</i> for more information.   |
| Ad-Hoc Channel        | This field is activated if you select <b>Ad-Hoc</b> in the <b>Network Type</b> field.<br>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.  |
| Transmit Rate         | Select a transmission rate from the drop-down list box. The default is <b>Auto</b> .  |
| Default               | Click <b>Default</b> to return the field settings under <b>Configuration</b> back to the factory defaults.  |
| Apply                 | Click <b>Apply</b> to save and activate the field settings under <b>Configuration</b> .   |
| Status                |   |
| State                 | This field displays the type of wireless network and the name and MAC address of the wireless device to which the ZyAIR is connected.   |
| Current Channel       | This field displays the radio channel the ZyAIR is currently using.   |
| Current Tx Rate       | This field displays the current transmission rate of the ZyAIR in megabits per second.  |
| Throughput (byte/sec) |   |
| TX                    | This field displays the number of data frames transmitted.  |
| RX                    | This field displays the number of data frames received.   |
| Link Quality          | The status bar and the percentage number show the quality of the signal.  |

**Table 2-1 Configuration**

| LABEL         | DESCRIPTION  |
|---------------|--|
| Link Strength | The status bar and the percentage number or a number in dBm show the strength of the signal.                         |
| Rescan        | Click <b>Rescan</b> to re-establish connection to the wireless device whose SSID is shown in the <b>State</b> field. |

### 2.3.1 The Advanced Configuration Screen

In the **Configuration** screen, click **Advanced** to display the pop-up screen as shown.



**Figure 2-10 Configuration: Advanced**

The following table describes the labels in this screen.

**Table 2-2 Configuration: Advanced**

| LABAL             | DESCRIPTION   |
|-------------------|---|
| Power Save Enable | Select this check box to reduce power consumption (especially for laptop computers). This forces the ZyAIR to go to sleep mode when it is not transmitting data. <div style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin-top: 10px; text-align: center;"> <b>This only works if the wireless device to which the ZyAIR is connected also supports this feature.</b> </div> |

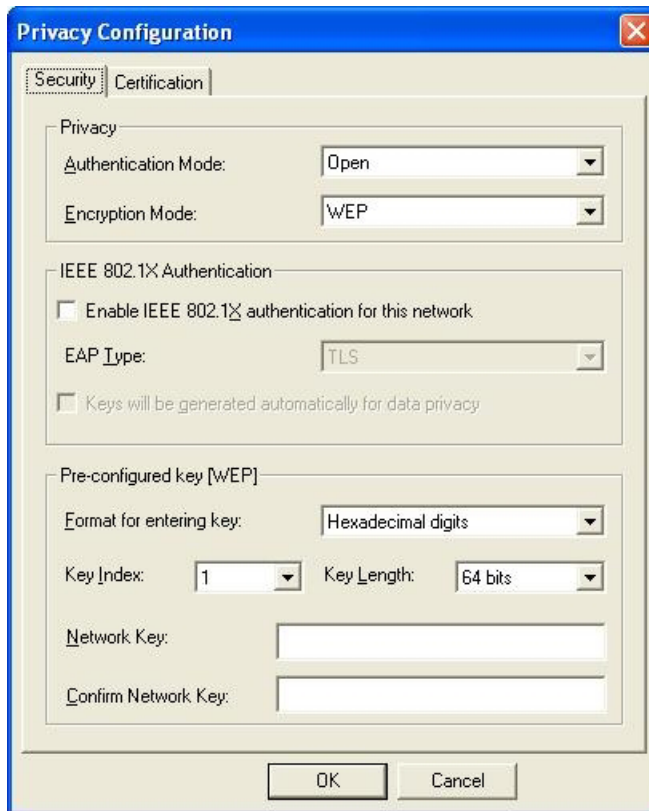
**Table 2-2 Configuration: Advanced**

| LABEL          | DESCRIPTION  |
|----------------|--|
| RTS Threshold  | Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. |
| Frag Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.   |
| Nitro Time     | This is the time interval (in usec) between packet bursts. This allows your ZyAIR to operate in a network with IEEE802.11b wireless LAN devices and still take advantage of higher transmission rates with IEEE802.11g standard.   |
| OK             | Click <b>OK</b> to save the settings.  |
| Cancel         | Click <b>Cancel</b> to discard all changes and close this screen.  |

### 2.3.2 The Security Screen

You can configure the ZyAIR to connect to a network with wireless security. In the **Configuration** screen, select **WEP Enable** and click **Edit**. A **Security** screen displays as shown.

Field choices vary depending on what encryption method or authentication mode you select in this screen. Refer to *Section 2.2.1* and *Section 2.2.3* for more information.



**Figure 2-11 Configuration: Privacy Configuration: Security**

The following table describes the labels in this screen.

**Table 2-3 Configuration: Privacy Configuration: Security**

| LABEL                      | DESCRIPTION   |
|----------------------------|---|
| Privacy                    |   |
| Authentication Mode        | Select an authentication mode. Choices are <b>Open</b> , <b>Share</b> , <b>WPA</b> and <b>WPA-PSK</b> . |
| Encryption Mode            | Select an encryption method. Choices are <b>WEP</b> , <b>TKIP</b> and <b>AES</b> .                      |
| IEEE 802.1X Authentication |   |

**Table 2-3 Configuration: Privacy Configuration: Security**

| LABEL  | DESCRIPTION  |
|--|--|
| Enable IEEE 802.1X Authentication for this network     | Select this checkbox to enable IEEE 802.1X authentication to log into the network.   |
| EAP Type   | Select an EAP type. Choices are <b>TLS</b> , <b>PEAP</b> and <b>LEAP</b> .   |
| Keys will be generated automatically for data privacy. | Select this checkbox to allow the ZyAIR to obtain the security keys from an authentication server (the RADIUS server). The authentication server automatically generates the security keys.  |
| Pre-configured Key (WEP)                               | Set the following fields when you select <b>WEP</b> in the <b>Encryption Mode</b> field.   |
| Format for entering key                                | Specify the key format. Select either <b>hexadecimal digits</b> or <b>characters</b> .   |
| Key Index  | Select the number (1 to 4) of a key you wish to configure.   |
| Key Length   | Specify the key length. Select <b>64 bits</b> or <b>128 bits</b> .   |
| Network Key  | <p>Enter the WEP keys in the fields provided.</p> <p>If you select <b>64 bits</b> in the <b>Key Length</b> field.</p> <ul style="list-style-type: none"> <li>♦ Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (e.g. 11AA22BB33) for HEX key type</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>♦ Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (e.g. MyKey) for ASCII key type.</li> </ul> <p>If you select <b>128 bits</b> in the <b>Key Length</b> field,</p> <ul style="list-style-type: none"> <li>♦ Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>♦ Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type.</li> </ul> <div style="border: 1px solid black; background-color: #cccccc; padding: 5px; text-align: center; margin-top: 10px;"> <p><b>ASCII WEP keys are case sensitive.</b></p> <p><b>Select a WEP key to use for data encryption.</b></p> </div> |
| Confirm Network Key                                    | Enter the key again for confirmation.  |
| Pre-Shared Key (WPA)                                   | Set the following fields when you select <b>WPA-PSK</b> in the <b>Encryption Mode</b> field.   |

**Table 2-3 Configuration: Privacy Configuration: Security**

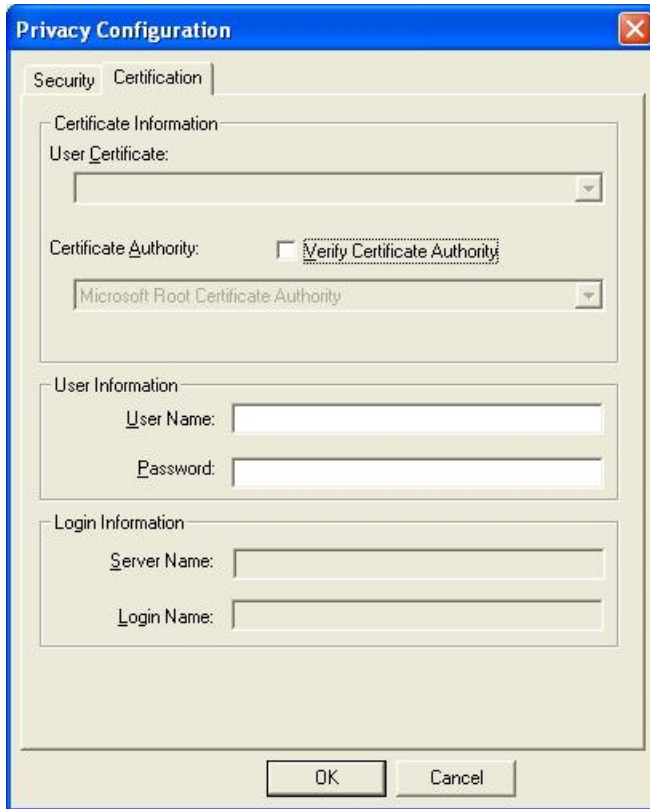
| LABEL               | DESCRIPTION   |
|---------------------|---|
| Network Key         | Enter the pre-shared key (PSK) or passphrase from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| Confirm Network Key | Enter the PSK again for confirmation.   |
| OK                  | Click <b>OK</b> to save the changes.  |
| Cancel              | Click <b>Cancel</b> to discard all changes and close the screen.  |

### 2.3.3 The Certificate Screen

If you set the ZyAIR to use an EAP type (**TLS**, **PEAP** or **LEAP**), configure the **Certificate** screen.

Click the **Certificate** tab in the **Privacy Configuration** screen to display the screen as shown.





**Figure 2-12 Configuration: Privacy Configuration: Certification**

The following table describes the labels in this screen.

**Table 2-4 Configuration: Privacy Configuration: Certification**

| LABEL                   | DESCRIPTION  |
|-------------------------|--|
| Certificate Information | Specify the certificate(s) in the fields.<br><div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>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.</b></p> </div> |
| User Certificate        | This field is applicable for TLS authentication mode.<br>Select a certificate you have enrolled.   |

**Table 2-4 Configuration: Privacy Configuration: Certification**

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| Certificate Authority     | This field is applicable for PEAP and TLS authentication modes.<br>Select a certificate authority.    |
| Verify Server Certificate | Select the check box to check the certificate of the authentication server.                           |
| User Information          | These fields are applicable for LEAP and PEAP authentication modes.                                   |
| User Name                 | Enter the user name.<br>This is the user name that you or an administrator set up on a RADIUS server. |
| Password                  | Enter the password associated with the user name above.   |
| Login Information         | These fields are applicable for PEAP and TLS authentication modes.                                    |
| Server Name               | Enter the name of the RADIUS server.  |
| Login Name                | Enter the user name.<br>This is the user name that you or an administrator set up on a RADIUS server. |
| OK                        | Click <b>OK</b> to save the changes.  |
| Cancel                    | Click <b>Cancel</b> to discard all changes and close the screen.                                      |

## 2.4 The Site Survey Screen

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

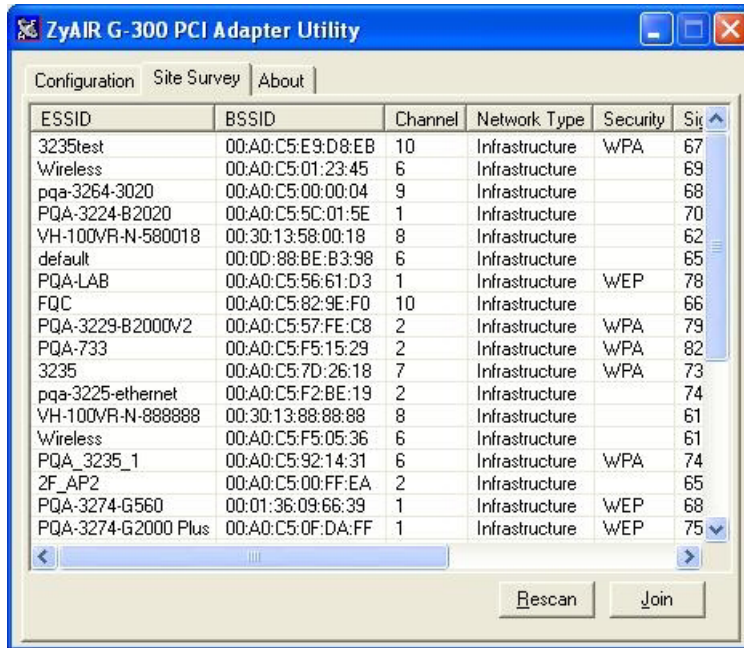


Figure 2-13 Site Survey

The following table describes the labels in the table.

Table 2-5 Site Survey

| LABEL        | DESCRIPTION  |
|--------------|--|
| ESSID        | This field displays the SSID (or name) of each wireless device.  |
| BSSID        | This field displays the MAC address of the wireless device.  |
| Channel      | This field displays the channel number used by each wireless device.   |
| Network Type | This field displays the wireless network type ( <b>Infrastructure</b> or <b>Ad Hoc</b> ) of the wireless device. |
| Security     | This field shows whether the data encryption or user authentication is activated or inactive.                    |
| Signal       | This field displays the signal strength of each wireless device in percentage.                                   |
| Rates        | This field displays the transmission rates the wireless device supports.   |
| Rescan       | Click <b>Rescan</b> to scan for available wireless device(s) within transmission range.                          |

**Table 2-5 Site Survey**

| LABEL | DESCRIPTION   |
|-------|---|
| Join  | Click <b>Join</b> to associate to the selected wireless device. |

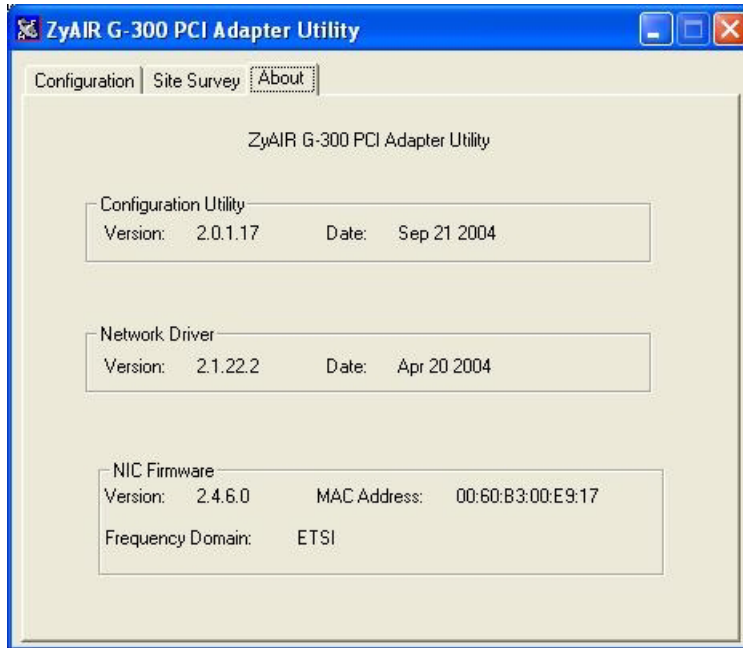
### 2.4.1 Connecting to a Network

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

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 **Security** field is **WEP** or **WPA** for the selected wireless network, you must also set up network security in the **Privacy Configuration** screens. Refer to *Section 2.3.2* and *Section 2.3.3* for more information.
4. Verify that you have successfully connected to the selected network and check the network information in the **Configuration** screen.

## 2.5 The About Screen

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



**Figure 2-14 ZyAIR Utility: About**

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

**Table 2-6 ZyAIR Utility: About**

| FIELD                         | DESCRIPTION  |
|-------------------------------|--|
| Configuration Utility Version | This field displays the version number of the ZyAIR Utility.   |
| Network Driver Version        | This field displays the version number of the Windows driver for the ZyAIR.  |
| NIC Firmware Version          | This field displays the firmware version and the MAC address of the ZyAIR.   |
| Frequency Domain              | This field displays the regional code. This field displays <b>MKK</b> (Japan), <b>ETSI</b> (Europe) or <b>FCC</b> (North America).<br>If you set your ZyAIR in Ad-Hoc mode, this field displays <b>FCC</b> . |



# 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. Close and exit the ZyAIR Utility.
2. Click **Start, (all) Programs, ZyAIR G-300 PCI Adapter Utility, Uninstall ZyAIR G-300 Adapter Utility**.
3. When prompted, click **OK** to remove the driver and the utility software.



**Figure 3-1 Confirm Uninstallation**

4. Click **Finish** and restart the 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.
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 <b>Device Manager</b> to check for possible hardware conflicts. Click <b>Start, Settings, Control Panel, System, Hardware</b> and <b>Device Manager</b> . Verify the status of the ZyAIR under <b>Network Adapter</b> . (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 authentication and encryption mode. Verify the settings in the <b>Privacy Configuration</b> screens.</p> |

**Table 4-2 Troubleshooting Communication Problems**

| <b>PROBLEM</b> | <b>CORRECTIVE ACTION</b>   |
|----------------|--|
| 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 computer and the AP shares the same authentication and encryption mode. Verify the settings in the <b>Privacy Configuration</b> screens..</p> |

### 4.3 Problem with the Link Status

**Table 4-3 Troubleshooting Link Quality**

| <b>PROBLEM</b>  | <b>CORRECTIVE ACTION</b>  |
|---|---|
| The link quality and/or signal strength is poor all the time. | <p>Search and connect to another AP with a better link quality using the <b>Site Survey</b> screen.</p> <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> |

# Appendix A

## Disable Windows XP Wireless LAN Configuration Tool

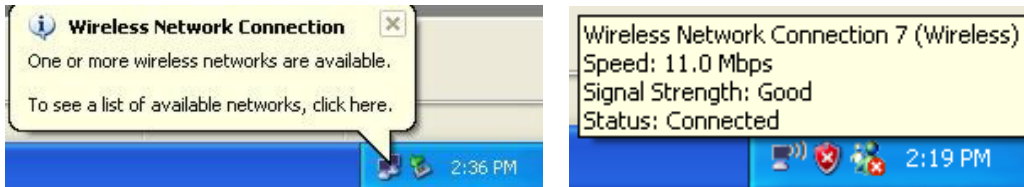
Windows XP includes a configuration tool (also known as Wireless Zero Configuration (WZC)) for wireless devices.

Follow the steps below to disable the configuration tool in Windows XP after you install the ZyAIR Utility. The screen varies depending on the version of Windows XP service pack.

### Via the Wireless Network System Tray Icon

If the network icon for wireless connections is not present in the system tray, see the next section.

1. Double-click the network icon for wireless connections in the system tray.



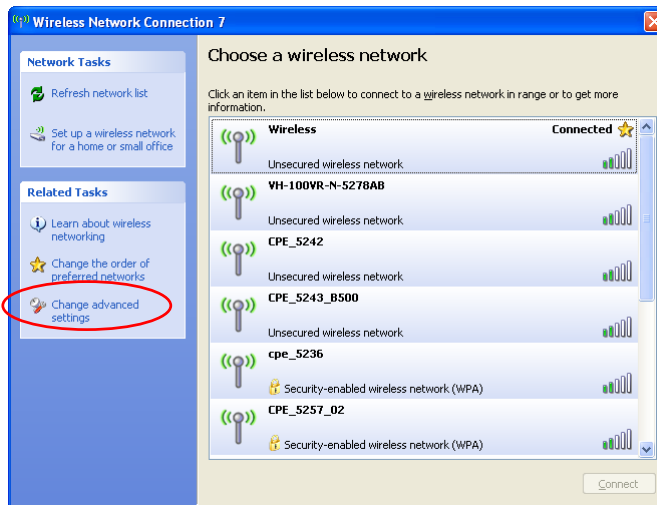
**Diagram 1 Windows XP: System Tray Icon**

2. Windows XP SP1: When a **Wireless Network Connection** window displays, click **Advanced....**



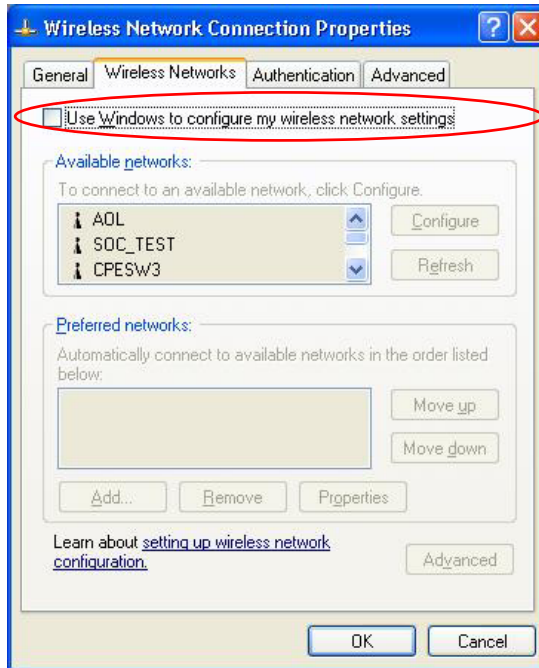
**Diagram 2 Windows XP SP1: Wireless Network Connection**

- Windows XP SP2: When a **Wireless Network Connection** window displays, click **Change advanced settings** under **Related Tasks** and then the **Wireless Networks** tab.

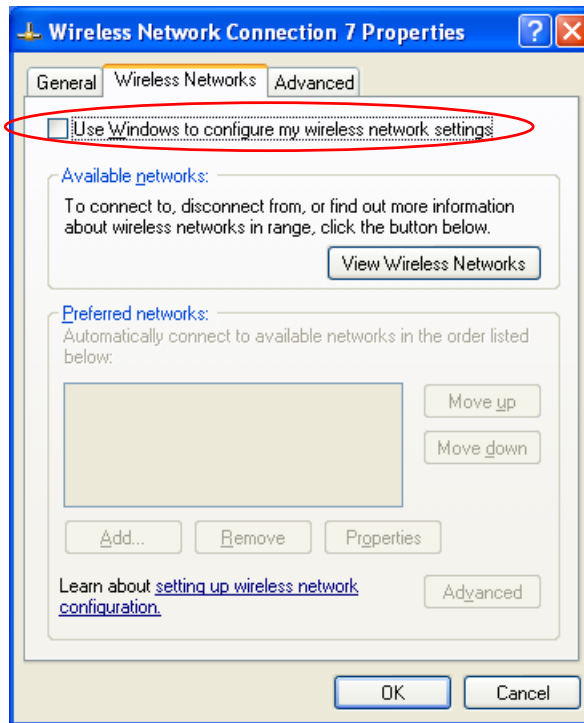


**Diagram 3 Windows XP SP2: Wireless Network Connection**

3. 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**.



**Diagram 4 Windows XP SP1: Wireless Network Connection Properties**



**Diagram 5 Windows XP SP2: Wireless Network Connection Properties**

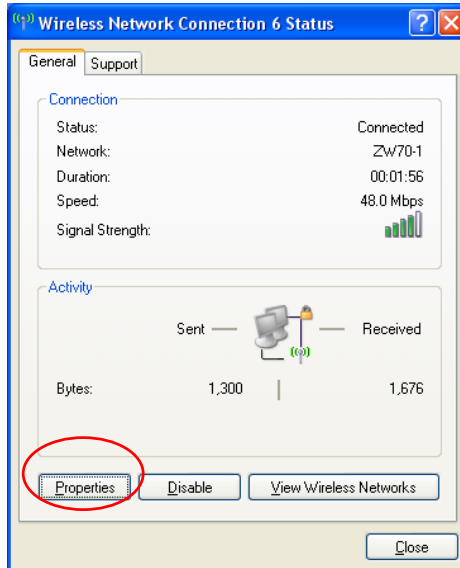
**Via the Control Panel**

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

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



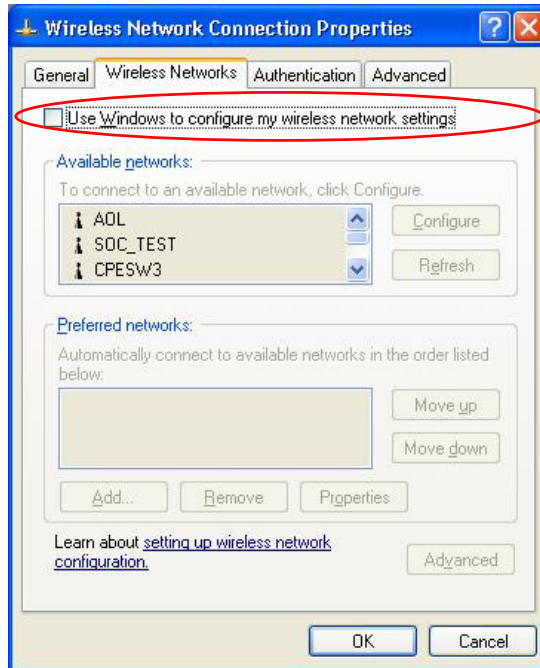
**Diagram 6 Windows XP SP1: Wireless Network Connection Status**



**Diagram 7 Windows XP SP2: Wireless Network Connection Status**

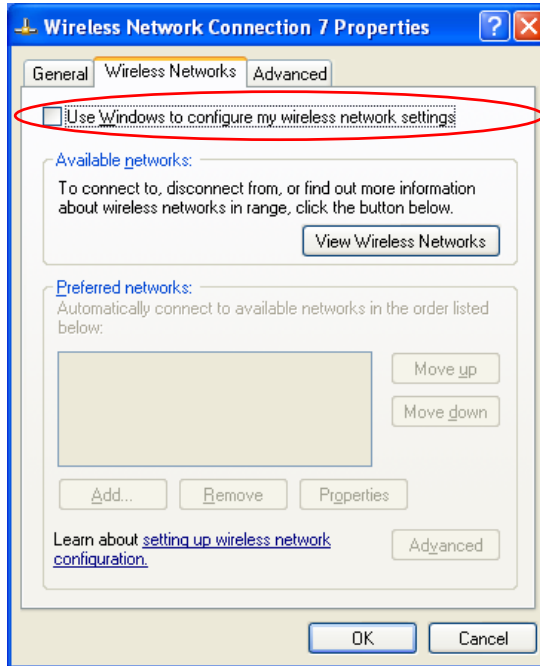
3. Click **Properties** and click the **Wireless Networks** tab.

4. 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**.



**Diagram 8 Windows XP SP1: Wireless Network Connection Properties**





**Diagram 9 Windows XP SP2: Wireless Network Connection Properties**




# Appendix B

## Management with Wireless Zero Configuration

*This appendix shows you how to manage your ZyAIR using the Windows XP wireless configuration tool.*

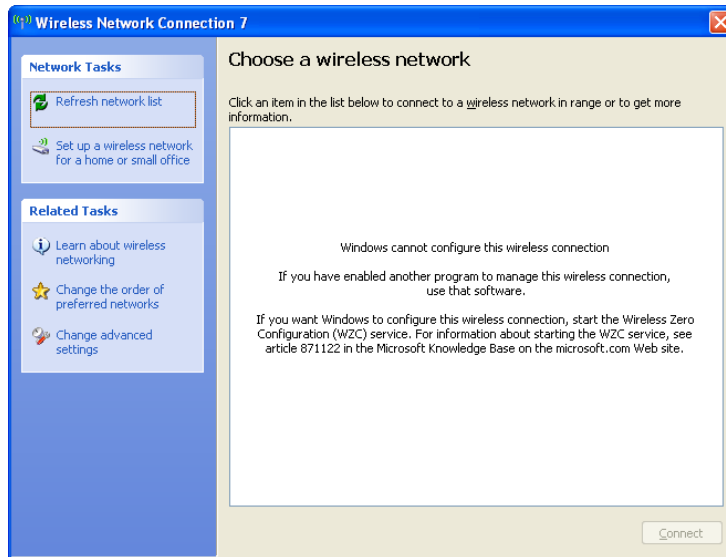
Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon (  ) in most screens, move the cursor to the item that you want the information about and click to view the help.

### Activating Wireless Zero Configuration

Make sure the **Use Windows to configure my wireless network settings** check box is selected in the **Wireless Network Connection Properties** screen. Refer to *Appendix A*.

If you see the following screen, refer to article 871122 on the Microsoft web site for information on starting WZC.



**Diagram 10 Windows XP SP2: WZC Not Available**

## Connecting to a Wireless Network





1. Double-click the network icon for wireless connections in the system tray to open the **Wireless Network Connection Status** screen.



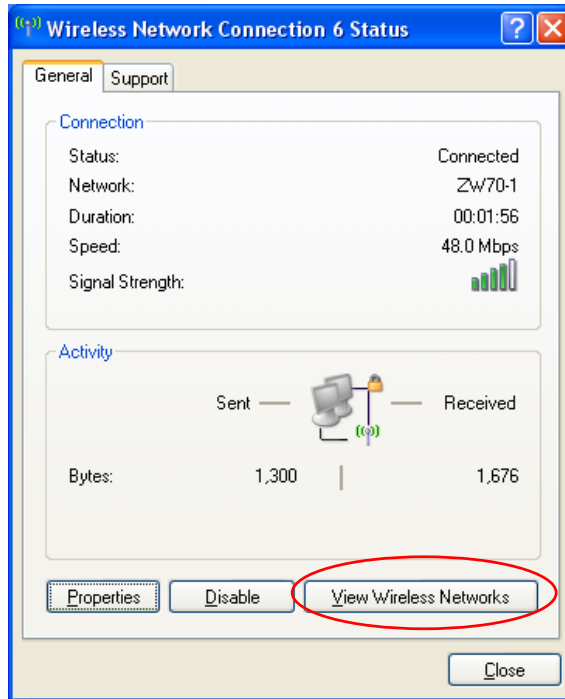
**Diagram 11 Windows XP SP2: System Tray Icon**

The type of the wireless network icon in Windows XP SP2 indicates the status of the ZyAIR. Refer to the following table for details.

**Chart 1 Windows XP SP2: System Tray Icon**

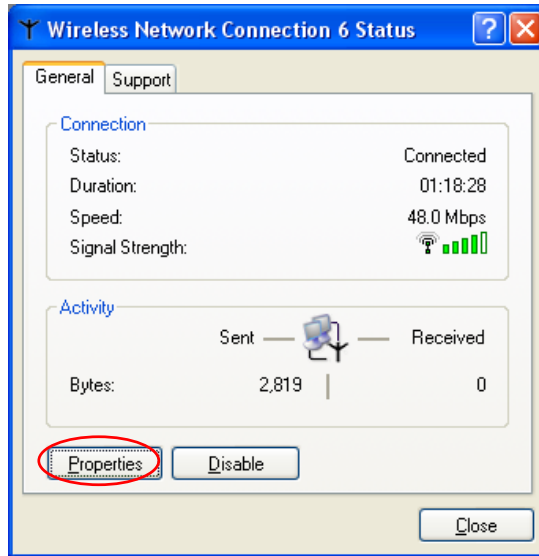
| ICON   | DESCRIPTION   |
|--|---|
|  | The ZyAIR is connected to a wireless network.   |
|  | The ZyAIR is in the process of connecting to a wireless network.  |
|  | The connection to a wireless network is limited because the network did not assign a network address to the computer. |
|  | The ZyAIR is not connected to a wireless network.   |

2. Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.



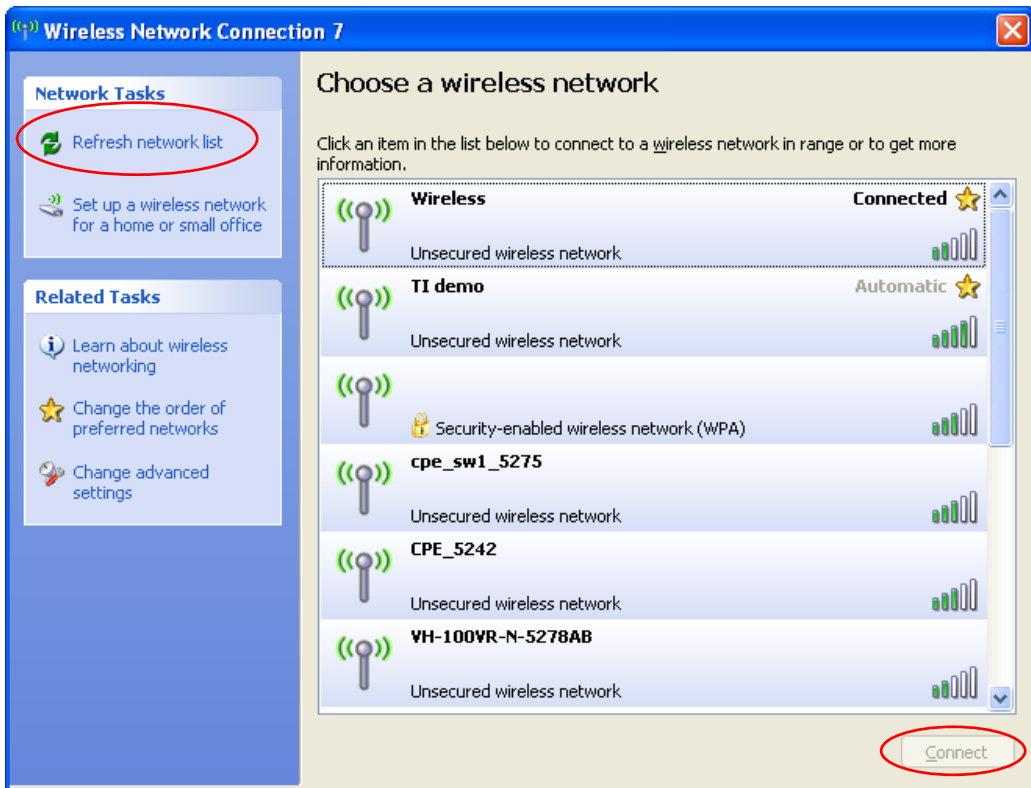
**Diagram 12 Windows XP SP2: Wireless Network Connection Status**

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.



**Diagram 13 Windows XP SP1: Wireless Network Connection Status**




3. Windows XP SP2: Click **Refresh network list** to reload and search for available wireless devices within transmission range. Select a wireless network in the list and click **Connect** to join the selected wireless network.



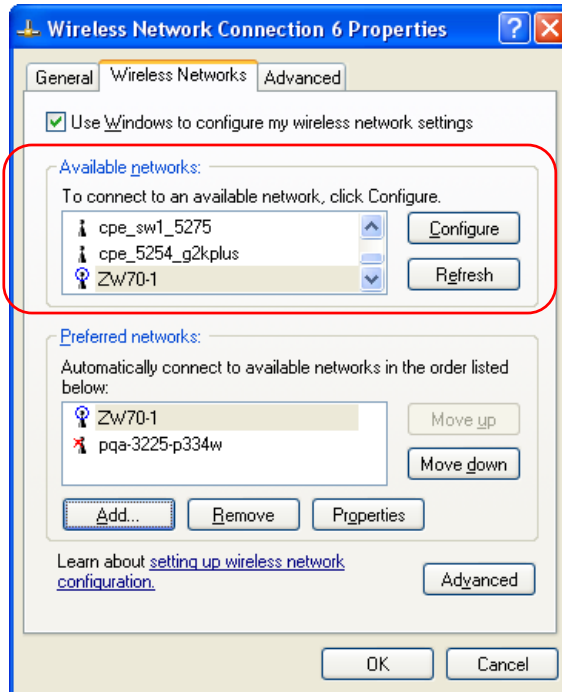
**Diagram 14 Windows XP SP2: Wireless Network Connection**

The following table describes the icons in the wireless network list.

**Chart 2 Windows XP SP2: Wireless Network Connection**

| ICON  | DESCRIPTION   |
|---|---|
|  | This denotes that the wireless security is activated for the wireless network.  |
|  | This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the ZyAIR tries to associate to the preferred network first in the order that you specify. Refer to the section on security settings for detailed information. |
|  | This denotes the signal strength of the wireless network.<br>Move your cursor to the icon to see details on the signal strength.  |

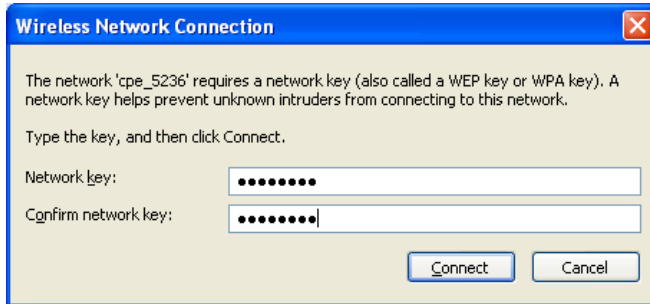
Windows XP SP1: Click **Refresh** to reload and search for available wireless devices within transmission range. Select a wireless network in the **Available networks** list, click **Configure** and set the related fields to the same security settings as the associated AP to add the selected network into the **Preferred networks** table. Click **OK** to join the selected wireless network. Refer to the section on security settings (discussed later) for more information.



**Diagram 15 Windows XP SP1: Wireless Network Connection Properties**

4. Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP. Refer to the section on security settings (discussed later) for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption. If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.





**Diagram 16 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK**






**Diagram 17 Windows XP SP2: Wireless Network Connection: No Security**

5. Verify that you have successfully connected to the selected network and check connection status in the wireless network list or the connection icon in the **Preferred networks** or **Available networks** list.

The following table describes the connection icons.

**Chart 3 Windows XP: Wireless Networks**

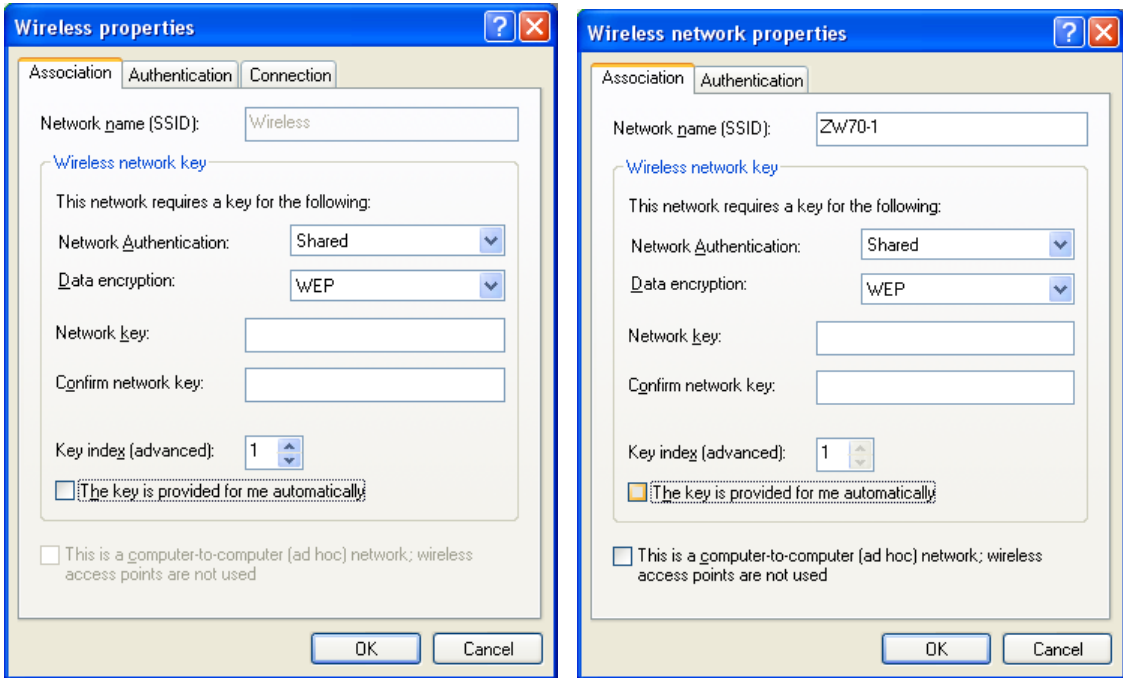
| ICON  | DESCRIPTION   |
|---|---|
|  | This denotes the wireless network is an available wireless network. |
|  | This denotes the ZyAIR is associated to the wireless network.       |
|  | This denotes the wireless network is not available.                 |

## Security Settings

When you configure ZyAIR to connect to a secure network but the security settings are not yet enabled on the ZyAIR, you will see different screens according to the authentication and encryption methods used by the selected network.

## Association

Select a network in the **Preferred networks** list and click **Properties** to view or configure security.



**Diagram 18 Windows XP: Wireless (network) properties: Association**

The following table describes the labels in this screen.

**Chart 4 Windows XP: Wireless (network) properties: Association**

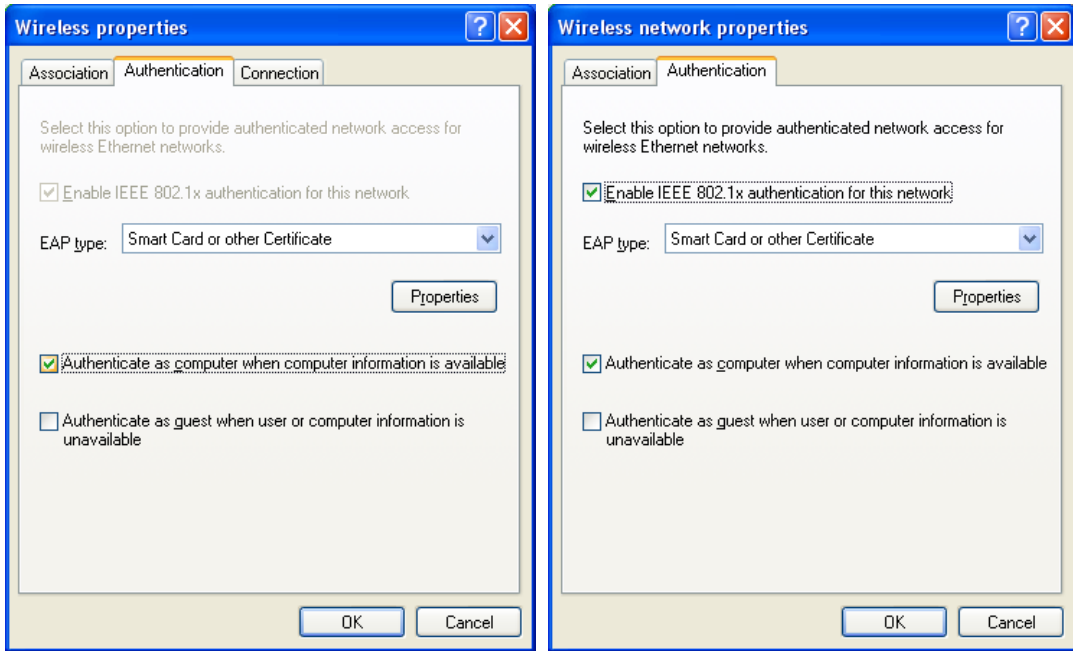
| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Network name (SSID)    | This field displays the SSID (Service Set Identifier) of each wireless network.   |
| Network Authentication | This field automatically shows the authentication method ( <b>Share</b> , <b>Open</b> , <b>WPA</b> or <b>WPA-PSK</b> ) used by the selected network.<br>Refer to <i>Section 0</i> for more information. |
| Data Encryption        | This field automatically shows the encryption type ( <b>TKIP</b> , <b>WEP</b> or <b>Disable</b> ) used by the selected network.   |
| Network Key            | Enter the passphrase, pre-shared key or WEP key.<br>The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN.   |

**Chart 4 Windows XP: Wireless (network) properties: Association**

| LABEL  | DESCRIPTION  |
|--|--|
| Confirm network key  | Enter the key again for confirmation.  |
| Key index (advanced)   | Select a default WEP key to use for data encryption. This field is available only when the network use <b>WEP</b> encryption method and the <b>The key is provided for me automatically</b> check box is not selected. |
| The key is provided for me automatically   | If this check box is selected, the wireless AP assigns the ZyAIR a key.  |
| This is a computer-to-computer (ad hoc) network; wireless access points are not used | If this check box is selected, you are connecting to another computer directly.  |
| OK   | Click <b>OK</b> to save your changes.  |
| Cancel   | Click <b>Cancel</b> to leave this screen without saving any changes you may have made.   |

**Authentication**

Click the **Authentication** tab in the **Wireless (network) properties** screen to display the screen shown next. The fields on this screen are grayed out when the network is in Ad-Hoc mode or data encryption is disabled.



**Diagram 19 Windows XP: Wireless (network) properties: Authentication**

The following table describes the labels in this screen.

**Chart 5 Windows XP: Wireless (network) properties: Authentication**

| LABEL   | DESCRIPTION   |
|---|---|
| Enable IEEE 802.1x authentication for this network              | This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to <b>Open</b> in the previous screen, you can choose to disable or enable this feature. |
| EAP Type  | Select the type of EAP authentication. Options are <b>Protected EAP (PEAP)</b> and <b>Smart Card or other Certificate</b> .   |
| Properties  | Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the <b>EAP type</b> field.  |
| Authenticate as computer when computer information is available | Select this check box to have the computer send its information to the network for authentication when a user is not logged on.   |

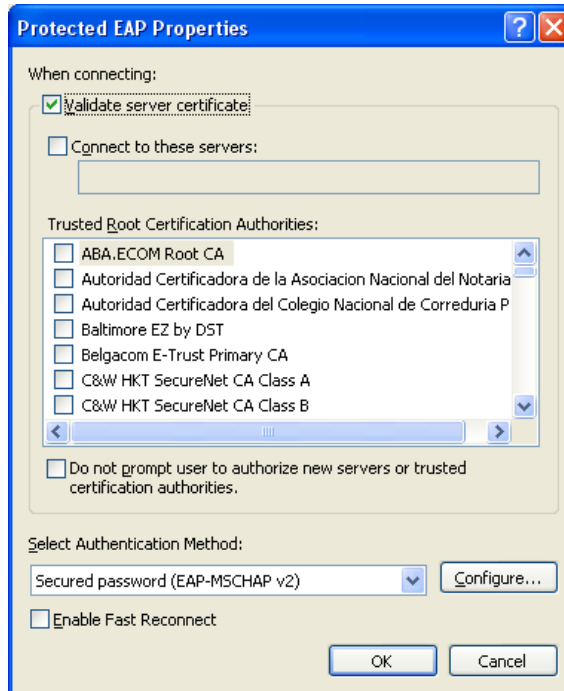
**Chart 5 Windows XP: Wireless (network) properties: Authentication**

| LABEL  | DESCRIPTION  |
|--|--|
| Authenticate as guest when user or computer information is unavailable | Select this check box to have the computer access to the network as a guest when a user is not logged on or computer information is not available. |
| OK   | Click <b>OK</b> to save your changes.  |
| Cancel   | Click <b>Cancel</b> to close this screen without saving any changes you may have made.   |

### Authentication Properties

Select an EAP authentication type in the **Wireless (network) properties: Authentication** screen and click the **Properties** button to display the following screen.

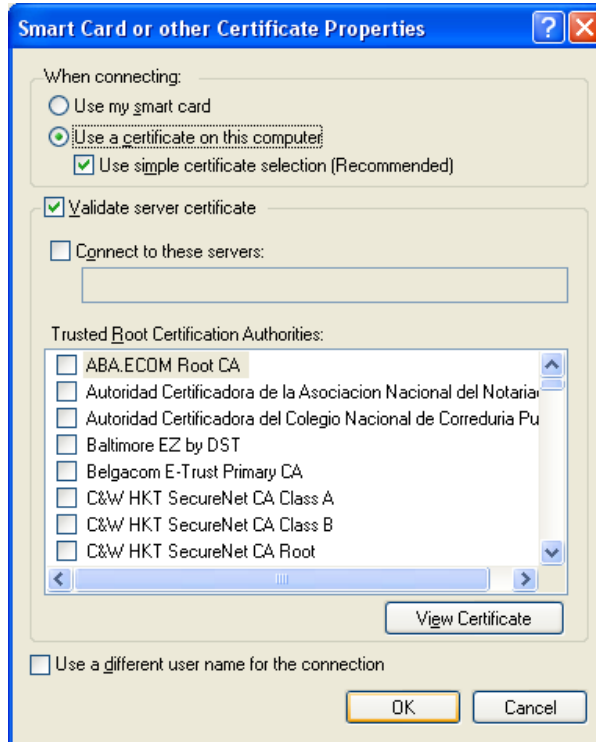
#### *Protected EAP Properties*

**Diagram 20 Windows XP: Protcted EAP Properties**

The following table describes the labels in this screen.

**Chart 6 Windows XP: Protected EAP Properties**

| LABEL  | DESCRIPTION  |
|--|--|
| Validate server certificate  | Select the check box to verify the certificate of the authentication server.   |
| Connect to these servers   | Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.  |
| Trusted Root Certification Authorities:  | Select a trusted certification authority from the list below. <div data-bbox="336 497 1176 598" style="border: 1px solid black; background-color: #e0e0e0; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;"><b>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.</b></p> </div> |
| Do not prompt user to authorize new server or trusted certification authorities. | Select this check box to authorize a new authentication server or trusted CA without prompting.<br>This field is available only if you installed the Windows XP server pack 2.   |
| Select Authentication Method:  | Select an authentication method from the drop-down list box and click <b>Configure</b> to do settings.   |
| Enable Fast Reconnect  | Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down.   |
| OK   | Click <b>OK</b> to save your changes.  |
| Cancel   | Click <b>Cancel</b> to leave this screen without saving any changes you may have made.   |

*Smart Card or other Certificate Properties***Diagram 21 Windows XP: Smart Card or other Certificate Properties**

The following table describes the labels in this screen.

**Chart 7 Windows XP: Smart Card or other Certificate Properties**

| LABEL                              | DESCRIPTION   |
|------------------------------------|---|
| Use my smart card                  | Select this check box to use the smart card for authentication.   |
| Use a certificate on this computer | Select this check box to use a certificate on your computer for authentication.   |
| Validate server certificate        | Select the check box to check the certificate of the authentication server.   |
| Connect to these servers           | Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain. |

**Chart 7 Windows XP: Smart Card or other Certificate Properties**

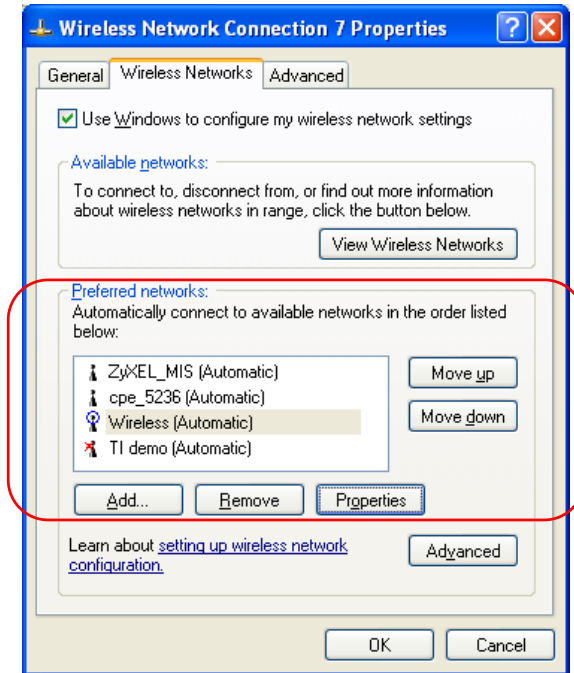
| LABEL   | DESCRIPTION   |
|---|---|
| Trusted Root Certification Authorities:       | Select a trusted certification authority from the list below.<br><div data-bbox="337 316 1176 416" style="border: 1px solid black; background-color: #cccccc; padding: 5px; text-align: center;"><b>You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.</b></div> |
| View Certificate                              | Click this button if you want to verify the selected certificate.   |
| Use a different user name for the connection: | Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to.   |
| OK  | Click <b>OK</b> to save your changes.   |
| Cancel  | Click <b>Cancel</b> to leave this screen without saving any changes you may have made.  |

**Ordering the Preferred Networks**

Follow the steps below to manage your preferred networks.

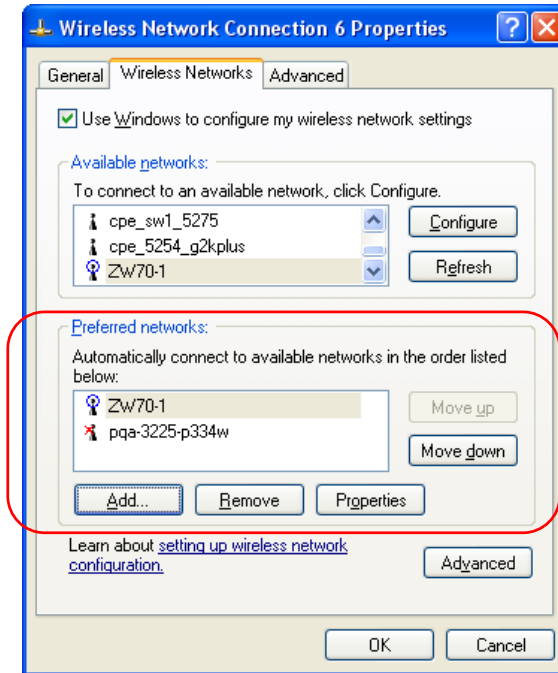
1. Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see *Diagram 14*). The screen displays as shown.





**Diagram 22 Windows XP SP2: Wireless Networks: Preferred Networks**

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the screen as shown.



**Diagram 23 Windows XP SP1: Wireless Networks: Preferred Networks**

2. Whenever the ZyAIR tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or **Move down** to change its order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

# 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 (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**

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

# Appendix D

## Product Specifications

### Product Specifications

|                              |  |
|------------------------------|--|
| <b>Product Name</b>          | ZyAIR G-300 Wireless LAN PCI Adapter   |
| <b>Type</b>                  | 3.3V 32-bit PCI adapter  |
| <b>Standards</b>             | IEEE 802.11b<br>IEEE 802.11g   |
| <b>Network Architectures</b> | Infrastructure<br>Ad-Hoc   |
| <b>Operating Frequencies</b> | 2.412-2.483GHz   |
| <b>Operating Channels</b>    | IEEE 802.11b: 11 Channels (North America)<br>IEEE 802.11g: 11 Channels (North America)<br>IEEE 802.11b: 13 Channels (Europe)<br>IEEE 802.11g: 13 Channels (Europe) |
| <b>Data Rate</b>             | IEEE 802.11b: 11, 5.5, 2, 1Mbps<br>IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps   |
| <b>Modulation</b>            | IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK)<br>IEEE 802.11b: Direct Spread Spectrum (CCK, DQPSK, DBOSK).                |
| <b>Security</b>              | 64/128-bit WEP<br>WPA<br>WPA-PSK<br>IEEE 802.1X (EAP-TLS, PEAP and LEAP)   |
| <b>Operating Temperature</b> | 0 ~ 55 degrees Centigrade  |
| <b>Storage Temperature</b>   | -10 ~ 65 degrees Centigrade  |
| <b>Operating Humidity</b>    | 90% (non-condensing)   |
| <b>Storage Humidity</b>      | 20 ~ 80% (non-condensing)  |
| <b>Power Consumption</b>     | TX: 460mA      RX: 310mA   |
| <b>Voltage</b>               | 3.3V±5%  |

**Product Specifications**

|                  |                           |
|------------------|---------------------------|
| <b>Weight</b>    | <80g                      |
| <b>Dimension</b> | 134mm(L)*121mm(W)*22mm(H) |

# Index

## A

About ..... 2-20  
 Accessing the ZyAIR Utility ..... 1-2  
 AdHoc Channel ..... 2-11  
 authentication ..... 2-19  
 authentication mode ..... 2-14  
 Authentication Mode ..... 2-6  
   Open ..... 2-6  
   Shared..... 2-6  
 automatically key generation ..... 2-15

## B

Basic Service Set ..... See BSS  
 BSS..... 2-2

## C

CA..... Y  
 certificate ..... 2-17  
   server ..... 2-18  
   user ..... 2-17  
 Certificate Authority ..... See CA  
 Certificate Authority (CA)..... 2-18  
 Certificate screen, the..... 2-16  
 Communication Problem ..... 4-1  
   Ad-hoc(IBSS) ..... 4-2  
   Infrastructure ..... 4-1  
 Configuration utility version ..... 2-21  
 Connecting to a Network ..... 2-20  
 Copyright ..... ii  
   Disclaimer ..... ii  
   Trademarks ..... ii  
 CTS (Clear to Send) ..... 2-4, 2-5  
 Customer Support ..... vii

## D

Data encryption..... 2-6  
 Disable Windows XP Wireless Support... 1-1

## E

EAP Authentication  
   MD5..... Y  
   PEAP ..... Y  
   TLS ..... Y  
   TTLS..... Y  
 EAP type ..... 2-15  
 encryption ..... 2-19  
 Encryption ..... 2-7  
 encryption method ..... 2-14  
 ESS..... 2-2  
 Extended Service Set ..... See ESS

## F

Federal Communications Commission  
   (FCC) Interference Statement..... v  
 Frag Threshold..... 2-13  
 Fragmentation Threshold..... 2-4  
 Frequency domain ..... 2-21

## G

Graphics Icons Key..... xiii

## H

Hidden node..... 2-4

## I

IBSS..... 2-1

IEEE 802.1X ..... 2-15  
 IEEE 802.1X authentication ..... 2-15  
 Independent Basic Service Set..... See IBSS  
 Information for Canadian Users..... iv  
     Caution ..... iv  
     Note ..... iv  
 Infrastructure..... 2-2

**L**

Link quality ..... 2-11  
 Link strength ..... 2-12

**M**

MD5 ..... Y  
 Message Digest Algorithm 5..... See MD5  
 Message Integrity Check ..... 2-7  
 MIC ..... See Message Integrity Check

**N**

Network driver version ..... 2-21  
 Network Type ..... 2-1  
     Ad-Hoc(IBSS)..... 2-1  
     Infrastructure ..... 2-2  
 NIC firmware version ..... 2-21  
 Nitro Time ..... 2-13

**O**

Online Registration ..... iii  
 Open authentication mode..... 2-6  
 Operating Mode ..... See Network Type

**P**

PEAP ..... Y  
 power save..... 2-12  
 Preface..... xiii  
 Pre-Shared Key (PSK)..... 2-15  
 problem description ..... 4-1

Product specifications ..... AA  
 profile ..... 2-10  
 Protected EAP..... See PEAP

**R**

radio frequency ..... 2-1  
 Related Documentation ..... xiii  
 Roaming..... 2-3  
     Example..... 2-3  
 RTS (Request To Send) ..... 2-4, 2-5  
 RTS Threshold ..... 2-4, 2-13  
 RTS/CTS handshake ..... 2-5

**S**

Security screen, the ..... 2-13  
 Service Set Identity ..... See SSID  
 Shared authentication mode ..... 2-6  
 Site Survey ..... 2-18, 2-19  
 SSID ..... 2-1, 2-11, 2-19  
 State ..... 2-11  
 Syntax Conventions ..... xiii

**T**

Temporal Key Integrity Protocol..... 2-7  
 Threshold ..... 2-13  
 Throughput..... 2-11  
 TKIP .... See Temporal Key Integrity Protocol  
 TLS..... Y  
 Transmission rate..... 2-1  
 Transmission rates..... 2-11  
 Transmission speeds ..... 2-11  
 Transport Layer Security..... See TLS  
 Troubleshooting ..... 4-1  
     Checking Hardware Conflict..... 4-1  
     Communication problems..... 4-1  
     Radio interference ..... 4-2  
     Starting ZyAIR Utility ..... 4-1  
 TTLS ..... Y  
 Tunneled Transport Layer Service See TTLS



**U**

|                                   |     |
|-----------------------------------|-----|
| Upgrading the ZyAIR Utility ..... | 3-1 |
| User Authentication .....         | 2-6 |
| Using the ZyAIR Utility.....      | 2-1 |

**W**

|                                |         |
|--------------------------------|---------|
| Warranty .....                 | iii     |
| Note.....                      | iii     |
| WEP .....                      | 2-6     |
| WEP Data Encryption with ..... | 2-6     |
| WEP key .....                  | 2-15    |
| confirmation .....             | 2-15    |
| format .....                   | 2-15    |
| index.....                     | 2-15    |
| length .....                   | 2-15    |
| WEP Key .....                  | 2-6     |
| Windows XP Requirement.....    | A       |
| Wired Equivalent Privacy.....  | See WEP |
| Wireless LAN Parameters        |         |
| Channel.....                   | 2-1     |

|                                   |      |
|-----------------------------------|------|
| Configuring .....                 | 2-9  |
| Network Type .....                | 2-1  |
| SSID .....                        | 2-1  |
| Transmission Rate .....           | 2-1  |
| Wireless LAN Security .....       | 2-5  |
| Data Encryption with WEP .....    | 2-6  |
| Wireless Network Basics .....     | A    |
| wireless network type .....       | 2-19 |
| WPA.....                          | 2-6  |
| WPA with RADIUS Application ..... | 2-8  |
| WPA-PSK .....                     | 2-7  |
| WPA-PSK Application.....          | 2-7  |

**Z**

|                                      |      |
|--------------------------------------|------|
| ZyAIR Utility .....                  | 3-1  |
| About .....                          | 2-21 |
| Before you upgrade.....              | 3-1  |
| Removing .....                       | 3-1  |
| Site Survey .....                    | 2-19 |
| Upgrading.....                       | 3-1  |
| ZyAIR Utility system tray icon ..... | 1-2  |