

# *ZyXEL G-120*

*802.11g Wireless CardBus Card*

## *User's Guide*

Version 1.00

Edition 1

7/2006

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "y" is lowercase and has a distinctive shape, while "XEL" is uppercase. The letters are closely spaced and have a slight shadow or depth.



# Copyright

Copyright © 2006 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 patent 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**

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Certifications

## 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 device 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 device 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 device does cause harmful interference to radio/television reception, which can be determined by turning the device 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.

## FCC Radiation Exposure Statement

- The wireless adapter has been tested to the FCC exposure requirements (Specific Absorption Rate).
- Testing was performed on laptop computers with antennas at 0mm spacing. The maximum SAR value is: 1.266W/kg. The device must not be collocated with any other antennas or transmitters.
- The device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance.
- This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- 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.

## 注意！

依據 低功率電波輻射性電機管理辦法

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

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

### Notices

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

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

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

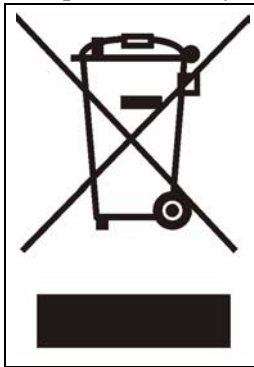
- 1 Go to <http://www.zyxel.com>.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

# Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.

This product is recyclable. Dispose of it properly.



# 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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been 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 to the purchaser.

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

## Online Registration

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

# Customer Support

Please have the following information ready when you contact customer support.

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

| METHOD                             | SUPPORT E-MAIL          | TELEPHONE                         | WEB SITE                              | REGULAR MAIL  |
|------------------------------------|-------------------------|-----------------------------------|---------------------------------------|---|
| LOCATION                           | SALES E-MAIL            | FAX                               | FTP SITE                              |   |
| CORPORATE HEADQUARTERS (WORLDWIDE) | support@zyxel.com.tw    | +886-3-578-3942                   | www.zyxel.com<br>www.europe.zyxel.com | ZyXEL Communications Corp.<br>6 Innovation Road II<br>Science Park<br>Hsinchu 300<br>Taiwan                           |
|                                    | sales@zyxel.com.tw      | +886-3-578-2439                   | ftp.zyxel.com<br>ftp.europe.zyxel.com |   |
| COSTA RICA                         | soporte@zyxel.co.cr     | +506-2017878                      | www.zyxel.co.cr                       | ZyXEL Costa Rica<br>Plaza Roble Escazú<br>Etapa El Patio, Tercer Piso<br>San José, Costa Rica                         |
|                                    | sales@zyxel.co.cr       | +506-2015098                      | ftp.zyxel.co.cr                       |   |
| CZECH REPUBLIC                     | info@cz.zyxel.com       | +420-241-091-350                  | www.zyxel.cz                          | ZyXEL Communications<br>Czech s.r.o.<br>Modranská 621<br>143 01 Praha 4 - Modrany<br>Česká Republika                  |
|                                    | info@cz.zyxel.com       | +420-241-091-359                  |                                       |   |
| DENMARK                            | support@zyxel.dk        | +45-39-55-07-00                   | www.zyxel.dk                          | ZyXEL Communications A/S<br>Columbusvej<br>2860 Soeborg<br>Denmark  |
|                                    | sales@zyxel.dk          | +45-39-55-07-07                   |                                       |   |
| FINLAND                            | support@zyxel.fi        | +358-9-4780-8411                  | www.zyxel.fi                          | ZyXEL Communications Oy<br>Malminkaari 10<br>00700 Helsinki<br>Finland  |
|                                    | sales@zyxel.fi          | +358-9-4780 8448                  |                                       |   |
| FRANCE                             | info@zyxel.fr           | +33-4-72-52-97-97                 | www.zyxel.fr                          | ZyXEL France<br>1 rue des Vergers<br>Bat. 1 / C<br>69760 Limonest<br>France   |
|                                    |                         | +33-4-72-52-19-20                 |                                       |   |
| GERMANY                            | support@zyxel.de        | +49-2405-6909-0                   | www.zyxel.de                          | ZyXEL Deutschland GmbH.<br>Adenauerstr. 20/A2 D-52146<br>Wuerselen<br>Germany   |
|                                    | sales@zyxel.de          | +49-2405-6909-99                  |                                       |   |
| HUNGARY                            | support@zyxel.hu        | +36-1-3361649                     | www.zyxel.hu                          | ZyXEL Hungary<br>48, Zoldomb Str.<br>H-1025, Budapest<br>Hungary  |
|                                    | info@zyxel.hu           | +36-1-3259100                     |                                       |   |
| KAZAKHSTAN                         | http://zyxel.kz/support | +7-3272-590-698                   | www.zyxel.kz                          | ZyXEL Kazakhstan<br>43, Dostyk ave., Office 414<br>Dostyk Business Centre<br>050010, Almaty<br>Republic of Kazakhstan |
|                                    | sales@zyxel.kz          | +7-3272-590-689                   |                                       |   |
| NORTH AMERICA                      | support@zyxel.com       | 1-800-255-4101<br>+1-714-632-0882 | www.us.zyxel.com                      | ZyXEL Communications Inc.<br>1130 N. Miller St.<br>Anaheim<br>CA 92806-2001<br>U.S.A.                                 |
|                                    | sales@zyxel.com         | +1-714-632-0858                   | ftp.us.zyxel.com                      |   |



| LOCATION       | METHOD | SUPPORT E-MAIL          | TELEPHONE                                 | WEB SITE         | REGULAR MAIL  |
|----------------|--------|-------------------------|---|------------------|---|
|                |        | SALES E-MAIL            | FAX                                       | FTP SITE         |   |
| NORWAY         |        | support@zyxel.no        | +47-22-80-61-80                           | www.zyxel.no     | ZyXEL Communications A/S<br>Niils Hansens vei 13<br>0667 Oslo<br>Norway   |
|                |        | sales@zyxel.no          | +47-22-80-61-81                           |                  |   |
| POLAND         |        | info@pl.zyxel.com       | +48 (22) 333 8250                         | www.pl.zyxel.com | ZyXEL Communications<br>ul. Okrzei 1A<br>03-715 Warszawa<br>Poland  |
|                |        |                         | +48 (22) 333 8251                         |                  |   |
| RUSSIA         |        | http://zyxel.ru/support | +7-095-542-89-29                          | www.zyxel.ru     | ZyXEL Russia<br>Ostrovityanova 37a Str.<br>Moscow, 117279<br>Russia   |
|                |        | sales@zyxel.ru          | +7-095-542-89-25                          |                  |   |
| SPAIN          |        | support@zyxel.es        | +34-902-195-420                           | www.zyxel.es     | ZyXEL Communications<br>Arte, 21 5 <sup>a</sup> planta<br>28033 Madrid<br>Spain   |
|                |        | sales@zyxel.es          | +34-913-005-345                           |                  |   |
| SWEDEN         |        | support@zyxel.se        | +46-31-744-7700                           | www.zyxel.se     | ZyXEL Communications A/S<br>Sjöporten 4, 41764 Göteborg<br>Sweden   |
|                |        | sales@zyxel.se          | +46-31-744-7701                           |                  |   |
| UKRAINE        |        | support@ua.zyxel.com    | +380-44-247-69-78                         | www.ua.zyxel.com | ZyXEL Ukraine<br>13, Pimonenko Str.<br>Kiev, 04050<br>Ukraine   |
|                |        | sales@ua.zyxel.com      | +380-44-494-49-32                         |                  |   |
| UNITED KINGDOM |        | support@zyxel.co.uk     | +44-1344 303044<br>08707 555779 (UK only) | www.zyxel.co.uk  | ZyXEL Communications UK<br>Ltd., 11 The Courtyard,<br>Eastern Road, Bracknell,<br>Berkshire, RG12 2XB,<br>United Kingdom (UK) |
|                |        | sales@zyxel.co.uk       | +44-1344 303034                           | ftp.zyxel.co.uk  |   |

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



# Table of Contents

|   |           |
|---|-----------|
| <b>Copyright</b> .....                            | <b>3</b>  |
| <b>Certifications</b> .....                       | <b>4</b>  |
| <b>Safety Warnings</b> .....                      | <b>6</b>  |
| <b>ZyXEL Limited Warranty</b> .....               | <b>7</b>  |
| <b>Customer Support</b> .....                     | <b>8</b>  |
| <b>Table of Contents</b> .....                    | <b>11</b> |
| <b>List of Figures</b> .....                      | <b>15</b> |
| <b>List of Tables</b> .....                       | <b>17</b> |
| <b>Preface</b> .....                              | <b>19</b> |
| <b>Chapter 1</b>                                  |           |
| <b>Getting Started</b> .....                      | <b>21</b> |
| 1.1 About Your G-120 .....                        | 21        |
| 1.2 Application Overview .....                    | 21        |
| 1.2.0.1 Infrastructure .....                      | 21        |
| 1.2.0.2 Ad-Hoc .....                              | 22        |
| 1.3 G-120 Hardware and Utility Installation ..... | 23        |
| 1.3.1 ZyXEL Utility Icon .....                    | 23        |
| 1.4 Configuration Methods .....                   | 23        |
| 1.4.1 Enabling WZC .....                          | 23        |
| 1.4.2 Accessing the ZyXEL Utility .....           | 24        |
| <b>Chapter 2</b>                                  |           |
| <b>Tutorial</b> .....                             | <b>25</b> |
| 2.1 Connecting to a Wireless LAN .....            | 25        |
| 2.2 Creating and Using a Profile .....            | 27        |
| <b>Chapter 3</b>                                  |           |
| <b>Wireless LAN Network</b> .....                 | <b>31</b> |
| 3.1 Wireless LAN Overview .....                   | 31        |
| 3.2 Wireless LAN Security .....                   | 32        |
| 3.2.1 User Authentication and Encryption .....    | 32        |
| 3.2.1.1 WEP .....                                 | 32        |

|  |           |
|--|-----------|
| 3.2.1.2 IEEE 802.1x .....                                | 33        |
| 3.2.1.3 WPA and WPA2 .....                               | 34        |
| 3.3 Introduction to OTIST .....                          | 34        |
| 3.3.1 Enabling OTIST .....                               | 34        |
| 3.3.1.1 AP .....   | 35        |
| 3.3.1.2 Wireless Client .....                            | 36        |
| 3.3.2 Starting OTIST .....                               | 36        |
| 3.3.3 Notes on OTIST .....                               | 37        |
| <b>Chapter 4</b>   |           |
| <b>ZyXEL Utility Configuration .....</b>                 | <b>39</b> |
| 4.1 The Link Info Screen .....                           | 39        |
| 4.1.1 Trend Chart .....                                  | 40        |
| 4.2 The Site Survey Screen .....                         | 41        |
| 4.2.1 Security Settings .....                            | 43        |
| 4.2.1.1 WEP Encryption .....                             | 43        |
| 4.2.1.2 WPA-PSK/WPA2-PSK .....                           | 44        |
| 4.2.1.3 WPA-RADIUS/WPA2-RADIUS .....                     | 45        |
| 4.2.1.4 RADIUS .....                                     | 46        |
| 4.2.2 Confirm New Settings .....                         | 47        |
| 4.3 The Profile Screen .....                             | 48        |
| 4.3.1 Adding a New Profile .....                         | 50        |
| 4.4 The Adapter Screen .....                             | 54        |
| <b>Chapter 5</b>   |           |
| <b>Maintenance .....</b>                                 | <b>57</b> |
| 5.1 The About Screen .....                               | 57        |
| 5.2 Uninstalling the ZyXEL Utility .....                 | 57        |
| 5.3 Upgrading the ZyXEL Utility .....                    | 58        |
| <b>Chapter 6</b>   |           |
| <b>Troubleshooting .....</b>                             | <b>61</b> |
| 6.1 Problems Starting the ZyXEL Utility .....            | 61        |
| 6.2 Problem with the Link Quality .....                  | 61        |
| 6.3 Problems Communicating With Other Computers .....    | 62        |
| <b>Appendix A</b>  |           |
| <b>Product Specifications .....</b>                      | <b>63</b> |
| <b>Appendix B</b>  |           |
| <b>Management with Wireless Zero Configuration .....</b> | <b>65</b> |
| <b>Appendix C</b>  |           |
| <b>Wireless Security .....</b>                           | <b>77</b> |

|   |           |
|---|-----------|
| <b>Appendix D</b>                                 |           |
| <b>Setting up Your Computer's IP Address.....</b> | <b>83</b> |
| <b>Index.....</b>                                 | <b>95</b> |



# List of Figures

|  |    |
|--|----|
| Figure 1 Application: Infrastructure .....                         | 22 |
| Figure 2 Application: Ad-Hoc .....                                 | 22 |
| Figure 3 ZyXEL Utility: System Tray Icon .....                     | 23 |
| Figure 4 Enable WZC .....  | 24 |
| Figure 5 Infrastructure Network .....                              | 25 |
| Figure 6 ZyXEL Utility: Site Survey .....                          | 26 |
| Figure 7 ZyXEL Utility: Security Settings .....                    | 26 |
| Figure 8 ZyXEL Utility: Confirm New Settings .....                 | 27 |
| Figure 9 ZyXEL Utility: Link Info .....                            | 27 |
| Figure 10 ZyXEL Utility: Profile .....                             | 28 |
| Figure 11 ZyXEL Utility: Add New Profile .....                     | 28 |
| Figure 12 ZyXEL Utility: Profile Security .....                    | 29 |
| Figure 13 ZyXEL Utility: Profile Encryption .....                  | 29 |
| Figure 14 ZyXEL Utility: Profile Confirm New Settings .....        | 29 |
| Figure 15 ZyXEL Utility: Profile Activate .....                    | 30 |
| Figure 16 Example of a Wireless Network .....                      | 31 |
| Figure 17 Link Info .....  | 39 |
| Figure 18 Station Mode: Link Info: Trend Chart .....               | 41 |
| Figure 19 Site Survey .....  | 42 |
| Figure 20 Security Setting: WEP .....                              | 43 |
| Figure 21 Security Setting: WPA-PSK/WPA2-PSK .....                 | 44 |
| Figure 22 Security Setting: WPA-RADIUS/WPA2-RADIUS .....           | 45 |
| Figure 23 Security Setting: RADIUS .....                           | 46 |
| Figure 24 Confirm New Settings .....                               | 47 |
| Figure 25 Profile .....  | 49 |
| Figure 26 Profile: Add a New Profile .....                         | 50 |
| Figure 27 Profile: Select a Channel .....                          | 52 |
| Figure 28 Profile: Security Settings .....                         | 53 |
| Figure 29 Profile: Security Settings .....                         | 53 |
| Figure 30 Profile: Confirm New Settings .....                      | 54 |
| Figure 31 Profile: Activate the Profile .....                      | 54 |
| Figure 32 Adapter .....  | 55 |
| Figure 33 About .....  | 57 |
| Figure 34 Uninstall: Confirm .....                                 | 58 |
| Figure 35 Uninstall: Finish .....                                  | 58 |
| Figure 36 Windows XP SP2: WZC Not Available .....                  | 65 |
| Figure 37 Windows XP SP2: System Tray Icon .....                   | 66 |
| Figure 38 Windows XP SP2: Wireless Network Connection Status ..... | 66 |

|  |    |
|--|----|
| Figure 39 Windows XP SP1: Wireless Network Connection Status .....         | 67 |
| Figure 40 Windows XP SP2: Wireless Network Connection .....                | 67 |
| Figure 41 Windows XP SP1: Wireless Network Connection Properties .....     | 68 |
| Figure 42 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK ..   | 69 |
| Figure 43 Windows XP SP2: Wireless Network Connection: No Security .....   | 69 |
| Figure 44 Windows XP: Wireless (network) properties: Association .....     | 70 |
| Figure 45 Windows XP: Wireless (network) properties: Authentication .....  | 71 |
| Figure 46 Windows XP: Protected EAP Properties .....                       | 72 |
| Figure 47 Windows XP: Smart Card or other Certificate Properties .....     | 73 |
| Figure 48 Windows XP SP2: Wireless Networks: Preferred Networks .....      | 75 |
| Figure 49 Windows XP SP1: Wireless Networks: Preferred Networks .....      | 75 |
| Figure 50 WPA-PSK Authentication .....                                     | 81 |
| Figure 51 WPA(2) with RADIUS Application Example .....                     | 82 |
| Figure 52 Windows 95/98/Me: Network: Configuration .....                   | 84 |
| Figure 53 Windows 95/98/Me: TCP/IP Properties: IP Address .....            | 85 |
| Figure 54 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....     | 86 |
| Figure 55 Windows XP: Start Menu .....                                     | 87 |
| Figure 56 Windows XP: Control Panel .....                                  | 87 |
| Figure 57 Windows XP: Control Panel: Network Connections: Properties ..... | 88 |
| Figure 58 Windows XP: Local Area Connection Properties .....               | 88 |
| Figure 59 Windows XP: Advanced TCP/IP Settings .....                       | 89 |
| Figure 60 Windows XP: Internet Protocol (TCP/IP) Properties .....          | 90 |
| Figure 61 Macintosh OS 8/9: Apple Menu .....                               | 91 |
| Figure 62 Macintosh OS 8/9: TCP/IP .....                                   | 91 |
| Figure 63 Macintosh OS X: Apple Menu .....                                 | 92 |
| Figure 64 Macintosh OS X: Network .....                                    | 93 |



# List of Tables

|  |    |
|--|----|
| Table 1 ZyXEL Utility: System Tray Icon .....                            | 23 |
| Table 2 Link Info .....  | 39 |
| Table 3 Station Mode: Link Info: Trend Chart .....                       | 41 |
| Table 4 Site Survey .....  | 42 |
| Table 5 Security Setting: WEP .....                                      | 43 |
| Table 6 Security Setting: WPA-PSK/WPA2-PSK .....                         | 45 |
| Table 7 Security Setting: WPA-RADIUS/WPA2-RADIUS .....                   | 45 |
| Table 8 Security Setting: RADIUS .....                                   | 47 |
| Table 9 Confirm New Settings .....                                       | 48 |
| Table 10 Profile .....   | 49 |
| Table 11 Profile: Add a New Profile .....                                | 50 |
| Table 12 Profile: Select a Channel .....                                 | 52 |
| Table 13 Adapter .....   | 55 |
| Table 14 About .....   | 57 |
| Table 15 Troubleshooting Starting ZyXEL Utility .....                    | 61 |
| Table 16 Troubleshooting Link Quality .....                              | 61 |
| Table 17 Troubleshooting Communication Problem .....                     | 62 |
| Table 18 Product Specifications .....                                    | 63 |
| Table 19 Windows XP SP2: System Tray Icon .....                          | 66 |
| Table 20 Windows XP SP2: Wireless Network Connection .....               | 68 |
| Table 21 Windows XP: Wireless Networks .....                             | 69 |
| Table 22 Windows XP: Wireless (network) properties: Association .....    | 70 |
| Table 23 Windows XP: Wireless (network) properties: Authentication ..... | 71 |
| Table 24 Windows XP: Protected EAP Properties .....                      | 73 |
| Table 25 Windows XP: Smart Card or other Certificate Properties .....    | 74 |
| Table 26 Comparison of EAP Authentication Types .....                    | 79 |
| Table 27 Wireless Security Relational Matrix .....                       | 82 |



# Preface

Congratulations on your purchase of the ZyXEL G-120 802.11g Wireless CardBus Card.

Your G-120 is easy to install and configure.

## About This User's Guide

This manual is designed to guide you through the configuration of your G-120 for its various applications.

## Related Documentation

- Supporting Disk  
Refer to the included CD for support documents.
- Quick Start Guide  
The Quick Start Guide is designed to help you get up and running right away. It contains hardware installation/connection information.
- 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 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.

## Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choice.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The ZyXEL G-120 802.11g Wireless CardBus Card may be referred to as the G-120 in this user’s guide.

## Graphics Icons Key

|  |  |  |
|--|--|--|
| <p>Wireless Access Point</p>  | <p>Computer</p>         | <p>Notebook Computer</p>  |
| <p>Server</p>                 | <p>Modem or Router</p>  | <p>Wireless Signal</p>    |
| <p>Internet Cloud</p>         |  |  |

# CHAPTER 1

## Getting Started

This chapter introduces the G-120 and prepares you to use the ZyXEL utility.

### 1.1 About Your G-120

The G-120 is an IEEE 802.11b/g compliant wireless LAN adapter. The ZyXEL utility is a tool that helps you configure your G-120. See the appendix for detailed product specifications.

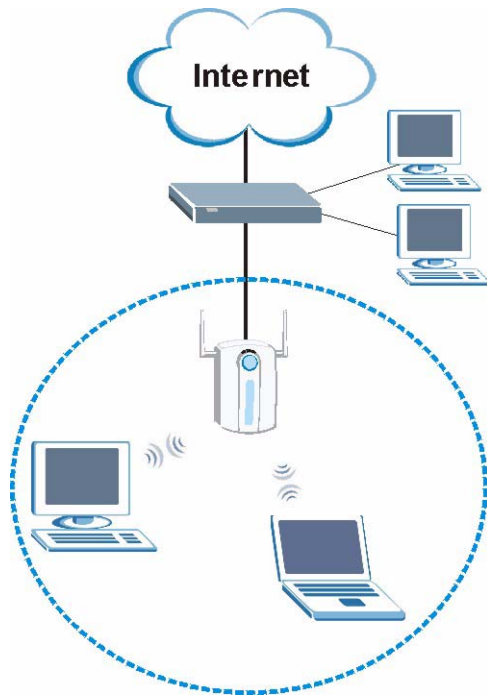
### 1.2 Application Overview

This section describes some network applications for the G-120. You can either set the network type to **Infrastructure** and connect to an AP or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

#### 1.2.0.1 Infrastructure

To connect to a network via an access point (AP), set the G-120 network type to **Infrastructure**. Through the AP, you can access the Internet or the wired network behind the AP.

**Figure 1** Application: Infrastructure

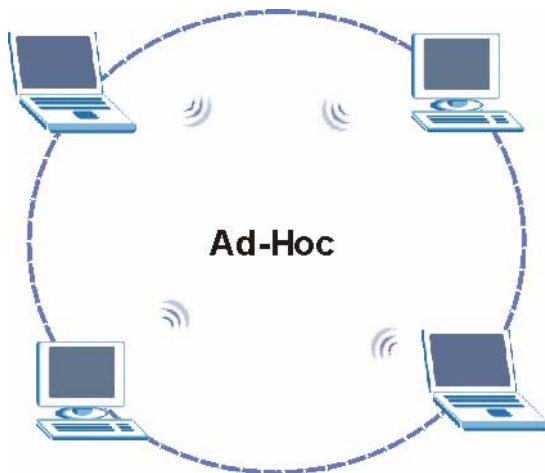


### 1.2.0.2 Ad-Hoc

To set up a small independent wireless workgroup without an AP, use **Ad-Hoc**.

**Ad-Hoc** does not require an AP or a wired network. Two or more wireless clients communicate directly to each other.

**Figure 2** Application: Ad-Hoc



## 1.3 G-120 Hardware and Utility Installation

Follow the instructions in the Quick Start Guide to install the ZyXEL utility and make hardware connections.

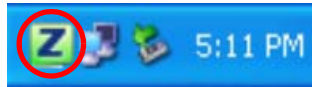
### 1.3.1 ZyXEL Utility Icon

After you install and start the ZyXEL utility, an icon for the ZyXEL utility appears in the system tray.

**Note:** The ZyXEL utility system tray icon displays only when the G-120 is installed properly.

When you use the ZyXEL utility, it automatically disables WZC.

**Figure 3** ZyXEL Utility: System Tray Icon



The color of the ZyXEL utility system tray icon indicates the status of the G-120. Refer to the following table for details.

**Table 1** ZyXEL Utility: System Tray Icon

| COLOR | DESCRIPTION   |
|-------|---|
| Red   | The G-120 is not connected to a wireless network or is searching for an available wireless network. |
| Green | The G-120 is connected to a wireless network.   |

## 1.4 Configuration Methods

To configure your G-120, use one of the following applications:

- Wireless Zero Configuration (WZC) (the Windows XP wireless configuration tool)
- ZyXEL Utility

### 1.4.1 Enabling WZC


**Note:** When you use the ZyXEL utility, it automatically disables WZC.

If you want to use WZC to configure the G-120, you need to disable the ZyXEL utility by right-clicking the utility icon (Z) in the system tray and selecting **Use Windows to configure my wireless network settings**.

**Figure 4** Enable WZC




Refer to the appendices for information on how to use WZC to manage the G-120.

To re-activate the ZyXEL utility, double-click the  icon on your desktop or click **Start, (All) Programs, ZyXEL G-120 Utility, ZyXEL G-120 Utility GUI**.

## 1.4.2 Accessing the ZyXEL Utility

Double-click on the ZyXEL wireless LAN utility icon in the system tray to open the ZyXEL utility. The ZyXEL utility screens are similar in all Microsoft Windows versions. Screens for Windows XP are shown in this User's Guide.

**Note:** Click the  icon (located in the top right corner) to display the online help window.

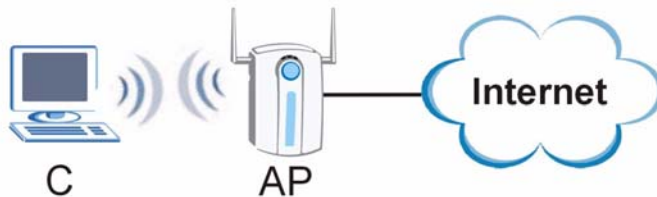


# CHAPTER 2

## Tutorial

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagrams. The wireless client is labeled **C** and the access point is labeled **AP**.

**Figure 5** Infrastructure Network



There are three ways to connect the wireless client to a network.

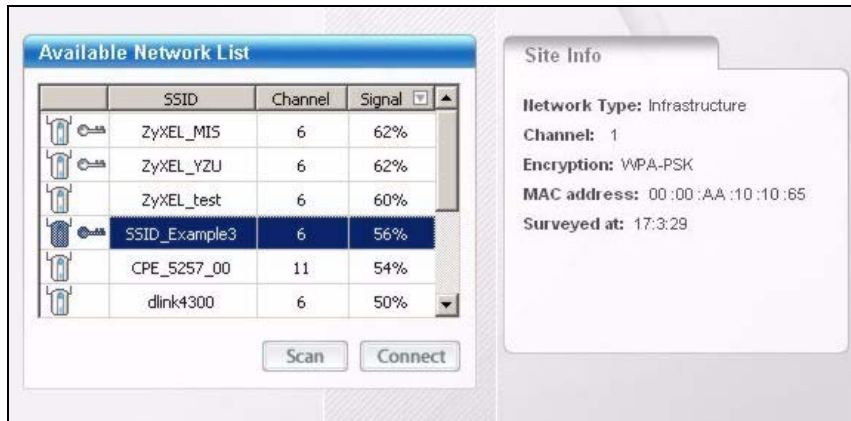
- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network (see [Section 2.1 on page 25](#)).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see [Section 2.2 on page 27](#)).

## 2.1 Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID\_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey” in the AP.

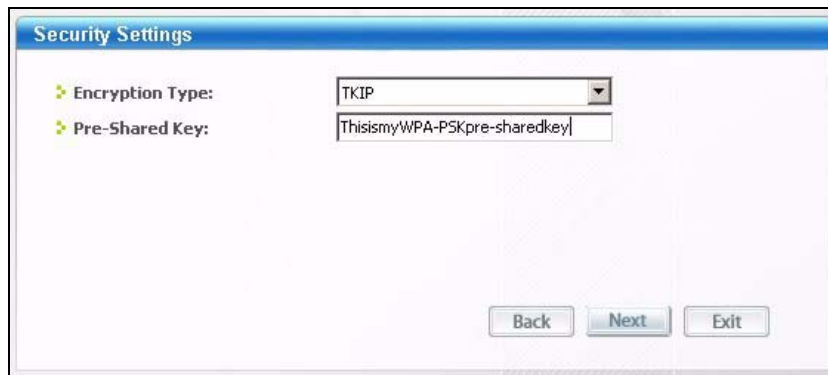
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen as shown next.

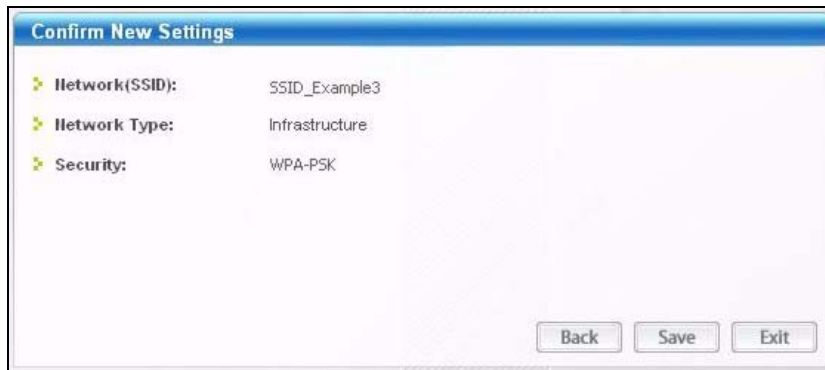
**Figure 6** ZyXEL Utility: Site Survey

- The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See [Table 4 on page 42](#) for detailed field descriptions.
- To connect to an AP or peer computer, either click an entry in the list and then click **Connect** or double-click an entry (with a SSID of **SSID\_Examples3** in this example).
- When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

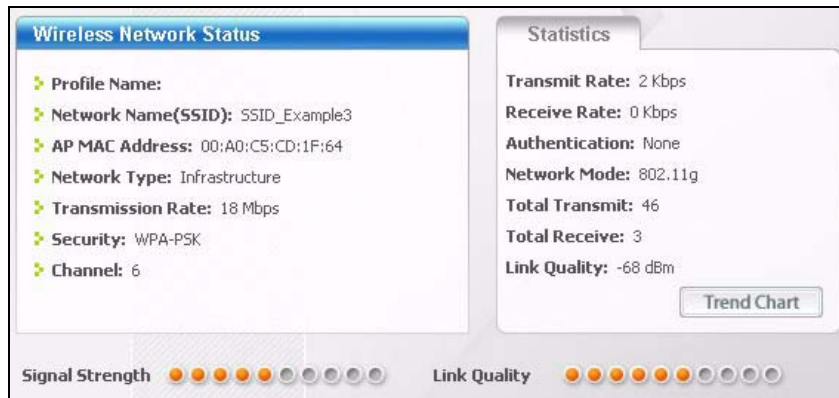
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

**Figure 7** ZyXEL Utility: Security Settings

- The **Confirm New Settings** window appears. Check your settings and click **Save** to continue.

**Figure 8** ZyXEL Utility: Confirm New Settings

- 6 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank. See [Table 2 on page 39](#) for detailed field descriptions.

**Figure 9** ZyXEL Utility: Link Info

- 7 Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured. If you cannot access the web site, check the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

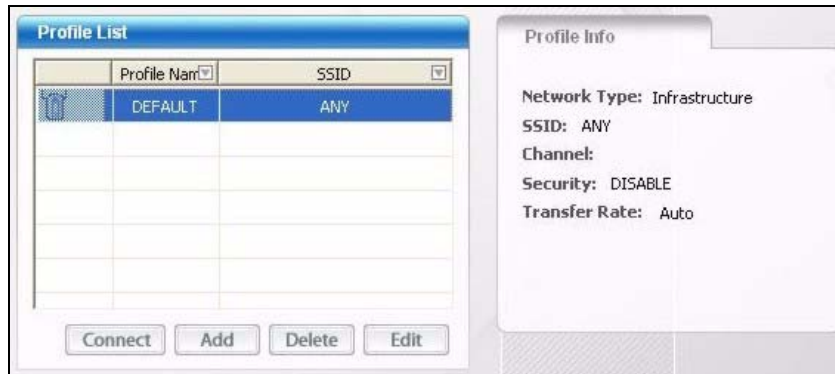
## 2.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the ZyXEL utility. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the SSID is “SSID\_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey” in the AP. You have chosen the profile name “PN\_Example3”.

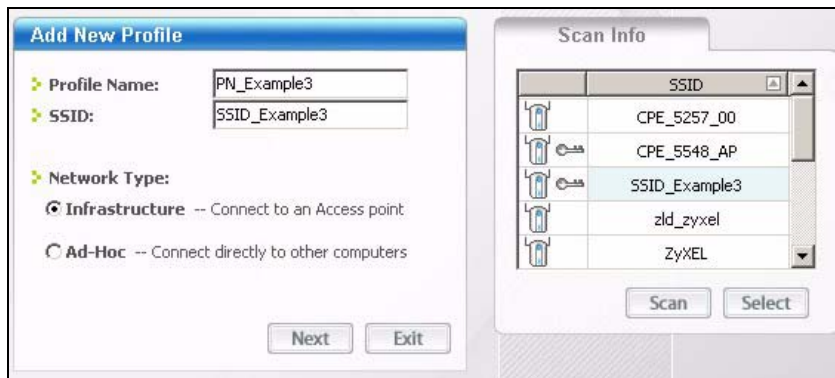
- 1 Open the ZyXEL utility and click the **Profile** tab to open the screen as shown. Click **Add** to configure a new profile.

**Figure 10** ZyXEL Utility: Profile



- 2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. You can also configure your profile for a wireless network that is not in the list.

**Figure 11** ZyXEL Utility: Add New Profile



- 3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.
- 4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

**Figure 12** ZyXEL Utility: Profile Security

Security Settings

Encryption Type: WPA-PSK

Back Next Exit

- 5 This screen varies depending on the encryption method you selected in the previous screen. In this example, enter the pre-shared key and leave the encryption type at the default setting.

**Figure 13** ZyXEL Utility: Profile Encryption

Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

Back Next Exit

- 6 Verify the profile settings in the ready-only screen. Click **Save** to save and go to the next screen.

**Figure 14** ZyXEL Utility: Profile Confirm New Settings

Confirm New Settings

Network(SSID): SSID\_Example3

Network Type: Infrastructure

Security: WPA-PSK

Back Save Exit

- 7 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button to go back to the **Profile List** screen.

If you clicked **Activate Later** you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

**Note:** Only one profile can be activated and used at any given time.

**Figure 15** ZyXEL Utility: Profile Activate



- 8** When you activate the new profile, the ZyXEL utility goes to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.
- 9** Make sure the selected AP in the active profile is connected to the Internet. Open your Internet browser, enter <http://www.zyxel.com> or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.
- 10** If you cannot access the Internet, go back to the **Profile** screen. Select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

# CHAPTER 3

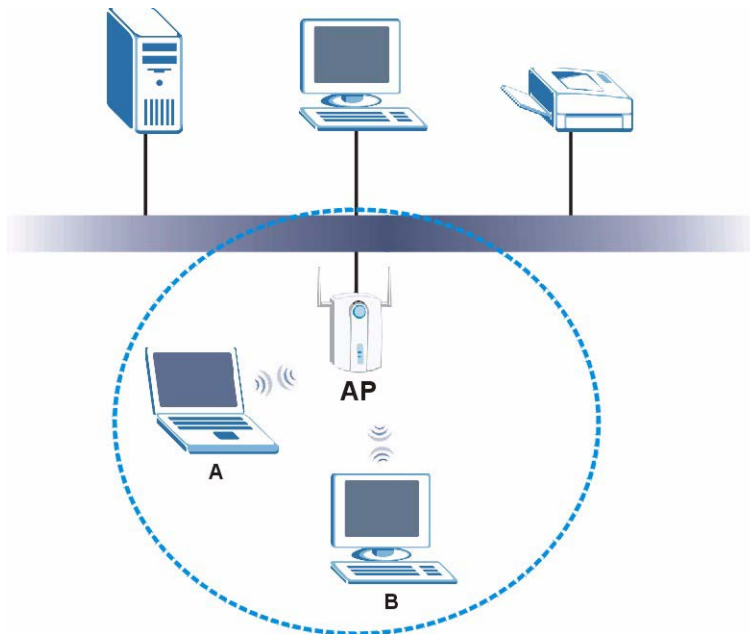
## Wireless LAN Network

This chapter provides background information on wireless LAN network.

### 3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See [Figure 2 on page 22](#) for an Ad Hoc network example.

**Figure 16** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP or peer computer.

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 3.2 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communications.

Configure the wireless LAN security using the **Profile Security Setting** screen. If you do not enable any wireless security on your G-120, the G-120's wireless communications are accessible to any wireless networking device that is in the coverage area.

**Note:** You can only use WEP encryption if you set the G-120 to Ad-hoc mode.

See the appendices for more detailed information about wireless security.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

### 3.2.1 User Authentication and Encryption

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

#### 3.2.1.1 WEP

##### 3.2.1.1.1 Data Encryption

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the G-120 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 G-120.

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



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 Setting** screen of the ZyXEL utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

Your G-120 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys and only one key is used as the default key at any one time.

### 3.2.1.1.2 Authentication Type

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

- Open System mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- Shared Key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
- Auto authentication mode allows the G-120 to switch between the open system and shared key modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations.

### 3.2.1.2 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.

#### 3.2.1.2.1 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 IEEE 802.1x. The G-120 supports EAP-TLS and EAP-PEAP. Refer to [Appendix C on page 77](#) 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.

### 3.2.1.3 WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## 3.3 Introduction to OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as “AP” here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn't configure one manually.

### 3.3.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

We use the P-334WT in this guide as the example AP. Screens may vary slightly for your ZyXEL devices.

**Note:** The AP and wireless client(s) MUST use the same **Setup key**.

### 3.3.1.1 AP

On the P-334WT, you can enable OTIST using the **Reset** button or the web configurator. If you use the **Reset** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

Hold in the **Reset** button for one or two seconds.

**Note:** If you hold in the **Reset** button too long, the device may reset to the factory defaults!

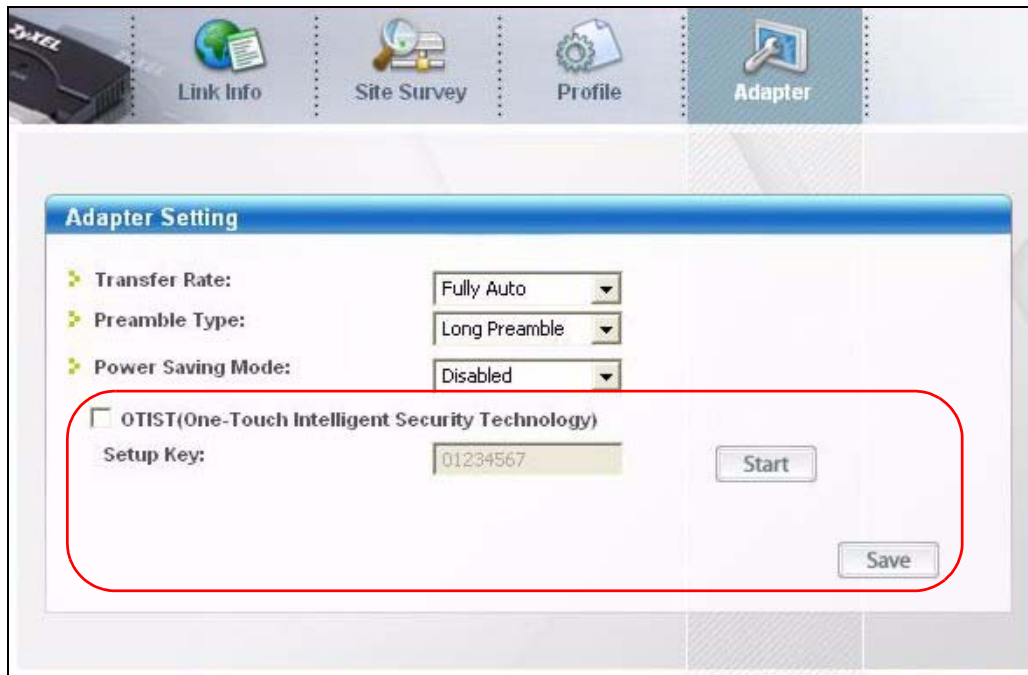
In the web configurator, go to the **Wireless LAN** main screen and then select **OTIST**. To change the **Setup key**, enter zero to eight printable characters. To have OTIST automatically generate a WPA-PSK key, select the **Yes** check box. If you manually configured a WEP key or a WPA-PSK key and you also selected this check box, then the key you manually configured is used.



The screenshot shows the 'WIRELESS LAN' configuration page with the 'OTIST' tab selected. The page title is 'One-touch Intelligent Security Technology'. There is a 'Setup Key' field containing '01234567'. Below it is a checked checkbox with the text: 'Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no any WLAN security has been set. This will generate a random PSK key later for your convenience.' At the bottom of the page is a 'Start' button.

### 3.3.1.2 Wireless Client

Start the ZyXEL utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP's and click **Save**.



### 3.3.2 Starting OTIST

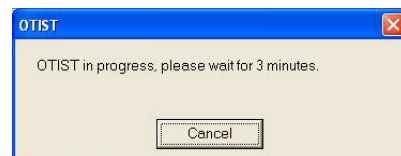
**Note:** You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

See the user's guide for more information.

- 1 In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.



- 2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.



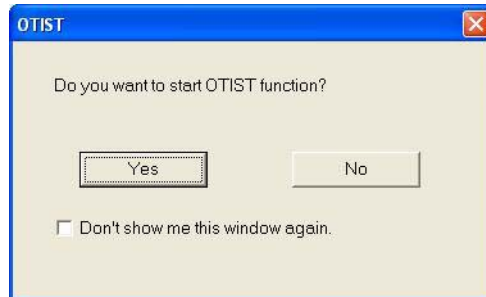
- In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup key**). Click **OK** to go back to the ZyXEL utility main screen.



- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

### 3.3.3 Notes on OTIST

- 1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.



- 2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)
- 3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **Reset** button (for one or two seconds) for the AP to transfer settings.
- 4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).
- 5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL the wireless clients again.



# CHAPTER 4

## ZyXEL Utility Configuration

This chapter shows you how to configure your G-120 using the ZyXEL utility.

### 4.1 The Link Info Screen

When the ZyXEL utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your G-120.

**Figure 17** Link Info



The following table describes the labels in this screen.

**Table 2** Link Info

| LABEL                   | DESCRIPTION   |
|-------------------------|---|
| Wireless Network Status |   |
| Profile Name            | This is the name of the profile you are currently using.  |
| Network Name (SSID)     | The SSID identifies the wireless network to which a wireless station is associated. This field displays the name of the wireless device to which the G-120 is associated. |

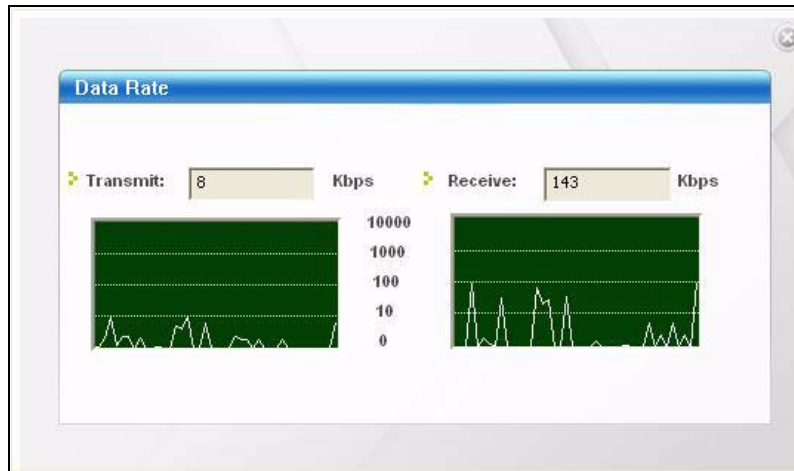
**Table 2** Link Info (continued)

| LABEL             | DESCRIPTION   |
|-------------------|---|
| AP MAC Address    | This field displays the MAC address of the AP or peer computer to which the G-120 is associated.  |
| Network Type      | This field displays the network type ( <b>Infrastructure</b> or <b>Ad-Hoc</b> ) of the wireless network.  |
| Transmission Rate | This field displays the current transmission rate of the G-120 in megabits per second (Mbps).   |
| Security          | This field displays whether data encryption is activated ( <b>WEP</b> (WEP or 802.1x), <b>TKIP</b> (WPA/WPA-PSK/WPA2/WPA2-PSK), <b>AES</b> (WPA/WPA-PSK/WPA2/WPA2-PSK)) or inactive ( <b>None</b> ).  |
| Channel           | This field displays the radio channel the G-120 is currently using.   |
| Statistics        |   |
| Transmit Rate     | This field displays the current data transmission rate in kilobits per second (Kbps).   |
| Receive Rate      | This field displays the current data receiving rate in kilobits per second (Kbps).  |
| Authentication    | This field displays the authentication method of the G-120.   |
| Network Mode      | This field displays the wireless standard ( <b>802.11b</b> or <b>802.11g</b> ) of the AP or peer computer.  |
| Total Transmit    | This field displays the total number of data frames transmitted.  |
| Total Receive     | This field displays the total number of data frames received.   |
| Link Quality      | This field displays the signal strength of the G-120.   |
| Trend Chart       | Click this button to display the real-time statistics of the data rate in kilobits per second (Kbps).   |
| Signal Strength   | The status bar shows the strength of the signal. The signal strength is mainly depending on the antenna output power and the distance between your G-120 and the AP or peer computer.   |
| Link Quality      | The status bar shows the quality of wireless connection. This refers to the percentage of packets transmitted successfully. If there are too many wireless stations in a wireless network, collisions may occur which could result in a loss of messages even though you have high signal strength. |

### 4.1.1 Trend Chart

Click **Trend Chart** in the **Link Info** screen to display a screen as shown below. Use this screen to view real-time data traffic statistics.



**Figure 18** Station Mode: Link Info: Trend Chart

The following table describes the labels in this screen.

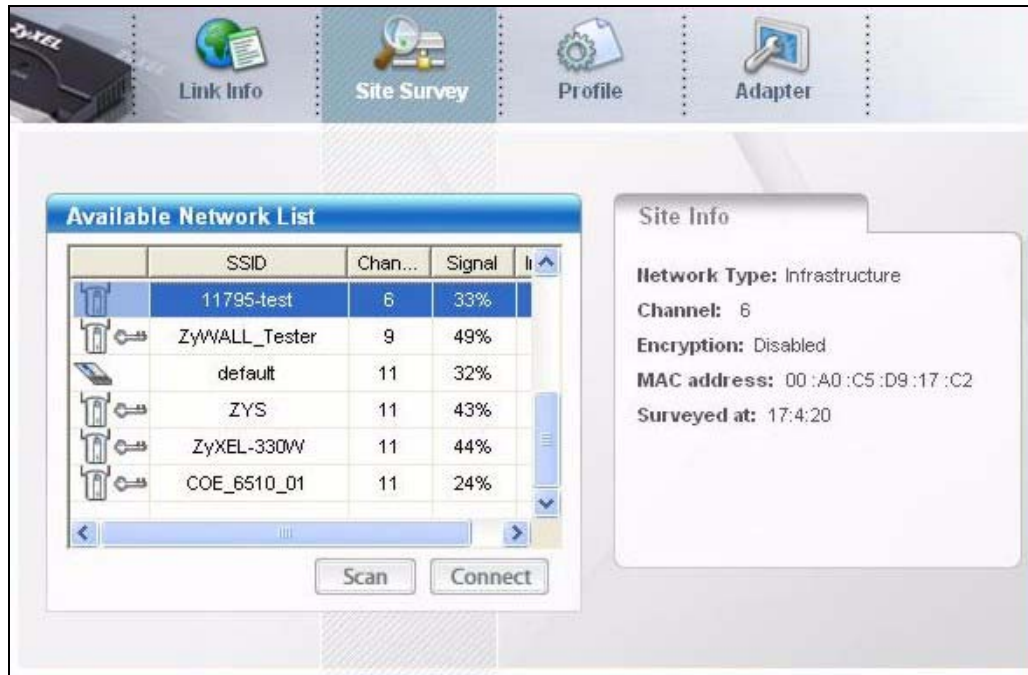
**Table 3** Station Mode: Link Info: Trend Chart

| LABEL    | DESCRIPTION   |
|----------|---|
| Transmit | This field displays the current data transmission rate in kilobits per second (Kbps). |
| Receive  | This field displays the current data receiving rate in kilobits per second (Kbps).    |

## 4.2 The Site Survey Screen

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

**Figure 19** Site Survey



The following table describes the labels in this screen.

**Table 4** Site Survey

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Available Network List | Click a column heading to sort the entries.   |
|                        | denotes that the wireless device is in infrastructure mode and the wireless security is activated.  |
|                        | denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.  |
| or                     | denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.  |
|                        | denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.  |
| SSID                   | This field displays the SSID (Service Set Identifier) of each wireless device.  |
| Channel                | This field displays the channel number used by each wireless device.  |
| Signal                 | This field displays the signal strength of each wireless device.  |
| Scan                   | Click <b>Scan</b> to search for available wireless devices within transmission range.   |
| Connect                | Click <b>Connect</b> to associate to the selected wireless device.  |
| Site Info              | Click an entry in the <b>Available Network List</b> table to display the information of the selected wireless device.                                     |
| Network Type           | This field displays the network type ( <b>Infrastructure</b> or <b>Ad-Hoc</b> ) of the wireless device.   |
| Channel                | This field displays the channel number used by each wireless device.  |
| Encryption             | This field shows whether data encryption is activated ( <b>WEP, WPA-PSK, WPA-RADIUS, RADIUS, WPA2-RADIUS, WPA2-PSK</b> ) or inactive ( <b>Disabled</b> ). |

**Table 4** Site Survey (continued)

| LABEL       | DESCRIPTION   |
|-------------|---|
| MAC address | This field displays the MAC address of the wireless device.       |
| Surveyed at | This field displays the time when the wireless device is scanned. |

## 4.2.1 Security Settings

When you configure the G-120 to connect to a network with wireless security activated and the security settings are disabled on the G-120, the screen varies according to the encryption method used by the selected network.

### 4.2.1.1 WEP Encryption

**Figure 20** Security Setting: WEP

The screenshot shows a window titled "Security Setting" with the following fields and values:

- WEP:** 128 Bits (dropdown menu)
- Authentication:** Auto (dropdown menu)
- Pass Phrase:** qwer1234 (text input field)
- Transmit Key:** Key1 (dropdown menu)
- Key1:** daa2ea0e314b7cb996a2 (text input field)

At the bottom right, there are three buttons: "Back", "Next", and "Exit".

The following table describes the labels in this screen.

**Table 5** Security Setting: WEP

| LABEL            | DESCRIPTION   |
|------------------|---|
| Security Setting |   |
| WEP              | Select <b>64 Bits</b> , <b>128 Bits</b> or <b>256 Bits</b> to activate WEP encryption and then fill in the related fields.  |
| Encryption Type  | Select an authentication method. Choices are <b>Auto</b> , <b>Open System</b> and <b>Shared Key</b> .<br>Refer to <a href="#">Section 3.2.1.1.2 on page 33</a> for more information.  |
| Pass Phrase      | Enter a passphrase of up to 63 case-sensitive printable characters. As you enter the passphrase, the G-120 automatically generates four different WEP keys and displays it in the key field below. Refer to <a href="#">Section 3.2.1.1.1 on page 32</a> for more information.<br>At the time of writing, you cannot use passphrase to generate 256-bit WEP keys. |
| Transmit Key     | Select a default WEP key to use for data encryption. The key displays in the field below.   |

**Table 5** Security Setting: WEP (continued)

| LABEL                                       | DESCRIPTION   |
|---|---|
| Key x (where x is a number between 1 and 4) | Select this option if you want to manually enter the WEP keys. Enter the WEP key in the field provided.<br>If you select <b>64 Bits</b> in the <b>WEP</b> field.<br>Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type.<br>or<br>Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type.<br>If you select <b>128 Bits</b> in the <b>WEP</b> field,<br>Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type<br>or<br>Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type.<br>If you select <b>256 Bits</b> in the <b>WEP</b> field,<br>Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type<br>or<br>Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey111122223333444455556678) for ASCII key type.<br><b>Note:</b> The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN.<br><br>ASCII WEP keys are case sensitive. |
| Back  | Click <b>Back</b> to go to the <b>Site Survey</b> screen to select and connect to another network.  |
| Next  | Click <b>Next</b> to confirm your selections and advance to the <b>Confirm New Settings</b> screen. Refer to <a href="#">Section 4.2.2 on page 47</a> .   |
| Exit  | Click <b>Exit</b> to return to the <b>Site Survey</b> screen without saving.  |

#### 4.2.1.2 WPA-PSK/WPA2-PSK

**Figure 21** Security Setting: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

**Table 6** Security Setting: WPA-PSK/WPA2-PSK

| LABEL           | DESCRIPTION  |
|-----------------|--|
| Encryption Type | The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>Select the encryption type ( <b>TKIP</b> or <b>AES</b> ) for data encryption.<br>Refer to <a href="#">Section 3.2.1.3 on page 34</a> for more information. |
| Pre-Shared Key  | Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.   |
| Back            | Click <b>Back</b> to go to the <b>Site Survey</b> screen to select and connect to another network.   |
| Next            | Click <b>Next</b> to confirm your selections and advance to the <b>Confirm New Settings</b> screen. Refer to <a href="#">Section 4.2.2 on page 47</a> .  |
| Exit            | Click <b>Exit</b> to return to the <b>Site Survey</b> screen without saving.   |

#### 4.2.1.3 WPA-RADIUS/WPA2-RADIUS

**Figure 22** Security Setting: WPA-RADIUS/WPA2-RADIUS

The screenshot shows a 'Security Setting' window with the following fields and options:

- Encryption Type:** TKIP (dropdown menu)
- Authentication Type:** PEAP (dropdown menu)
- Login Name:** (text input field)
- Password:** (password input field)
- Validate Server Certificate**(Click to Enable or Disable)
- PEAP Inner EAP:** MSCHAPV2 (dropdown menu)

At the bottom right, there are three buttons: **Back**, **Next**, and **Exit**.

The following table describes the labels in this screen.

**Table 7** Security Setting: WPA-RADIUS/WPA2-RADIUS

| LABEL               | DESCRIPTION  |
|---------------------|--|
| Encryption Type     | The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>Select the encryption type ( <b>TKIP</b> or <b>AES</b> ) for data encryption.<br>Refer to <a href="#">Section 3.2.1.3 on page 34</a> for more information. |
| Authentication Type | The type of authentication you use depends on the RADIUS server or AP.<br>Select an authentication method from the drop down list. Options are <b>TLS</b> and <b>PEAP</b> .  |
| Login Name          | Enter a user name.<br>This is the user name that you or an administrator set up on a RADIUS server.  |

**Table 7** Security Setting: WPA-RADIUS/WPA2-RADIUS

| LABEL                       | DESCRIPTION  |
|-----------------------------|--|
| Password                    | This field is not available when you select <b>TLS</b> in the <b>Authentication Type</b> field. Enter the password associated with the user name above.  |
| Certificate                 | This field is only available when you select <b>TLS</b> in the <b>Authentication Type</b> field. Select a certificate used by the authentication server to authenticate the G-120.<br><b>Note:</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. |
| Validate Server Certificate | Select the check box to check the certificate of the authentication server.  |
| PEAP Inner EAP              | This field is only available when you select <b>PEAP</b> in the <b>Authentication Type</b> field.<br>The PEAP method used by the RADIUS server or AP for client authentication is <b>MS CHAP v2</b> .  |
| Back                        | Click <b>Back</b> to go to the <b>Site Survey</b> screen to select and connect to another network.   |
| Next                        | Click <b>Next</b> to confirm your selections and advance to the <b>Confirm New Settings</b> screen. Refer to <a href="#">Section 4.2.2 on page 47</a> .  |
| Exit                        | Click <b>Exit</b> to return to the <b>Site Survey</b> screen without saving.   |

#### 4.2.1.4 RADIUS

Configure IEEE 802.1x security with various authentication methods in this screen.

**Figure 23** Security Setting: RADIUS

The screenshot shows a window titled "Security Setting" with the following fields and controls:

- Authentication Type:** A dropdown menu with "PEAP" selected.
- Login Name:** An empty text input field.
- Password:** An empty text input field.
- Validate Server Certificate(Click to Enable or Disable)**
- PEAP Inner EAP:** A dropdown menu with "MS-CHAP-V2" selected.
- At the bottom right, there are three buttons: "Back", "Next", and "Exit".

The following table describes the labels in this screen.

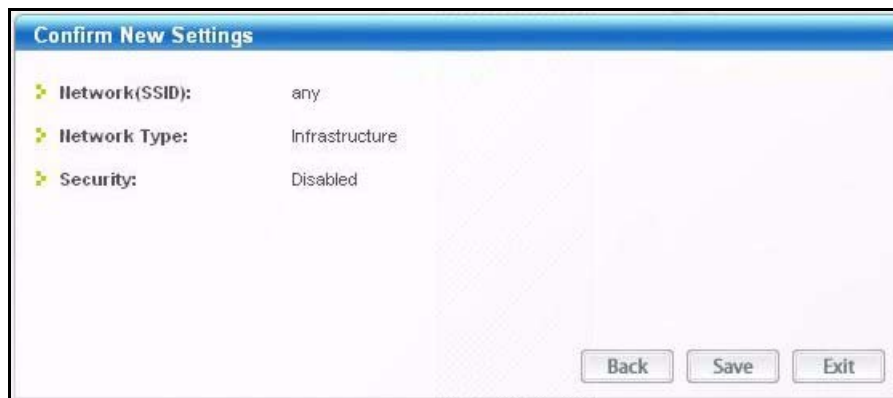
**Table 8** Security Setting: RADIUS

| LABEL                       | DESCRIPTION  |
|-----------------------------|--|
| Authentication Type         | The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are <b>TLS</b> and <b>PEAP</b> .   |
| Login Name                  | Enter a user name.<br>This is the user name that you or an administrator set up on a RADIUS server.  |
| Password                    | This field is not available when you select <b>TLS</b> in the <b>Authentication Type</b> field. Enter the password associated with the user name above.  |
| Certificate                 | This field is only available when you select <b>TLS</b> in the <b>Authentication Type</b> field. Select a certificate used by the authentication server to authenticate the G-120.<br><b>Note:</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. |
| Validate Server Certificate | Select the check box to check the certificate of the authentication server.  |
| PEAP Inner EAP              | This field is only available when you select <b>PEAP</b> in the <b>Authentication Type</b> field.<br>The PEAP method used by the RADIUS server or AP for client authentication is <b>MS CHAP v2</b> .  |
| Back                        | Click <b>Back</b> to go to the <b>Site Survey</b> screen to select and connect to another network.   |
| Next                        | Click <b>Next</b> to confirm your selections and advance to the <b>Confirm New Settings</b> screen. Refer to <a href="#">Section 4.2.2 on page 47</a> .  |
| Exit                        | Click <b>Exit</b> to return to the <b>Site Survey</b> screen without saving.   |

## 4.2.2 Confirm New Settings

Use this screen to confirm and save the security settings.

**Figure 24** Confirm New Settings



The following table describes the labels in this screen.

**Table 9** Confirm New Settings

| <b>LABEL</b>   | <b>DESCRIPTION</b>  |
|----------------|---|
| Network (SSID) | This field displays the <b>SSID</b> previously entered.   |
| Network Type   | This field displays the network type ( <b>Infrastructure</b> or <b>Ad-Hoc</b> ) of the wireless device.   |
| Security       | This field shows whether data encryption is activated ( <b>WEP, WPA-PSK, WPA-RADIUS, RADIUS, WPA2-RADIUS, WPA2-PSK</b> ) or inactive ( <b>Disabled</b> ). |
| Back           | Click <b>Back</b> to return to the previous screen.   |
| Save           | Click <b>Save</b> to save the changes back to the G-120 and display the <b>Link Info</b> screen.  |
| Exit           | Click <b>Exit</b> to discard changes and return to the <b>Site Survey</b> screen.   |

## 4.3 The Profile Screen

A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the G-120, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the G-120 cannot connect to a network.

If you do not configure and activate a profile, each time you start the G-120, the G-120 uses the default profile to connect to any available network with security disabled.

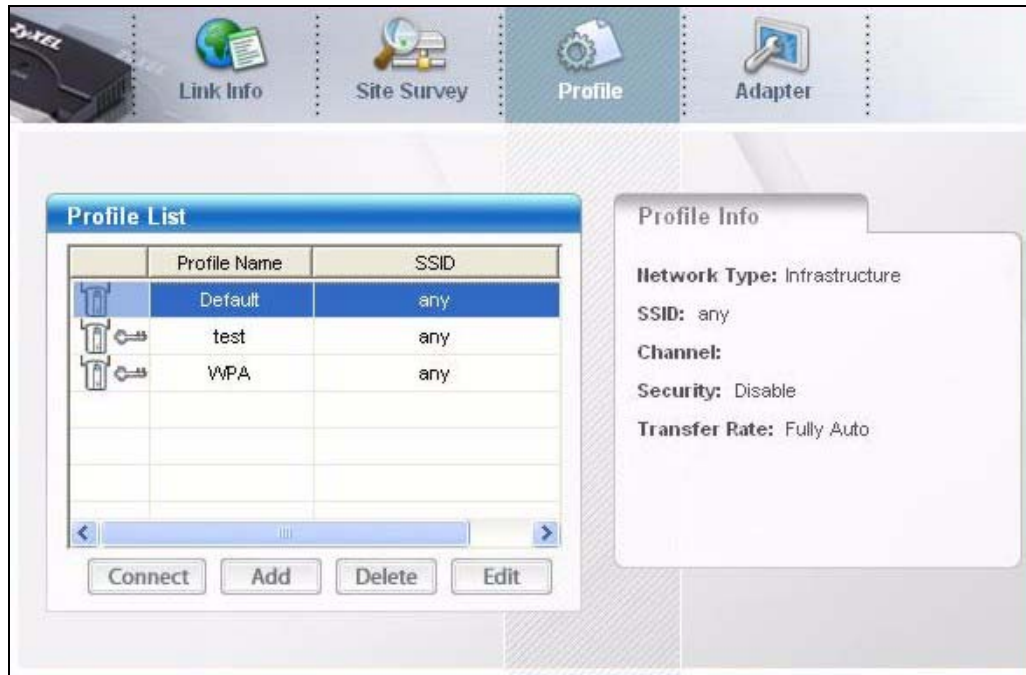
The default profile is a profile that allows you to connect to any SSID without security.

Click the **Profile** tab in the ZyXEL utility program to display the **Profile** screen as shown next.

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











Figure 25 Profile



The following table describes the labels in this screen.

Table 10 Profile

| LABEL   | DESCRIPTION  |
|---|--|
| Profile List  | Click a column heading to sort the entries.  |
|  ,<br> ,<br> or<br> |  denotes that the wireless device is in infrastructure mode and the wireless security is activated.<br> denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.<br> denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.<br> denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated. |
| Profile Name  | This is the name of the pre-configured profile.  |
| SSID  | This is the SSID of the wireless network to which the selected profile associate.  |
| Connect   | To use and activate a previously saved network profile, select a pre-configured profile name in the table and click <b>Connect</b> .   |
| Add   | To add a new profile into the table, click <b>Add</b> .  |
| Delete  | To delete an existing wireless network configuration, select a profile in the table and click <b>Delete</b> .  |
| Edit  | To edit an existing wireless network configuration, select a profile in the table and click <b>Edit</b> .  |
| Profile Info  | The following fields display detail information of the selected profile in the <b>Profile List</b> table.  |
| Network Type  | This field displays the network type ( <b>Infrastructure</b> or <b>Ad-Hoc</b> ) of the profile.  |
| SSID  | This field displays the SSID (Service Set Identifier) of the profile.  |

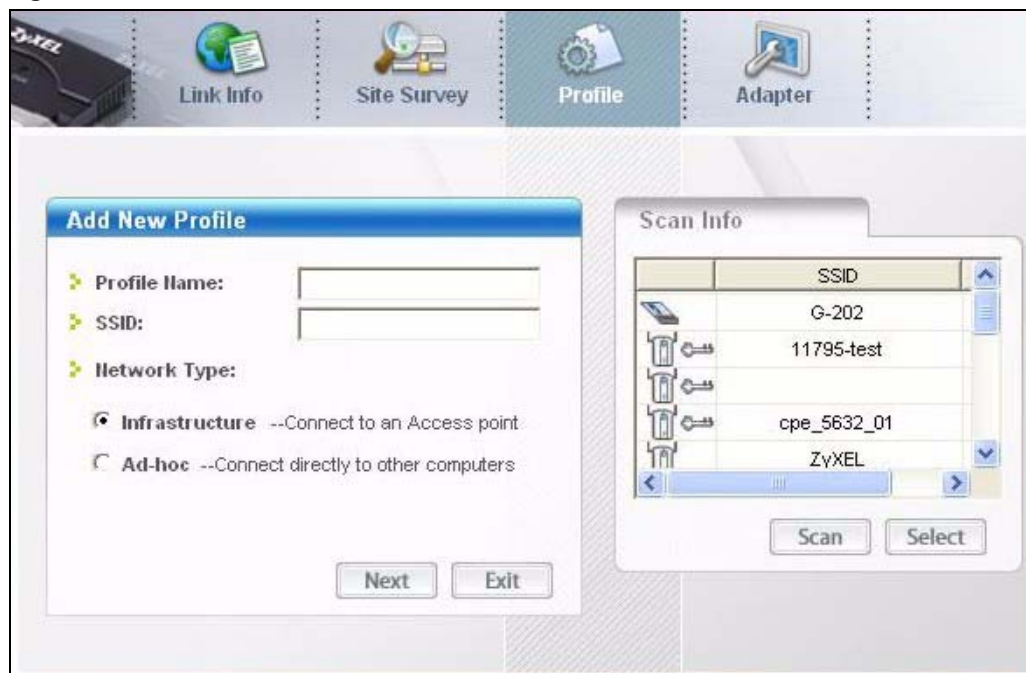
**Table 10** Profile (continued)

| LABEL         | DESCRIPTION  |
|---------------|--|
| Channel       | This field displays the channel number used by the profile.  |
| Security      | This field shows whether data encryption is activated ( <b>WEP, WPA-PSK, WPA-RADIUS, RADIUS, WPA2-RADIUS, WPA2-PSK</b> ) or inactive ( <b>Disable</b> ). |
| Transfer Rate | This field displays the transmission speed of the selected profile in megabits per second (Mbps).  |

### 4.3.1 Adding a New Profile

Follow the steps below to add a new profile.

- 1 Click **Add** in the **Profile** screen. An **Add New Profile** screen displays as shown next. Click **Next** to continue.

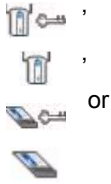




**Figure 26** Profile: Add a New Profile

The following table describes the labels in this screen.

**Table 11** Profile: Add a New Profile

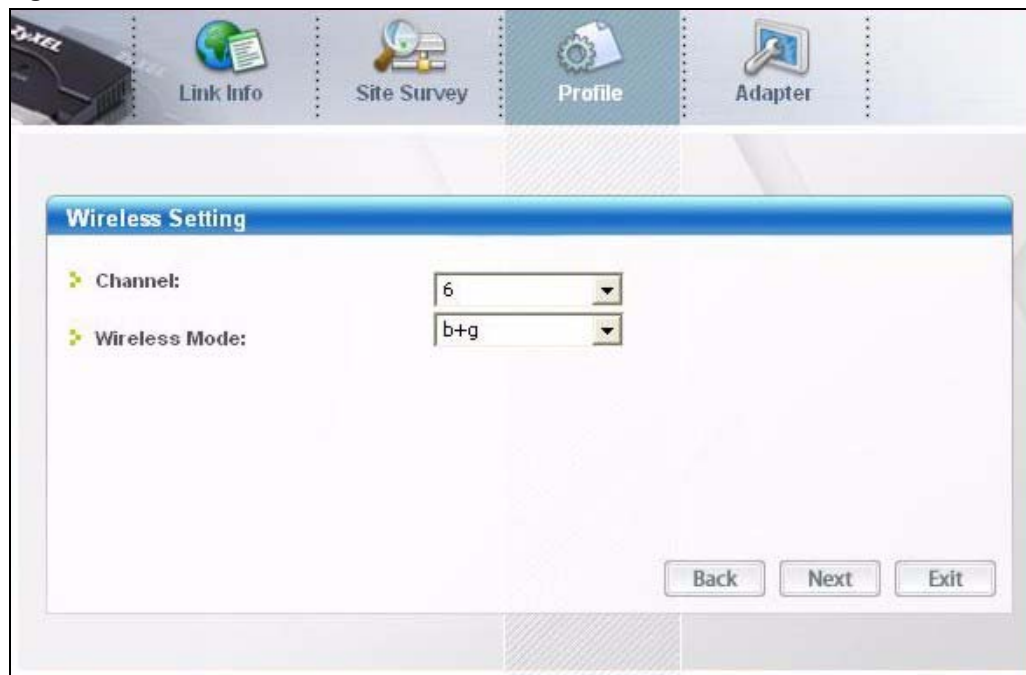
| LABEL           | DESCRIPTION   |
|-----------------|---|
| Add New Profile |   |
| Profile Name    | Enter a descriptive name in this field.   |
| SSID            | Select an available wireless device in the <b>Scan Info</b> table and click <b>Select</b> , or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter <b>Any</b> to have the G-120 associate to any AP or roam between any infrastructure wireless networks. |

**Table 11** Profile: Add a New Profile (continued)

| LABEL   | DESCRIPTION   |
|---|---|
| Network Type  | Select <b>Infrastructure</b> to associate to an AP. Select <b>Ad-Hoc</b> to associate to a peer computer.   |
| Next  | Click <b>Next</b> to go to the next screen.   |
| Exit  | Click <b>Exit</b> to go back to the previous screen without saving.   |
| Scan Info   | This table displays the information of the available wireless networks within the transmission range.   |
|  | <p> denotes that the wireless device is in infrastructure mode and the wireless security is activated.</p> <p> denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.</p> <p> denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.</p> <p> denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated.</p> |
| SSID  | This field displays the SSID (Service Set Identifier) of each AP or peer device.  |
| Scan  | Click <b>Scan</b> to search for available wireless devices within transmission range.   |
| Select  | <p>Select an available wireless device in the table and click <b>Select</b> to add it to this profile.</p> <p>Whenever you activate this profile, the G-120 associates to the selected wireless network only.</p>   |

- 2** If you select the **Infrastructure** network type in the previous screen, skip to step **3**. If you select the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a channel number and click **Next** to continue.

**Note:** To associate to an ad-hoc network, you must use the same channel as the peer computer.

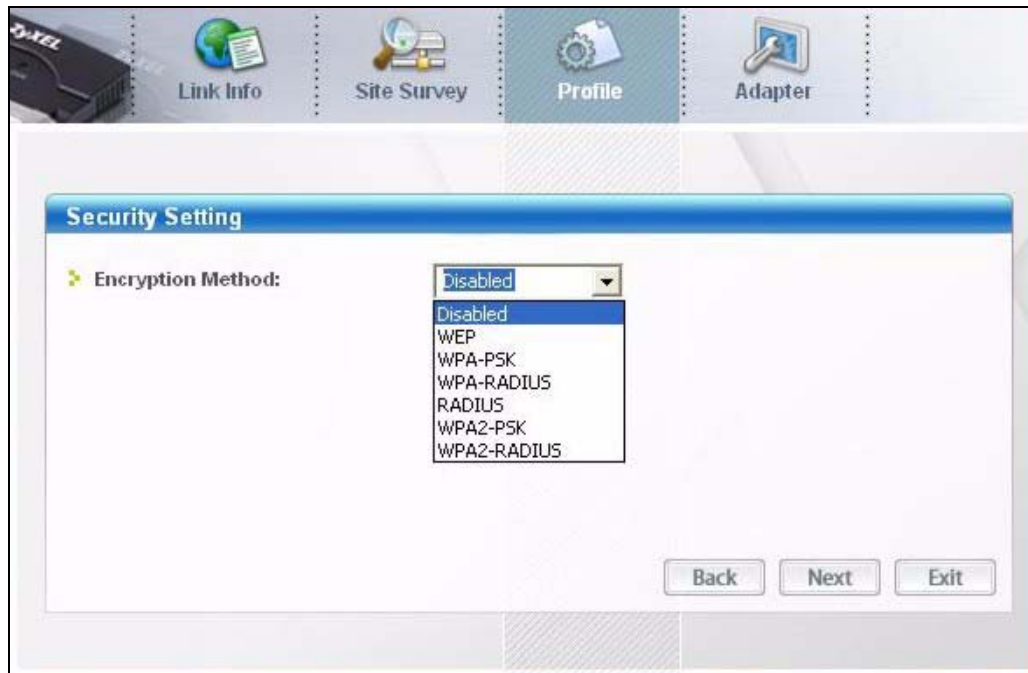
**Figure 27** Profile: Select a Channel

The following table describes the labels in this screen.

**Table 12** Profile: Select a Channel

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Wireless Settings |   |
| Channel           | Select a channel number from the drop-down list box. To associate to an ad-hoc network, you must use the same channel as the peer computer. |
| Wireless Mode     | This displays <b>b+g</b> and allows the G-120 to connect to either an IEEE 802.11g or IEEE 802.11b wireless device.                         |

- If you select **Infrastructure** network type in the first screen, select **WEP**, **WPA-PSK**, **WPA-RADIUS**, **WPA2-PSK**, **WPA2-RADIUS** or **RADIUS** from the drop-down list box to enable data encryption. If you select **Ad-Hoc** network type in the first screen, you can only use **WEP** encryption method. Otherwise, select **Disabled** to allow the G-120 to communicate with the access points or other peer wireless computers without any data encryption and skip to step 5.

**Figure 28** Profile: Security Settings

- 4 The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the APs or other peer wireless computers as they are on the G-120. Refer to [Section 4.2.1 on page 43](#) for detailed information on wireless security configuration.

**Figure 29** Profile: Security Settings

- 5 This read-only screen shows a summary of the new profile settings. Verify that the settings are correct. Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen. Otherwise, click **Exit** to go back to the **Profile** screen without saving.

**Figure 30** Profile: Confirm New Settings

**6** To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button. You can activate only one profile at a time.

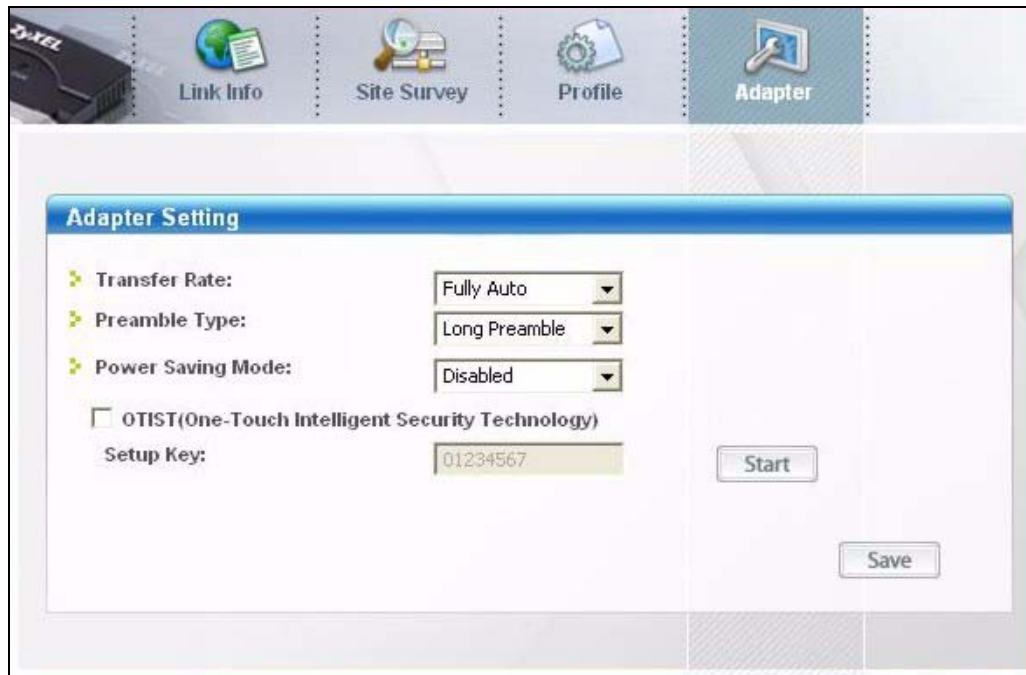
**Note:** Once you activate a profile, the ZyXEL utility will use that profile the next time it is started.

**Figure 31** Profile: Activate the Profile

## 4.4 The Adapter Screen

To set the advanced features on the G-120, click the **Adapter** tab.

Figure 32 Adapter



The following table describes the labels in this screen.

Table 13 Adapter

| LABEL   | DESCRIPTION   |
|---|---|
| Adapter Setting                                   |   |
| Transmission Rate                                 | In most networking scenarios, the factory default <b>Fully Auto</b> setting is the most efficient and allows your G-120 to operate at the highest possible transmission (data) rate.<br>If you want to select a specific transmission rate, select one that the AP or peer wireless device supports.  |
| Preamble Type                                     | Preamble is used to signal that data is coming to the receiver. Select the preamble type that the AP uses.<br><b>Short Preamble</b> increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support <b>Long Preamble</b> , but not all support short preamble.<br>Select <b>Auto</b> to have the G-120 automatically use short preamble when all access point or wireless stations support it; otherwise the G-120 uses long preamble.<br><b>Note:</b> The G-120 and the access point or wireless stations <b>MUST</b> use the same preamble mode in order to communicate. |
| Power Saving Mode                                 | Select <b>Enabled</b> to save power (especially for notebook computers). This forces the G-120 to go to sleep mode when it is not transmitting data.<br>When you select <b>Disabled</b> , the G-120 will never go to sleep mode.  |
| OTIST (One-Touch Intelligent Security Technology) | Select this check box to enable OTIST.  |

**Table 13** Adapter (continued)

| LABEL     | DESCRIPTION   |
|-----------|---|
| Setup Key | Enter the same setup key (up to eight printable characters) as the ZyXEL AP or wireless router to which you want to associate. The default OTIST setup key is "01234567".<br><b>Note:</b> If you change the OTIST setup key on the ZyXEL AP or wireless router, you must also make the same change here.  |
| Start     | Click <b>Start</b> to encrypt the wireless security data using the setup key and have the ZyXEL AP or wireless router set your G-120 to use the same wireless settings as the ZyXEL AP or wireless router. You must also activate and start OTIST on the ZyXEL AP or wireless router all within three minutes. See <a href="#">Section 3.3 on page 34</a> for more information. |
| Save      | Click <b>Save</b> to save the changes back to the G-120 and return to the <b>Link Info</b> screen.  |




# CHAPTER 5

## Maintenance

This chapter describes how to uninstall or upgrade the ZyXEL utility.

### 5.1 The About Screen

The **About** screen displays driver and utility version numbers of the G-120. To display the screen as shown below, click the about (  ) button.

**Figure 33** About



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

**Table 14** About

| LABEL           | DESCRIPTION  |
|-----------------|--|
| Driver Version  | This field displays the version number of the G-120 driver.  |
| Utility Version | This field displays the version number of the ZyXEL utility. |

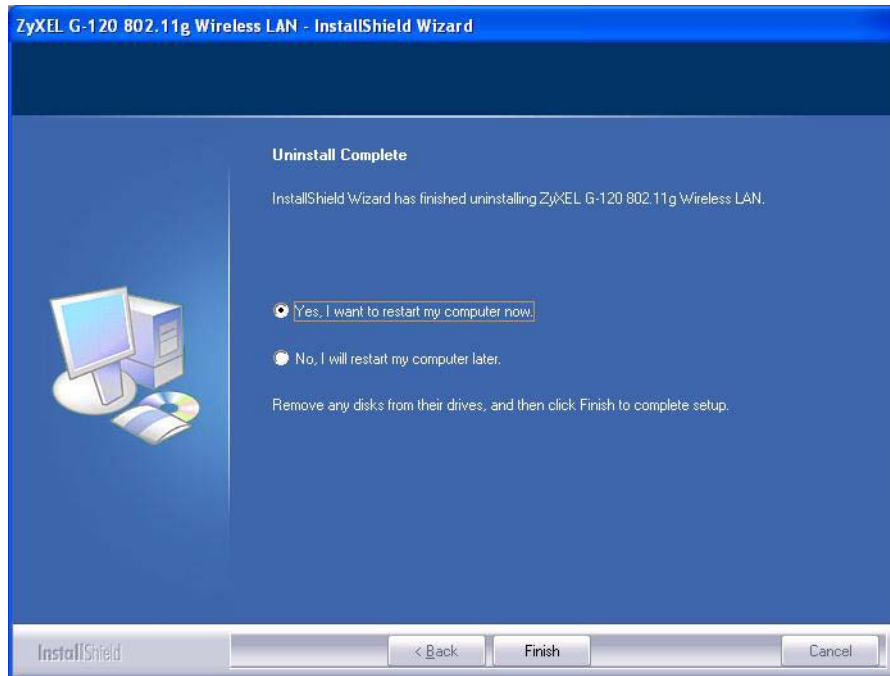
### 5.2 Uninstalling the ZyXEL Utility

Follow the steps below to remove (or uninstall) the ZyXEL utility from your computer.

- 1** Click **Start**, **(All) Programs**, **ZyXEL G-120 Utility**, **Uninstall ZyXEL G-120 Software**.
- 2** When prompted, click **OK** or **Yes** to remove the driver and the utility software.

**Figure 34** Uninstall: Confirm

- 3 Click **Finish** to complete uninstalling the software and restart the computer when prompted.

**Figure 35** Uninstall: Finish

## 5.3 Upgrading the ZyXEL Utility

**Note:** Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

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 [Section 5.2 on page 57](#) to remove the current ZyXEL utility from your computer.
- 3 Restart your computer when prompted.
- 4 Disconnect the G-120 from your computer.
- 5 Double-click on the setup program for the new utility to start the ZyXEL utility installation.

- 6 Insert the G-120 and check the version numbers in the **About** screen to make sure the new utility is installed properly.



# CHAPTER 6

## 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.

### 6.1 Problems Starting the ZyXEL Utility

**Table 15** Troubleshooting Starting ZyXEL Utility

| PROBLEM                                     | CORRECTIVE ACTION  |
|---|--|
| Cannot start the ZyXEL Wireless LAN utility | <p>Make sure the G-120 is properly inserted and the LED(s) is on. Refer to the Quick Start Guide for the LED descriptions.</p> <p>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 G-120 under <b>Network Adapter</b>. (Steps may vary depending on the version of Windows).</p> <p>Install the G-120 in another computer.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.</p> |
| The ZyXEL utility icon does not display.    | <p>If you install the Funk Odyssey Client software on the computer, uninstall (remove) both the Funk Odyssey Client software and ZyXEL utility, and then install the ZyXEL utility again after restarting the computer.</p>  |

### 6.2 Problem with the Link Quality

**Table 16** Troubleshooting Link Quality

| PROBLEM   | CORRECTIVE ACTION  |
|---|--|
| 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 may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Lower the output power of each AP.</p> <p>Make sure there are not too many wireless stations connected to a wireless network.</p> |

## 6.3 Problems Communicating With Other Computers

**Table 17** Troubleshooting Communication Problem

| PROBLEM  | CORRECTIVE ACTION  |
|--|--|
| The computer with the G-120 installed cannot communicate with the other computer(s). | <p>In Infrastructure Mode</p> <ul style="list-style-type: none"><li>• Make sure that the AP and the associated computers are turned on and working properly.</li><li>• Make sure the G-120 computer and the associated AP use the same SSID.</li><li>• Change the AP and the associated wireless clients to use another radio channel if interference is high.</li><li>• Make sure that the computer and the AP share the same security option and key. Verify the settings in the <b>Profile Security Setting</b> screen.</li><li>• If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.</li></ul> <p>In Ad-Hoc (IBSS) Mode</p> <ul style="list-style-type: none"><li>• Verify that the peer computer(s) is turned on.</li><li>• Make sure the G-120 computer and the peer computer(s) are using the same SSID and channel.</li><li>• Make sure that the computer and the peer computer(s) share the same security settings.</li><li>• Change the wireless clients to use another radio channel if interference is high.</li></ul> |

# APPENDIX A

## Product Specifications

**Table 18** Product Specifications

| <b>PHYSICAL AND ENVIRONMENTAL</b> |  |
|-----------------------------------|--|
| Product Name                      | ZyXEL G-120 802.11g Wireless CardBus Card  |
| Interface                         | CardBus Type II  |
| Standards                         | IEEE 802.11b<br>IEEE 802.11g   |
| Network Architectures             | Infrastructure<br>Ad-Hoc   |
| Operating Frequencies             | 2.412-2.4835GHz  |
| Operating Channels                | IEEE 802.11b: 11 Channels (North America and Taiwan)<br>IEEE 802.11g: 11 Channels (North America and Taiwan)<br>IEEE 802.11b: 13 Channels (Europe)<br>IEEE 802.11g: 13 Channels (Europe) |
| Data Rate                         | IEEE 802.11b: 11, 5.5, 2, 1Mbps<br>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)<br>IEEE 802.11b: PBCC, Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK).                       |
| Operating Temperature             | 0 ~ 50 degrees Centigrade  |
| Storage Temperature               | -30 ~ 60 degrees Centigrade  |
| Operating Humidity                | 20 ~ 95% (non-condensing)  |
| Storage Humidity                  | 20 ~ 95% (non-condensing)  |
| Power                             | IEEE 802.11g: TX: 450mA RX: 345mA<br>IEEE 802.11b: TX: 450mA RX: 345mA   |
| Voltage                           | 3.3V   |
| Weight                            | 40 g   |
| Dimension                         | (W) 115 mm × (D) 53 mm × (H) 6 mm  |
| <b>RADIO SPECIFICATIONS</b>       |  |
| Media Access Protocol             | IEEE 802.11  |
| Frequency                         | 2.4 ~ 2.484GHz (Industrial Scientific Medical Band)  |
| Channels                          | 1~11 Channels (USA, Canada and Taiwan)<br>1~13 Channels (Europe)   |
| Data Rate                         | IEEE 802.11g (OFDM): 6, 9, 12, 18, 24, 36, 48, 54 Mbps<br>IEEE 802.11b: 1, 2, 5.5, 11 Mbps   |

**Table 18** Product Specifications (continued)

|                                |  |
|--------------------------------|--|
| Modulation                     | IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps (OFDM)<br>IEEE 802.11b: 11, 5.5 Mbps (CCK), 2 Mbps (DQPSK), 1 Mbps (DBPSK) |
| Output Power                   | 18 dBm (typical) at 11Mbps CCK, QPSK, BPSK<br>15 dBm (typical) at 54Mbps OFDM  |
| RX Sensitivity                 | IEEE 802.11g (OFDM): 54 Mbps: < -70 dBm<br>IEEE 802.11b (CCK): 11 Mbps: < -85 dBm  |
| <b>SOFTWARE SPECIFICATIONS</b> |  |
| Device Drivers                 | Microsoft Windows 98 Second Edition, Windows ME, Windows 2000, Windows XP  |
| Security                       | 64/128/256-bit WEP<br>WPA/WPA-PSK/WPA2/WPA2-PSK<br>IEEE 802.1x   |



# APPENDIX B

## Management with Wireless Zero Configuration

This appendix shows you how to manage your G-120 using the Windows XP wireless zero 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.

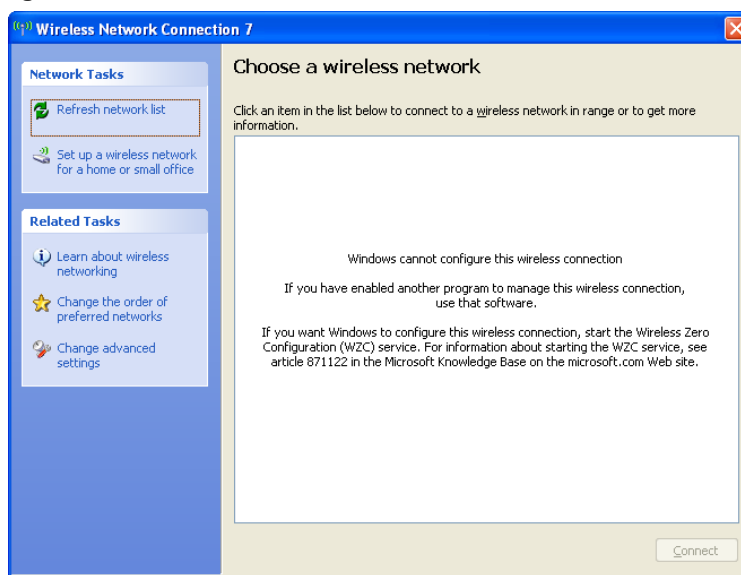
Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon ( ? ) in most screens, move the cursor to the item that you want the information about and click to view the help.

### Activating Wireless Zero Configuration

Make sure the the ZyXEL utility is disabled. Refer to [Section 1.4 on page 23](#) to enable WZC.

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

**Figure 36** 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.

**Figure 37** Windows XP SP2: System Tray Icon



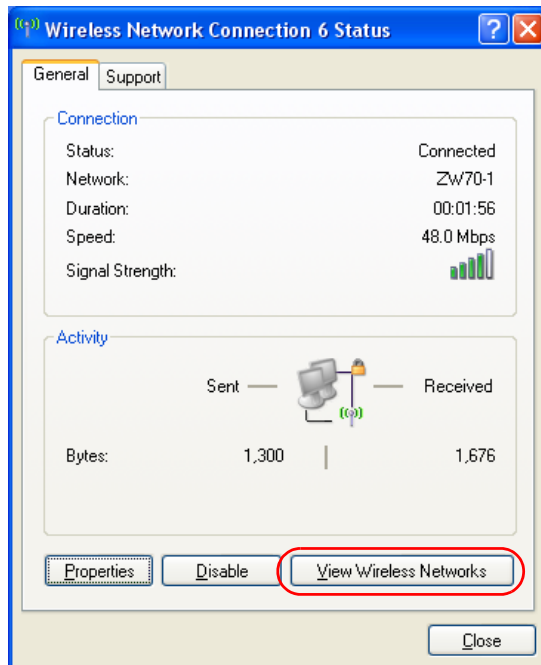
The type of the wireless network icon in Windows XP SP2 indicates the status of the G-120. Refer to the following table for details.

**Table 19** Windows XP SP2: System Tray Icon

| ICON | DESCRIPTION   |
|------|---|
|      | The G-120 is connected to a wireless network.   |
|      | The G-120 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 G-120 is not connected to a wireless network.   |

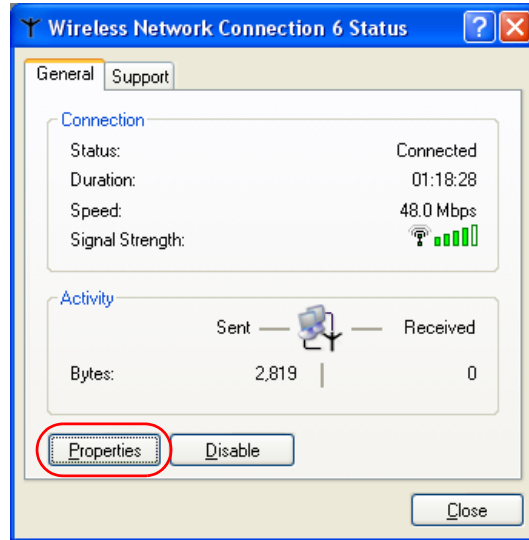
- 2 Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.

**Figure 38** Windows XP SP2: Wireless Network Connection Status



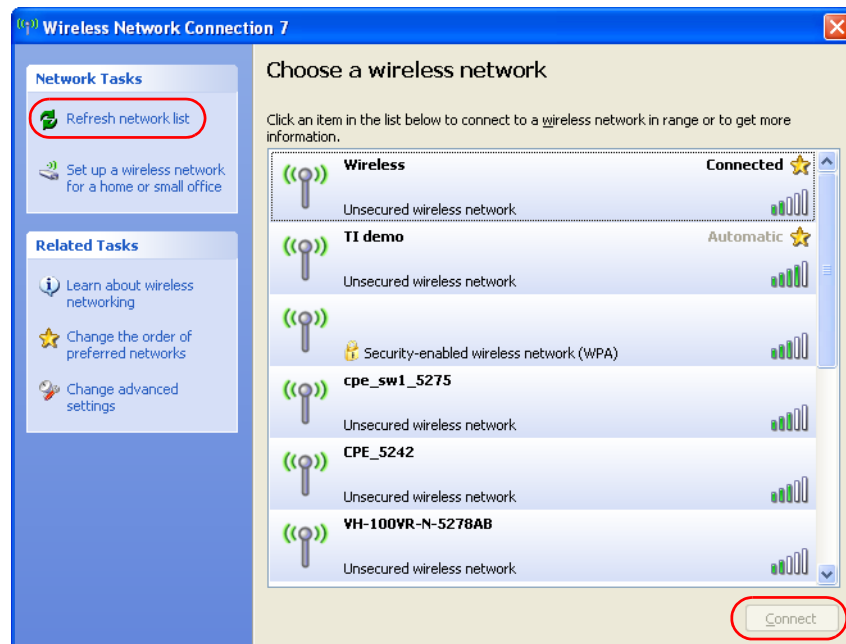
Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.

**Figure 39** 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.

**Figure 40** Windows XP SP2: Wireless Network Connection



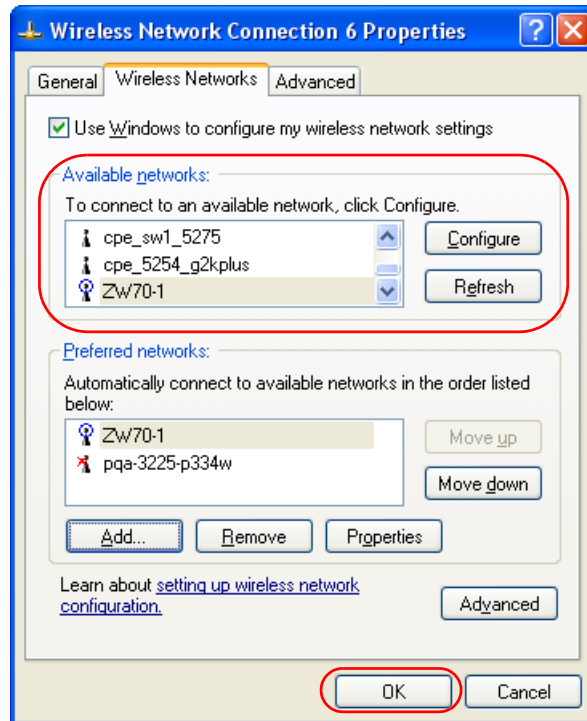
The following table describes the icons in the wireless network list.

**Table 20** Windows XP SP2: Wireless Network Connection

| ICON  | DESCRIPTION   |
|---|---|
|  | This denotes that 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 G-120 tries to associate to the preferred network first in the order that you specify. Refer to the section on ordering the preferred networks 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.

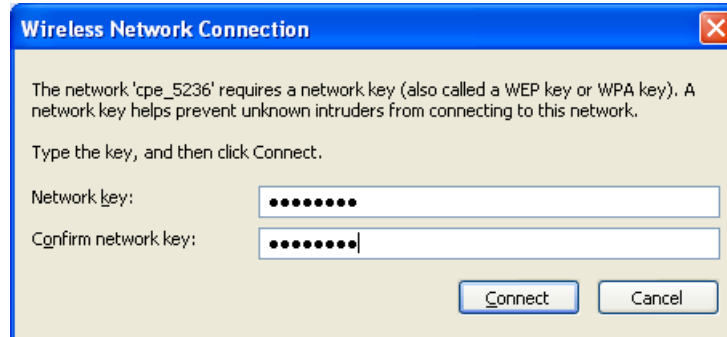
**Figure 41** Windows XP SP1: Wireless Network Connection Properties



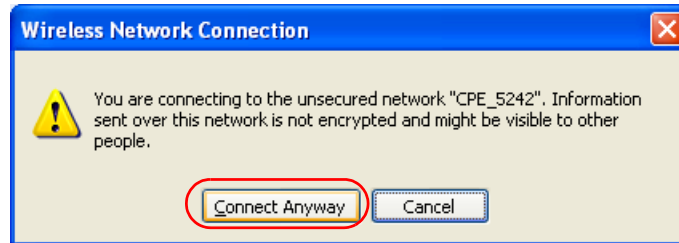
4. Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP and click **Connect**. Refer to the section about security settings 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.

**Figure 42** Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK






**Figure 43** Windows XP SP2: Wireless Network Connection: No Security



- 5 Verify that you have successfully connected to the selected network and check the 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.

**Table 21** Windows XP: Wireless Networks

| ICON  | DESCRIPTION   |
|---|---|
|  | This denotes the wireless network is an available wireless network. |
|  | This denotes the G-120 is associated to the wireless network.       |
|  | This denotes the wireless network is not available.                 |

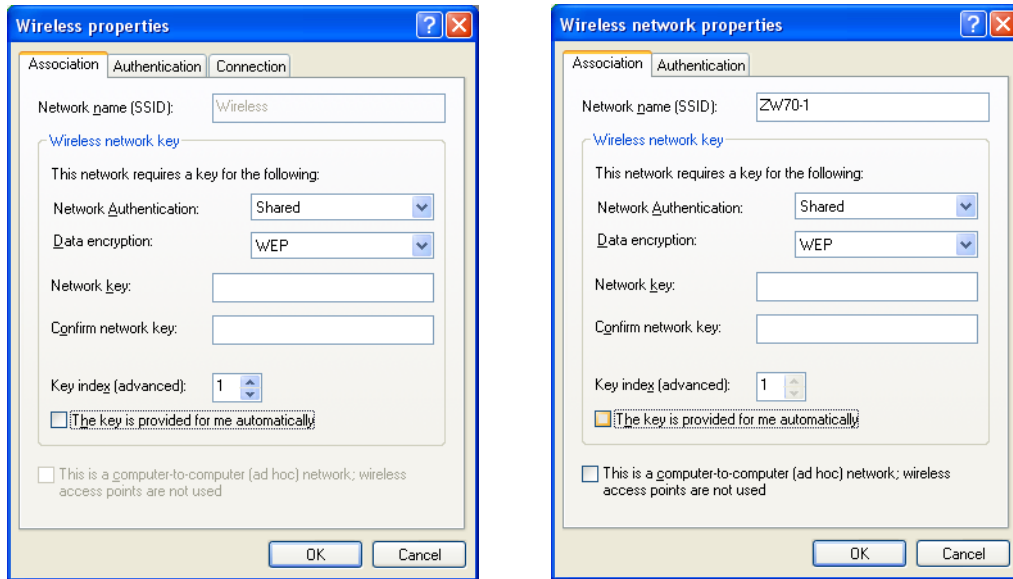
## Security Settings

When you configure the G-120 to connect to a secure network but the security settings are not yet enabled on the G-120, 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.

**Figure 44** Windows XP: Wireless (network) properties: Association



The following table describes the labels in this screen.

**Table 22** Windows XP: Wireless (network) properties: Association

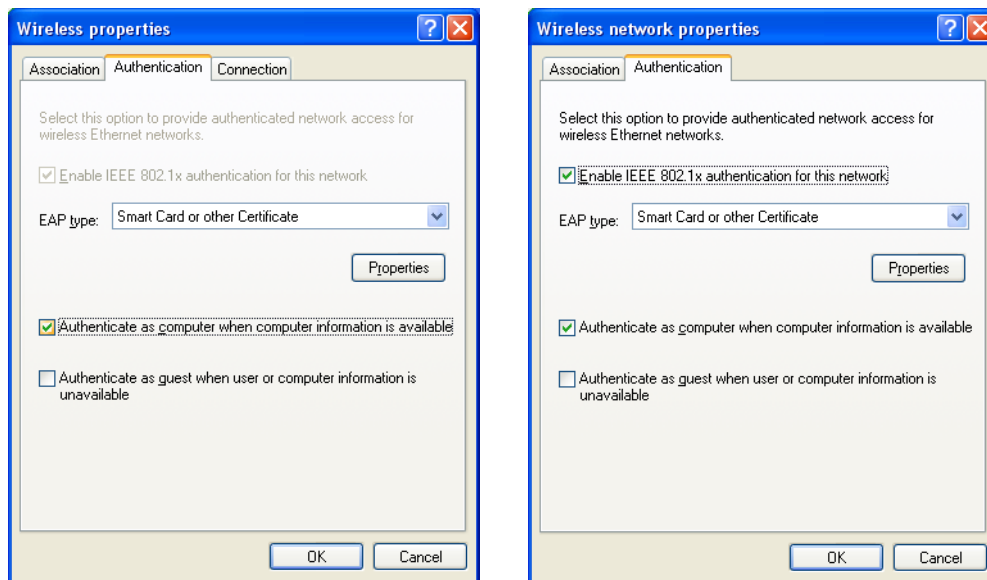
| LABEL                                    | DESCRIPTION   |
|--|---|
| Network name (SSID)                      | This field displays the SSID (Service Set Identifier) of each wireless network.   |
| Network Authentication                   | This field automatically shows the authentication method ( <b>Share</b> , <b>Open</b> , <b>WPA</b> or <b>WPA-PSK</b> ) used by the selected network.  |
| 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 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.   |
| Confirm network key                      | Enter the key again for confirmation.   |
| Key index (advanced)                     | Select a default WEP key to use for data encryption.<br>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 G-120 a key.   |

**Table 22** Windows XP: Wireless (network) properties: Association (continued)

| LABEL  | DESCRIPTION  |
|--|--|
| 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.

**Figure 45** Windows XP: Wireless (network) properties: Authentication

The following table describes the labels in this screen.

**Table 23** 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.  |

**Table 23** Windows XP: Wireless (network) properties: Authentication (continued)

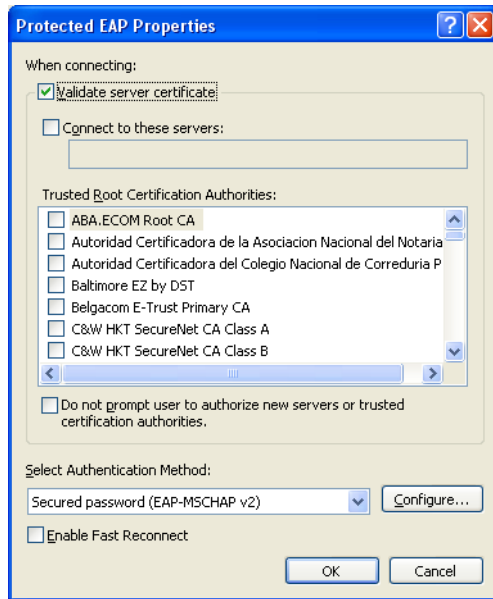
| LABEL  | DESCRIPTION  |
|--|--|
| Authenticate as computer when computer information is available        | Select this check box to have the computer send its information to the network for authentication when a user is not logged on.                    |
| Authenticate as guest when user or computer 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 leave 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

**Figure 46** Windows XP: Protected EAP Properties





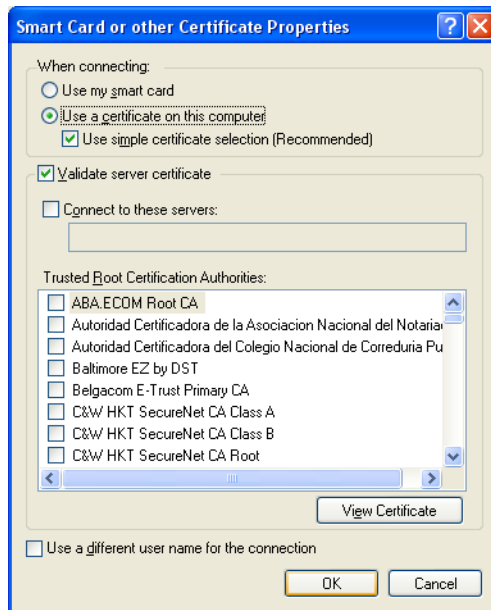
The following table describes the labels in this screen.

**Table 24** 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.<br><br><b>Note:</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. |
| Do not prompt user to authorize new server or trusted certification authorities. | Select this check box to verify 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

**Figure 47** Windows XP: Smart Card or other Certificate Properties



The following table describes the labels in this screen.

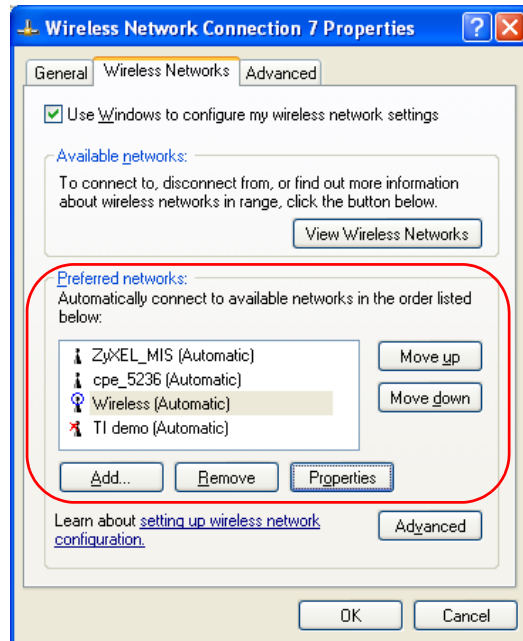
**Table 25** Windows XP: Smart Card or other Certificate Properties

| 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.   |
| Trusted Root Certification Authorities:       | Select a trusted certification authority from the list below.<br><b>Note:</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. |
| 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.  |

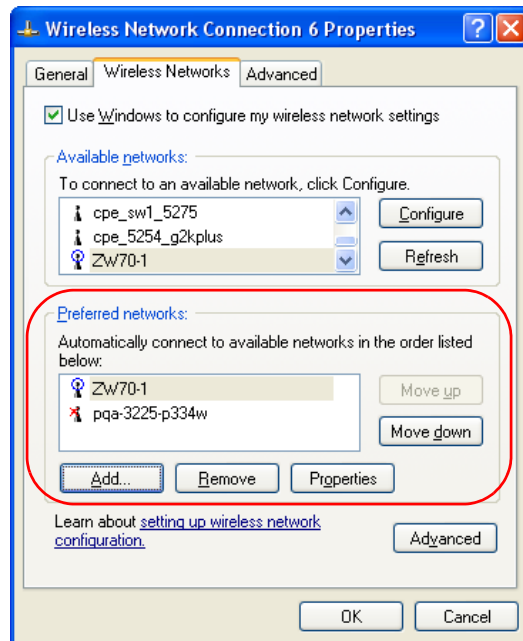
## Ordering the Preferred Networks

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 [Figure 40 on page 67](#)). The screen displays as shown.

**Figure 48** 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.

**Figure 49** Windows XP SP1: Wireless Networks: Preferred Networks

- Whenever the G-120 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

## Wireless Security

### Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

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 IEEE 802.1x. .

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.

### 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 IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

**Note:** EAP-MD5 cannot be used with Dynamic WEP Key Exchange

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 authentication types.

**Table 26** 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       |

## WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include 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.

WPA and WPA2 regularly change and rotate 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 PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

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

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

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

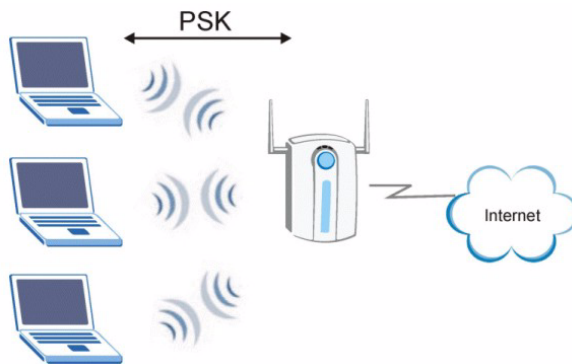


## WPA(2)-PSK Application Example

A WPA(2)s-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 or 64 hexadecimal 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 and wireless clients use the pre-shared key to generate a common PMK.
- 4** The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 50** WPA-PSK Authentication

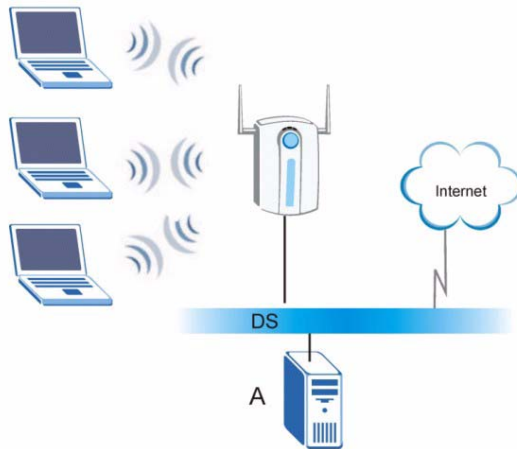


## WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) 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 51** WPA(2) with RADIUS Application Example



## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 27** Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X                    |
|--|-------------------|------------------|--------------------------------|
| Open   | None              | No               | Disable                        |
|  |                   |                  | Enable without Dynamic WEP Key |
| Open   | WEP               | No               | Enable with Dynamic WEP Key    |
|  |                   | Yes              | Enable without Dynamic WEP Key |
|  |                   | Yes              | Disable                        |
| Shared   | WEP               | No               | Enable with Dynamic WEP Key    |
|  |                   | Yes              | Enable without Dynamic WEP Key |
|  |                   | Yes              | Disable                        |
| WPA  | TKIP/AES          | No               | Enable                         |
| WPA-PSK  | TKIP/AES          | Yes              | Disable                        |
| WPA2   | TKIP/AES          | No               | Enable                         |
| WPA2-PSK                                       | TKIP/AES          | Yes              | Disable                        |

# APPENDIX D

## Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

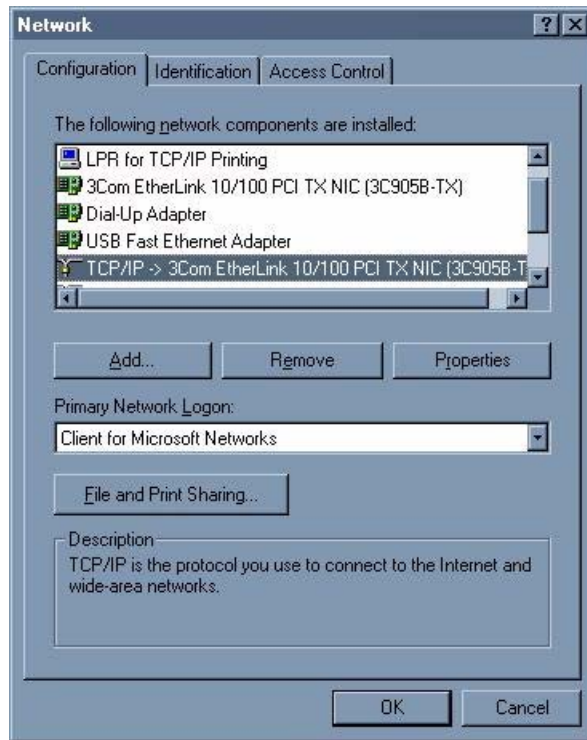
Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

### Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

**Figure 52** WIndows 95/98/Me: Network: Configuration

## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

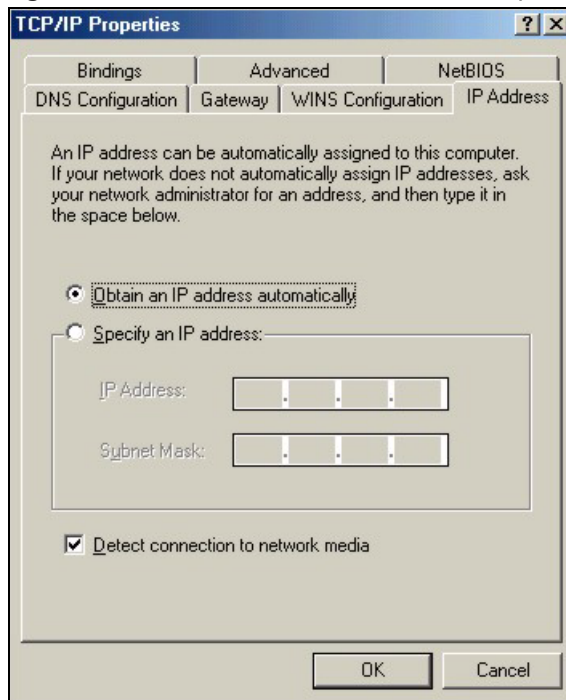
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

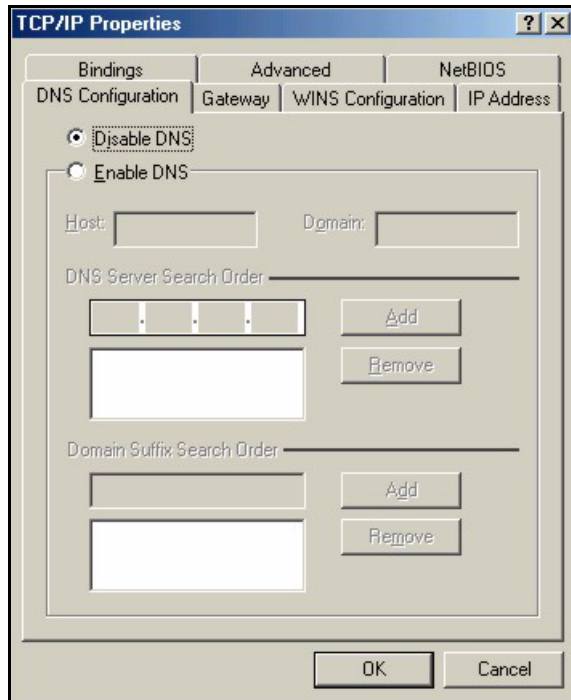
## Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 53** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 54** Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

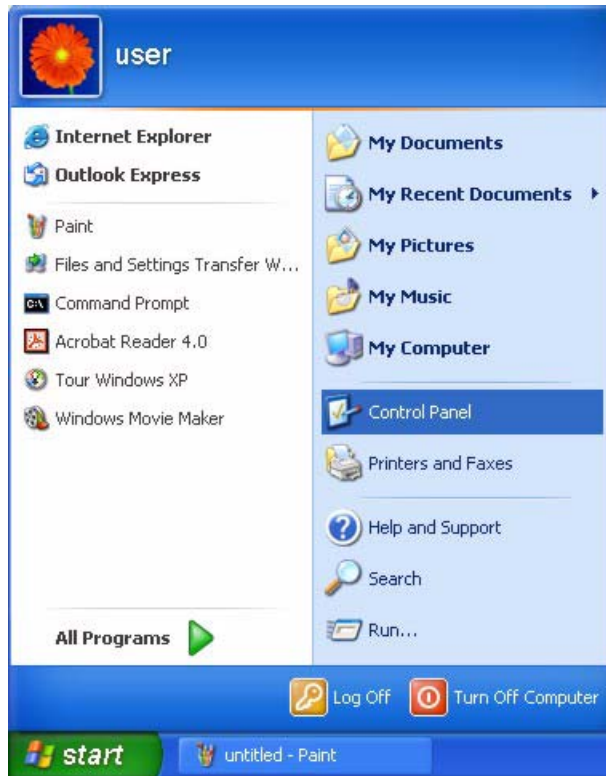
**5** Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Restart your computer when prompted.

## Verifying Settings

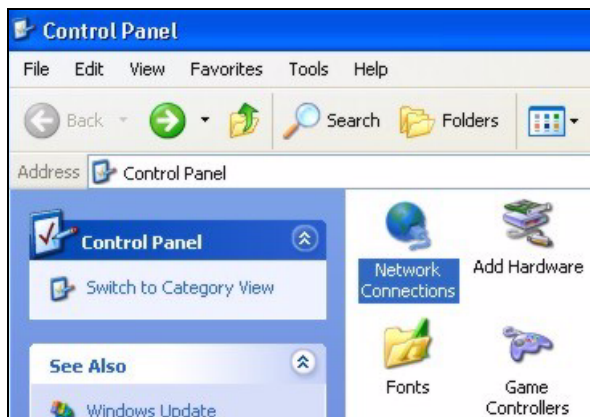
**1** Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

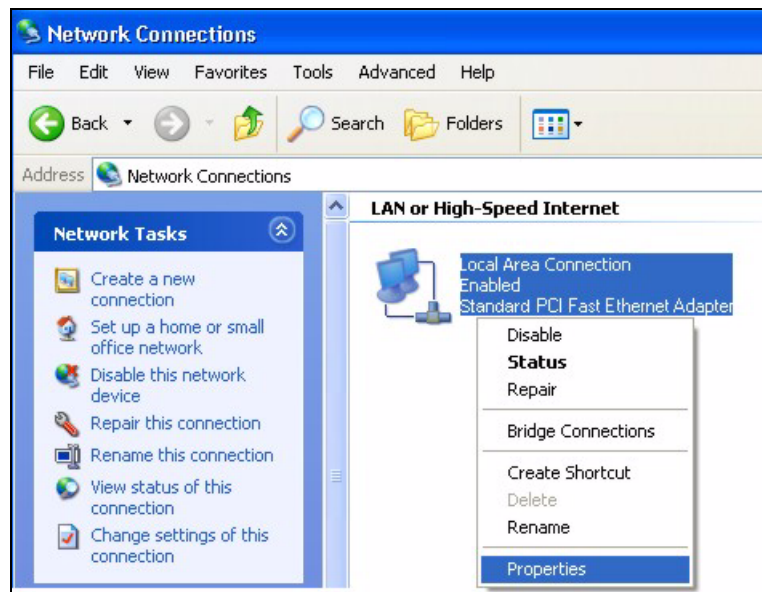
**1** For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

**Figure 55** Windows XP: Start Menu

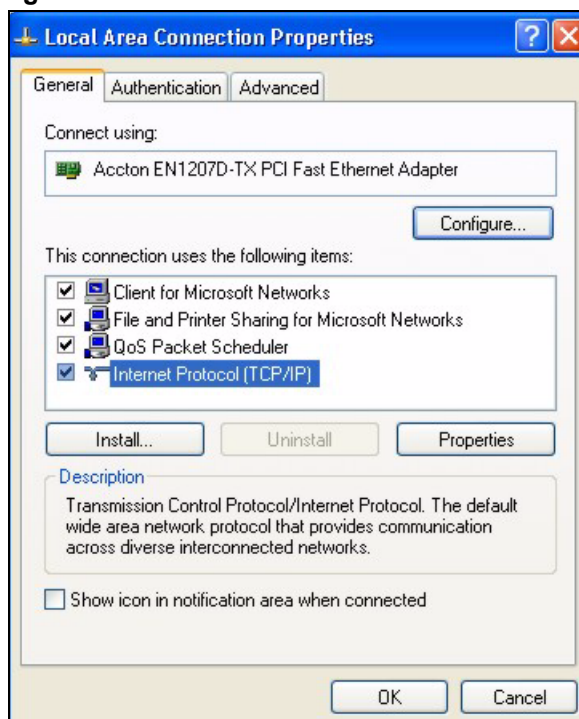
**2** For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 56** Windows XP: Control Panel

**3** Right-click **Local Area Connection** and then click **Properties**.

**Figure 57** Windows XP: Control Panel: Network Connections: Properties

- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

**Figure 58** Windows XP: Local Area Connection Properties

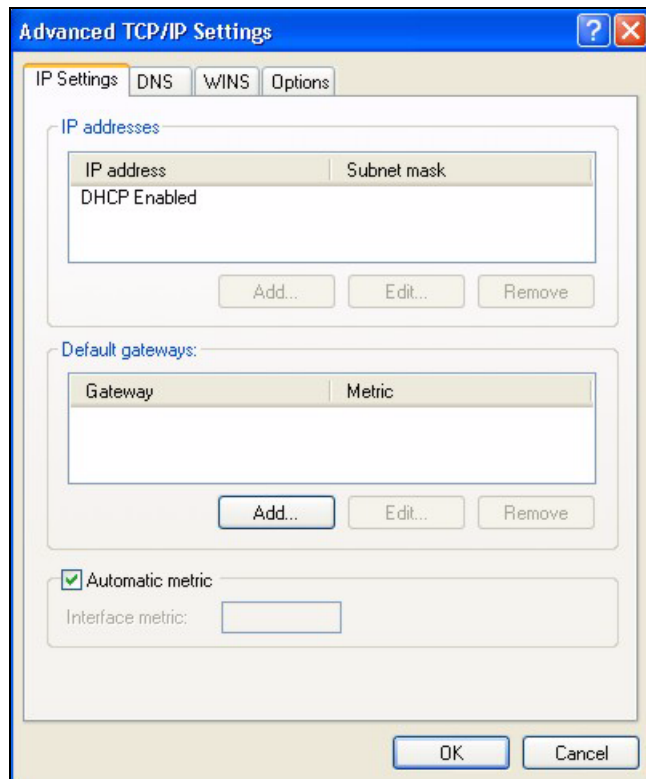
- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.



- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

**Figure 59** Windows XP: Advanced TCP/IP Settings



- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

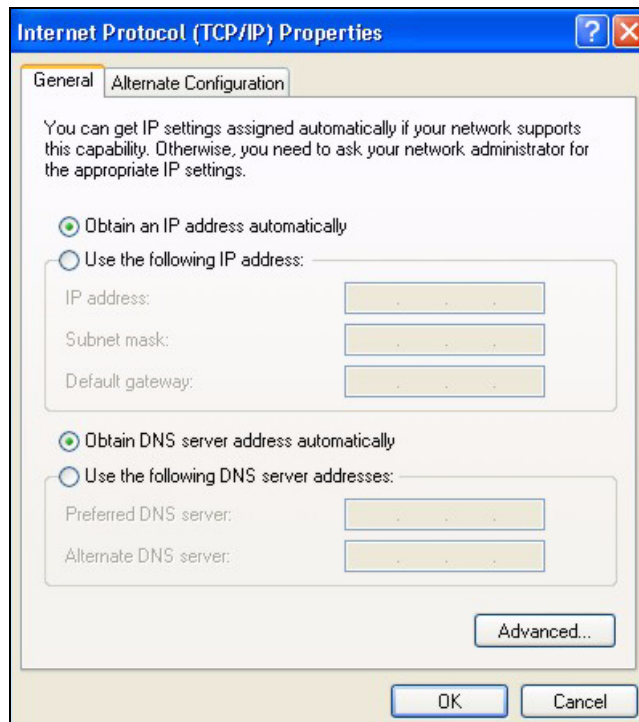
- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 60** Windows XP: Internet Protocol (TCP/IP) Properties



**8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

**9** Click **OK** to close the **Local Area Connection Properties** window.

**10** Restart your computer (if prompted).

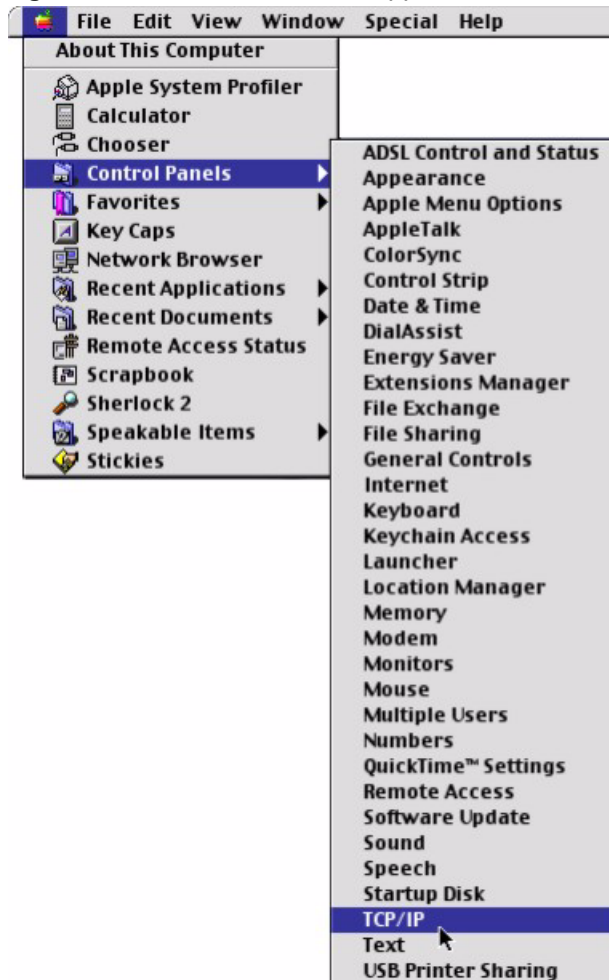
## Verifying Settings

- 1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

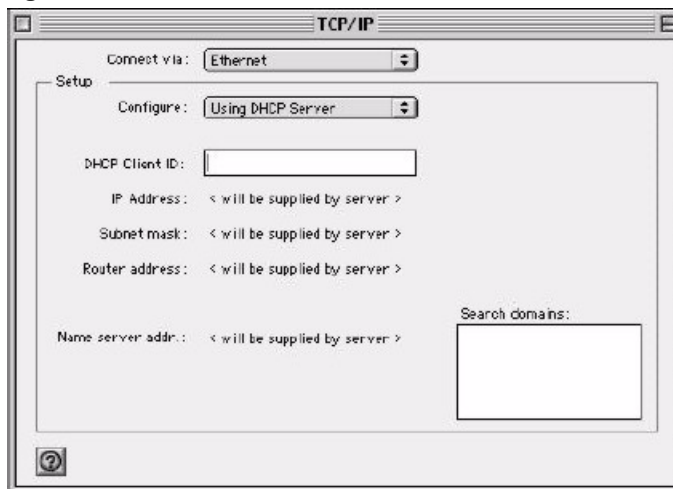
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 61 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 62 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your gateway in the **Router address** box if you have one.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Restart your computer (if prompted).

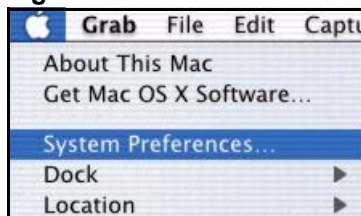
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

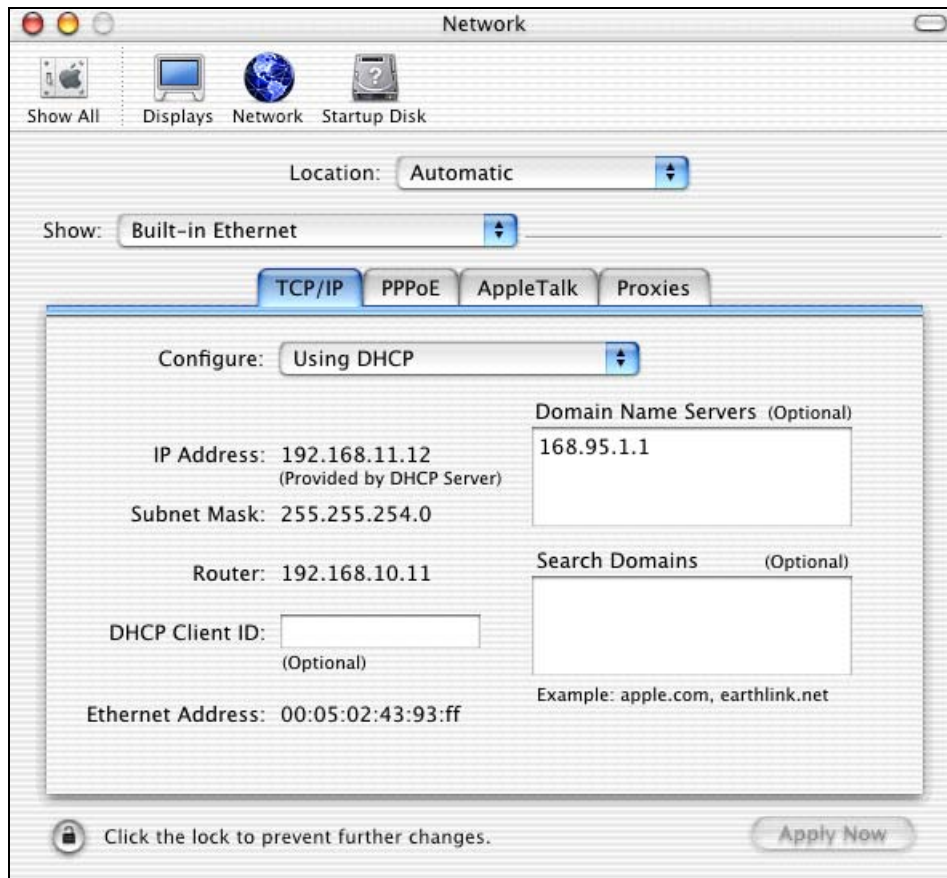
## Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 63** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 64** Macintosh OS X: Network

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box if you have one.

**5** Click **Apply Now** and close the window.

**6** Restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.



# Index

## A

About [57](#)  
About your G-120 [21](#)  
access point [31](#)  
access point. See also AP.  
activating a profile [54](#)  
Adapter [54](#)  
Ad-Hoc [22](#), [51](#)  
Advanced Encryption Standard [34](#), [79](#)  
advanced settings [54](#)  
antenna power output [63](#)  
AP [31](#)  
AP. See also access point.  
authentication method  
    auto [33](#)  
    open system [33](#)  
    shared key [33](#)  
auto authentication [33](#)

## C

CA [78](#)  
Certificate Authority [78](#)  
Certifications  
    viewing [5](#)  
certifications  
    Notices [5](#)  
channel [40](#), [42](#), [51](#), [63](#)  
configuration method [23](#)  
    Wireless Zero Configuration (WZC) [23](#)  
Copyright [3](#)  
creating a new profile [50](#)  
current configuration [39](#)  
current connection status [39](#)  
Customer Support [8](#)

## D

data encryption [42](#)  
Disclaimer [3](#)

driver version [57](#)  
Dynamic WEP Key Exchange [78](#)

## E

EAP Authentication [34](#)  
Enabling OTIST [34](#)  
Encryption [79](#)  
Encryption Type [33](#)

## F

FCC [4](#)

## G

getting started [21](#)  
graphics icons key [20](#)

## H

hardware connections [23](#)

## I

IEEE 802.1x [33](#), [46](#)  
Infrastructure [21](#)  
initialization vector (IV) [80](#)  
Interference Statement [4](#)

## L

link information [39](#)

## M

Message Integrity Check (MIC) [34, 79](#)

## N

network type [40](#)

## O

One-Touch Intelligent Security Technology [34](#)

open system authentication [33](#)

OTIST Introduction [34](#)

## P

PA2-PSK [44](#)

Pairwise Master Key (PMK) [80](#)

passphrase [32, 43](#)

password phrase [22](#)

Power Saving Mode [55](#)

product specifications [63](#)

profile [39, 49](#)

    activation [54](#)

    add new [49, 50](#)

    delete [49](#)

    edit [49](#)

    information [49](#)

## Q

Quick Start Guide [19, 23](#)

## R

radio interference [61](#)

real-time data traffic statistics [40](#)

Related Documentation [19](#)

## S

safety warnings [6](#)

save power [55](#)

Scan Info [51](#)

security [32, 64](#)

    data encryption [32](#)

Security Parameters [82](#)

Setup Key [35](#)

shared key authentication [33](#)

signal strength [42](#)

site survey [41](#)

    scan [42](#)

    security settings [43](#)

sleep mode [55](#)

SSID [39, 42](#)

Starting OTIST [36](#)

statistics [40](#)

support CD [19](#)

syntax conventions [19](#)

## T

Temporal Key Integrity Protocol (TKIP) [34, 79](#)

Trademarks [3](#)

transmission rate [40, 50, 63](#)

transmit key [43](#)

Trend Chart [40](#)

troubleshooting [61](#)

    link status [61](#)

    network communication [62](#)

    starting ZyXEL Utility [61](#)

## U

uninstalling ZyXEL Utility [57](#)

upgrading ZyXEL Utility [58](#)

    important step [58](#)

User Authentication [80](#)

user authentication [32](#)

## V

voltage [63](#)



## W

- WEP [32, 43](#)
  - manual setup [33, 44](#)
  - passphrase [32, 43](#)
- WEP (Wired Equivalent Privacy) [32](#)
- WEP Encryption [43](#)
- Wi-Fi Protected Access [34, 79](#)
- Windows XP [23](#)
- wireless client [31](#)
- wireless LAN
  - introduction [31](#)
  - security [32](#)
- Wireless LAN (WLAN) [31](#)
- wireless network [31](#)
- wireless standard [40, 63](#)
- WLAN
  - Security parameters [82](#)
- WPA [34, 45, 79](#)
- WPA2 [34, 45, 79](#)
- WPA2-Pre-Shared Key [34, 79](#)
- WPA2-PSK [34, 79](#)
- WPA-PSK [34, 44, 79](#)
- WZC (Wireless Zero Configuration) [23](#)

## Z

- ZyXEL Limited Warranty
  - Note [7](#)
- ZyXEL Utility [23](#)
  - accessing [24](#)
  - help [24](#)
  - opening [24](#)
  - system tray icon [23](#)
  - upgrade [58](#)
  - version [57](#)