

# *ZyXEL G-570U*

*IEEE 802.11a/b/g Wireless Access Point / Bridge*

## *User's Guide*

Version 1.00

Edition 1

07/2006

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 residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation.

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 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. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- 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。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

## Notices

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

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

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

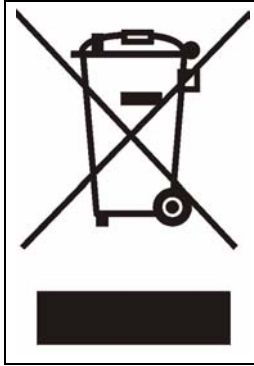
- 1 Go to <http://www.zyxel.com>.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

# 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.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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 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.

## 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 www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso 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 Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská 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 Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 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 Niils Hansens vei 13 0667 Oslo Norway
		sales@zyxel.no	+47-22-80-61-81		
POLAND		info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
			+48 (22) 333 8251		
RUSSIA		http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
		sales@zyxel.ru	+7-095-542-89-25		
SPAIN		support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
		sales@zyxel.es	+34-913-005-345		
SWEDEN		support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
		sales@zyxel.se	+46-31-744-7701		
UKRAINE		support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
		sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM		support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, 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>8</b>
<b>Customer Support</b> .....	<b>9</b>
<b>Table of Contents</b> .....	<b>11</b>
<b>List of Figures</b> .....	<b>15</b>
<b>List of Tables</b> .....	<b>19</b>
<b>Preface</b> .....	<b>21</b>
<b>Chapter 1</b>	
<b>Getting to Know Your G-570U</b> .....	<b>23</b>
1.1 Introducing the G-570U Wireless Access Point .....	23
1.2 G-570U Features .....	23
1.3 Applications for the G-570U .....	26
1.3.1 Access Point for Internet Access .....	26
1.3.2 Corporate Network Access Application .....	26
1.3.3 Wireless Client Application .....	27
1.3.4 Bridge / Repeater .....	27
1.3.5 Access Point and Repeater .....	28
1.4 The LED Display .....	29
1.5 The Rear Panel .....	30
<b>Chapter 2</b>	
<b>Management Computer Setup</b> .....	<b>31</b>
2.1 Introduction .....	31
2.2 Wired Connection .....	31
2.2.1 Setting Up Your Computer's IP Address .....	31
2.2.1.1 Windows 2000/NT/XP .....	32
2.3 Wireless Connection .....	34
2.4 Restarting the G-570U .....	35
2.5 Resetting the G-570U .....	35
2.5.1 Methods of Restoring Factory-Defaults .....	35

<b>Chapter 3</b>	
<b>Introducing the Web Configurator .....</b>	<b>37</b>
3.1 Web Configurator Overview .....	37
3.2 Accessing the G-570U Web Configurator .....	37
3.3 Configuring the G-570U Using the Wizard .....	39
3.3.1 Wizard: Basic Settings .....	39
3.3.2 Wizard: Wireless Settings .....	40
3.3.3 Wizard: Security Settings .....	41
3.3.3.1 Disable .....	41
3.3.3.2 WEP .....	42
3.3.3.3 WPA(2)-PSK .....	43
3.3.4 Wizard: Confirm Your Settings .....	44
3.4 Navigating the Advanced Screens .....	45
3.4.1 Navigation Panel .....	46
<b>Chapter 4</b>	
<b>Status Screens .....</b>	<b>49</b>
4.1 System Status .....	49
4.1.1 Statistics .....	50
4.1.2 Association List .....	52
<b>Chapter 5</b>	
<b>System Screen .....</b>	<b>53</b>
5.1 TCP/IP Parameters .....	53
5.1.1 IP Address Assignment .....	53
5.1.2 IP Address and Subnet Mask .....	53
5.2 System Settings .....	54
<b>Chapter 6</b>	
<b>Wireless Screens .....</b>	<b>57</b>
6.1 Wireless LAN Overview .....	57
6.1.1 IBSS .....	57
6.1.2 BSS .....	57
6.1.3 ESS .....	58
6.2 Wireless LAN Basics .....	59
6.2.1 Channel .....	59
6.2.2 SSID .....	59
6.2.3 RTS/CTS .....	60
6.2.4 Fragmentation Threshold .....	61
6.3 Configuring Wireless .....	61
6.3.1 Access Point Mode .....	61
6.3.2 Wireless Client Mode .....	63
6.3.3 Bridge Mode .....	65

6.3.4 AP+Repeater Mode .....	68
6.4 Wireless Security Overview .....	71
6.4.1 Encryption .....	71
6.4.2 Authentication .....	71
6.4.3 Restricted Access .....	72
6.4.4 Hide G-570U Identity .....	72
6.5 WEP Overview .....	72
6.5.1 Data Encryption .....	72
6.5.2 Authentication .....	72
6.6 802.1x Overview .....	73
6.7 Introduction to RADIUS .....	74
6.7.1 Types of RADIUS Messages .....	74
6.8 EAP Authentication Overview .....	75
6.9 Dynamic WEP Key Exchange .....	75
6.10 Introduction to WPA and WPA2 .....	76
6.10.1 Encryption .....	76
6.10.2 User Authentication .....	77
6.11 WPA(2)-PSK Application Example .....	77
6.12 WPA(2) with RADIUS Application Example .....	77
6.13 Security Parameters Summary .....	78
6.14 Configuring Wireless Security .....	79
6.14.1 Wireless Security: Disable .....	79
6.14.2 Wireless Security: WEP .....	79
6.14.3 Wireless Security: WPA(2)-PSK .....	80
6.14.4 Wireless Security: WPA(2) .....	81
6.14.5 Wireless Security: 802.1x .....	83
6.15 MAC Filter .....	85
6.16 OTIST .....	87
6.16.1 Enabling OTIST: G-570U in AP Mode .....	87
6.16.1.1 AP .....	87
6.16.1.2 Wireless Client .....	88
6.16.1.3 G-570U in Wireless Client Mode .....	88
6.16.2 Starting OTIST .....	89
6.16.3 Notes on OTIST .....	90
<b>Chapter 7</b>	
<b>Management Screens .....</b>	<b>93</b>
7.1 Maintenance Overview .....	93
7.2 Password .....	93
7.3 Logs .....	94
7.4 Configuration File .....	95
7.4.1 Backup Configuration .....	95
7.4.2 Restore Configuration .....	96

7.4.3 Back to Factory Defaults .....	97
7.5 F/W Upload Screen .....	97
<b>Chapter 8</b>	
<b>Troubleshooting .....</b>	<b>99</b>
8.1 Problems Starting Up the G-570U .....	99
8.2 Problems with the Password .....	99
8.3 Problems with the WLAN Interface .....	100
8.4 Problems with the Ethernet Interface .....	100
8.4.1 Pop-up Windows, JavaScripts and Java Permissions .....	101
8.4.1.1 Internet Explorer Pop-up Blockers .....	101
8.4.1.2 JavaScripts .....	104
8.4.1.3 Java Permissions .....	106
8.5 Testing the Connection to the G-570U .....	108
<b>Appendix A</b>	
<b>Product Specifications .....</b>	<b>109</b>
<b>Appendix B</b>	
<b>Setting up Your Computer's IP Address.....</b>	<b>115</b>
<b>Appendix C</b>	
<b>Wireless LANs .....</b>	<b>131</b>
<b>Appendix D</b>	
<b>IP Subnetting .....</b>	<b>145</b>
<b>Appendix E</b>	
<b>Open Software Announcements.....</b>	<b>153</b>
<b>Index.....</b>	<b>159</b>

# List of Figures

Figure 1 WDS Functionality Example .....	24
Figure 2 Internet Access Application .....	26
Figure 3 Corporate Network Application .....	27
Figure 4 Wireless Client Application .....	27
Figure 5 Bridge Application .....	28
Figure 6 Bridge Repeater Application .....	28
Figure 7 AP+Repeater Application .....	29
Figure 8 Front Panel .....	29
Figure 9 G-570U: Rear Panel .....	30
Figure 10 Wired Connection .....	31
Figure 11 Control Panel .....	32
Figure 12 Network Connection .....	32
Figure 13 Local Area Connection Properties .....	33
Figure 14 Internet Protocol Properties .....	33
Figure 15 Advanced TCP/IP Settings .....	34
Figure 16 Wireless Connection .....	34
Figure 17 Web Configurator Address .....	38
Figure 18 Login Screen .....	38
Figure 19 Language Screen .....	38
Figure 20 Select Wizard or Advanced Setup Screen .....	39
Figure 21 Wizard: Basic Settings .....	40
Figure 22 Wizard: Wireless Settings .....	41
Figure 23 Setup Wizard 3: Disable .....	42
Figure 24 Wizard 3: WEP .....	43
Figure 25 Wizard 3: WPA(2)-PSK .....	44
Figure 26 Wizard: Confirm Your Settings .....	45
Figure 27 Status Screen .....	46
Figure 28 Status .....	49
Figure 29 Status: View Statistics .....	51
Figure 30 Status: View Association List .....	52
Figure 31 System Settings .....	54
Figure 32 IBSS (Ad-hoc) Wireless LAN .....	57
Figure 33 Basic Service set .....	58
Figure 34 Extended Service Set .....	59
Figure 35 RTS/CTS .....	60
Figure 36 Wireless Settings: Access Point .....	61
Figure 37 Wireless Settings: Wireless Client .....	64
Figure 38 Bridging Example .....	65

Figure 39 Bridge Loop: Two Bridges Connected to Hub .....	66
Figure 40 Bridge Loop: Bridge Connected to Wired LAN .....	66
Figure 41 Wireless Settings: Bridge .....	67
Figure 42 Wireless Settings: AP+Repeater .....	69
Figure 43 WEP Authentication Steps .....	73
Figure 44 EAP Authentication .....	75
Figure 45 WPA(2)-PSK Authentication .....	77
Figure 46 WPA with RADIUS Application Example .....	78
Figure 47 Wireless Security: Disable .....	79
Figure 48 Wireless Security: WEP .....	80
Figure 49 Wireless Security: WPA(2)-PSK .....	81
Figure 50 Wireless Security: WPA(2) .....	82
Figure 51 Wireless Security: 802.1x .....	83
Figure 52 MAC Filter .....	86
Figure 53 AP Mode: OTIST .....	87
Figure 54 Example Wireless Client OTIST Screen .....	88
Figure 55 G-570U in Wireless Client Mode: OTIST Screen .....	89
Figure 56 Security Key .....	89
Figure 57 OTIST in Progress (AP) .....	90
Figure 58 OTIST in Progress (Client) .....	90
Figure 59 No AP with OTIST Found .....	90
Figure 60 Start OTIST? .....	91
Figure 61 Management: Password .....	93
Figure 62 Management: Logs .....	94
Figure 63 Management: Configuration File .....	95
Figure 64 Configuration Upload Successful .....	96
Figure 65 Network Temporarily Disconnected .....	96
Figure 66 Configuration Upload Error .....	97
Figure 67 Reset Warning Message .....	97
Figure 68 Management: F/W Upload .....	97
Figure 69 Firmware Upgrading Screen .....	98
Figure 70 Network Temporarily Disconnected .....	98
Figure 71 Firmware Upload Error .....	98
Figure 72 Pop-up Blocker .....	102
Figure 73 Internet Options .....	102
Figure 74 Internet Options .....	103
Figure 75 Pop-up Blocker Settings .....	104
Figure 76 Internet Options .....	105
Figure 77 Security Settings - Java Scripting .....	106
Figure 78 Security Settings - Java .....	107
Figure 79 Java (Sun) .....	108
Figure 80 Pinging the G-570U .....	108
Figure 81 WIndows 95/98/Me: Network: Configuration .....	116



Figure 82 Windows 95/98/Me: TCP/IP Properties: IP Address .....	117
Figure 83 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	118
Figure 84 Windows XP: Start Menu .....	119
Figure 85 Windows XP: Control Panel .....	119
Figure 86 Windows XP: Control Panel: Network Connections: Properties .....	120
Figure 87 Windows XP: Local Area Connection Properties .....	120
Figure 88 Windows XP: Internet Protocol (TCP/IP) Properties .....	121
Figure 89 Windows XP: Advanced TCP/IP Properties .....	122
Figure 90 Windows XP: Internet Protocol (TCP/IP) Properties .....	123
Figure 91 Macintosh OS 8/9: Apple Menu .....	124
Figure 92 Macintosh OS 8/9: TCP/IP .....	124
Figure 93 Macintosh OS X: Apple Menu .....	125
Figure 94 Macintosh OS X: Network .....	126
Figure 95 Red Hat 9.0: KDE: Network Configuration: Devices .....	127
Figure 96 Red Hat 9.0: KDE: Ethernet Device: General .....	127
Figure 97 Red Hat 9.0: KDE: Network Configuration: DNS .....	128
Figure 98 Red Hat 9.0: KDE: Network Configuration: Activate .....	128
Figure 99 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	129
Figure 100 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	129
Figure 101 Red Hat 9.0: DNS Settings in resolv.conf .....	129
Figure 102 Red Hat 9.0: Restart Ethernet Card .....	130
Figure 103 Red Hat 9.0: Checking TCP/IP Properties .....	130
Figure 104 Peer-to-Peer Communication in an Ad-hoc Network .....	131
Figure 105 Basic Service Set .....	132
Figure 106 Infrastructure WLAN .....	133
Figure 107 RTS/CTS .....	134
Figure 108 EAP Authentication .....	137
Figure 109 WEP Authentication Steps .....	139
Figure 110 Roaming Example .....	142



# List of Tables

Table 1 Front Panel LED Description .....	29
Table 2 G-570U: Rear Panel .....	30
Table 3 Factory Defaults .....	35
Table 4 Global Icon Key .....	46
Table 5 Screens Summary .....	47
Table 6 Status .....	49
Table 7 Status: View Statistics .....	51
Table 8 Status: View Association List .....	52
Table 9 Private IP Address Ranges .....	53
Table 10 System Settings .....	54
Table 11 Wireless Settings: Access Point .....	62
Table 12 Wireless Settings: Wireless Client .....	64
Table 13 Wireless Settings: Bridge .....	67
Table 14 Wireless Settings: AP + Repeater .....	69
Table 15 Wireless Security Levels .....	71
Table 16 Wireless Security Relational Matrix .....	78
Table 17 Wireless Security: Disable .....	79
Table 18 Wireless Security: WEP .....	80
Table 19 Wireless Security: WPA-PSK .....	81
Table 20 Wireless Security: WPA(2) .....	82
Table 21 Wireless Security: 802.1x .....	84
Table 22 MAC Filter .....	86
Table 23 OTIST .....	88
Table 24 Management: Password .....	93
Table 25 Management: Logs .....	94
Table 26 Management: Configuration File: Restore Configuration .....	96
Table 27 Management: F/W Upload .....	98
Table 28 Troubleshooting the Start-Up of Your G-570U .....	99
Table 29 Troubleshooting the Password .....	99
Table 30 Troubleshooting the WLAN Interface .....	100
Table 31 Troubleshooting the Ethernet Interface .....	100
Table 32 Device Specifications .....	109
Table 33 Feature Specifications .....	109
Table 34 Wireless RF Specifications .....	110
Table 35 Approvals .....	111
Table 36 Power Adapter Specifications .....	112
Table 37 IEEE 802.11g .....	135
Table 38 Comparison of EAP Authentication Types .....	140

Table 39 Classes of IP Addresses .....	146
Table 40 Allowed IP Address Range By Class .....	146
Table 41 "Natural" Masks .....	147
Table 42 Alternative Subnet Mask Notation .....	147
Table 43 Two Subnets Example .....	148
Table 44 Subnet 1 .....	148
Table 45 Subnet 2 .....	149
Table 46 Subnet 1 .....	149
Table 47 Subnet 2 .....	150
Table 48 Subnet 3 .....	150
Table 49 Subnet 4 .....	150
Table 50 Eight Subnets .....	151
Table 51 Class C Subnet Planning .....	151
Table 52 Class B Subnet Planning .....	152

# Preface

Congratulations on your purchase of the ZyXEL G-570U IEEE 802.11a/b/g Wireless Access Point / Bridge.

**Note:** 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.

An access point (AP) acts as a bridge between the wireless and wired networks, extending your existing wired network without any additional wiring.

This User's Guide is designed to guide you through the configuration of your ZyXEL G-570U using the web configurator.

## 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 connection and installation information.
- ZyXEL Web Site  
Please go to <http://www.zyxel.com> for product news, firmware, updated documents, and other support materials.










## 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 choices.
- Mouse action sequences are denoted using a right arrow bracket key (>). For example, “In Windows, click **Start** > **Settings** > **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-570U 802.11g Wireless Access Point may be referred to simply as the G-570U in the User's Guide.

## Graphics Icons Key

G-570U 	Computer 	Notebook computer 
Server 	Modem 	Wireless Signal 
Telephone 	Switch 	Router 

# CHAPTER 1

## Getting to Know Your G-570U

This chapter introduces the main features and applications of the G-570U.

### 1.1 Introducing the G-570U Wireless Access Point

The ZyXEL G-570U is a 4-in-1 wireless Access Point.

Access Point (AP), repeater, bridge and wireless client functions allow you to use the G-570U in various network deployments.

The G-570U Access Point (AP) allows wireless stations to communicate and/or access a wired network. It can work as a bridge and repeater to extend your wireless network. You can also use it as a wireless client to access a wired network through another AP. The G-570U uses IEEE 802.1x, WEP data encryption, WPA (Wi-Fi Protected Access), WPA2 and MAC address filtering to give mobile users highly secured wireless connectivity. IEEE 802.11a, IEEE 802.11b and IEEE 802.11g compliant wireless devices can associate with the G-570U.

In addition to being highly flexible, the G-570U is easy to install and configure.

### 1.2 G-570U Features

The following sections describe the features of the G-570U.

#### Bridge/Repeater

The G-570U can act as a bridge, establishing wireless links with other APs or as a repeater, establishing wireless links to APs.

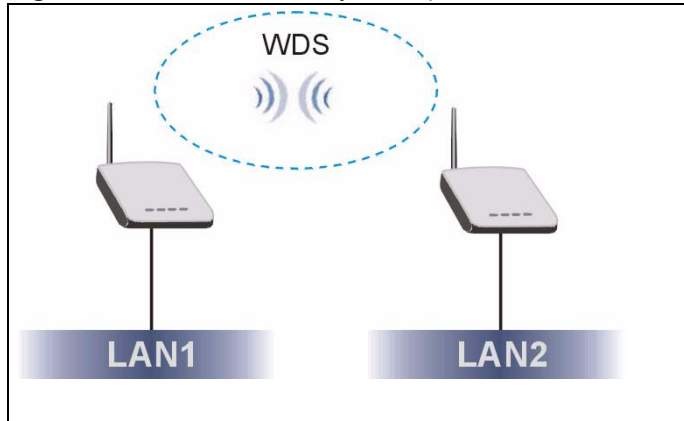
#### WDS Functionality

A Distribution System (DS) is a wired connection between two or more APs, while a Wireless Distribution System (WDS) is a wireless connection. Your G-570U supports WDS connections to other G-570U APs.<sup>1</sup> This provides a cost-effective solution for wireless network expansion.

---

1. The G-570U only supports WDS connections to G-570U APs, not other devices.

**Figure 1** WDS Functionality Example



### **OTIST (One-Touch Intelligent Security Technology)**

OTIST allows your G-570U to assign its SSID and security settings (WEP or WPA-PSK) to the ZyXEL wireless adapters that support OTIST and are within transmission range. The ZyXEL wireless adapters must also have OTIST enabled. The G-570U also supports OTIST in Wireless Client mode.

### **10/100M Auto-negotiating Ethernet/Fast Ethernet Interface**

This auto-negotiating feature allows the G-570U to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.

### **10/100M Auto-crossover Ethernet/Fast Ethernet Interface**

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable.

### **Reset Button**

The G-570U reset button is built into the rear panel. Use this button to restart the device or restore the factory default password.

### **802.11g Wireless LAN Standard**

The ZyXEL wireless products containing the letter "G" in the model name, such as G-570U and G-162, comply with the IEEE 802.11g wireless standard.



IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range.

## **Wi-Fi Protected Access**

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

## **WPA2**

WPA 2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

## **SSL Passthrough**

The G-570U allows SSL connections to go through the G-570U. SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https" instead of "http".

## **Wireless LAN MAC Address Filtering**

Your G-570U checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

## **WEP Encryption**

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

## **IEEE 802.1x Network Security**

The G-570U supports the IEEE 802.1x standard to enhance user authentication. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate a limitless number of users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication.

## **Full Network Management**

The embedded web configurator is an all-platform web-based utility that allows you to easily access the G-570U's management settings.

## **Logging and Tracing**

Built-in message logging and packet tracing.

## Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the G-570U to access your wired network. When the G-570U is in client mode, the wireless association list displays details of the access point to which the G-570U is connected.

## Limit the Number of Client Connections

You may set a maximum number of wireless stations that may connect to the G-570U. This may be necessary if for example, there is interference or difficulty with channel assignment due to a high density of APs within a coverage area.

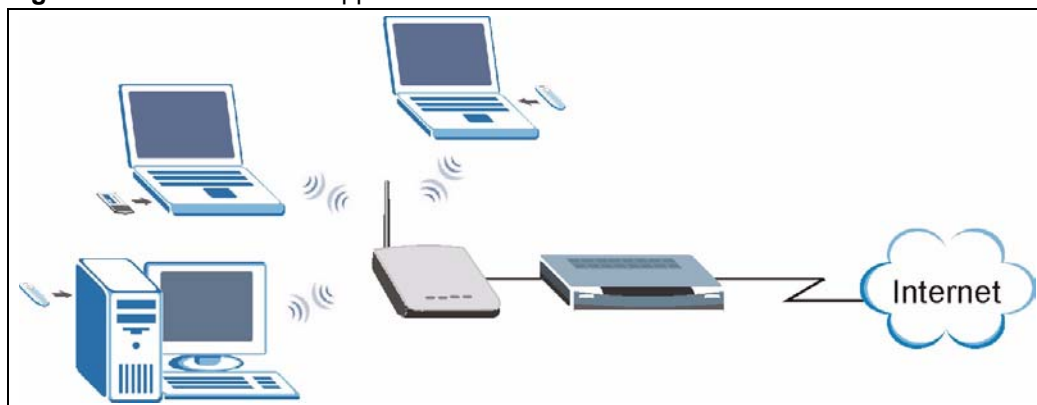
## 1.3 Applications for the G-570U

Here are some application examples of how you can use your G-570U.

### 1.3.1 Access Point for Internet Access

The G-570U is an ideal access solution for wireless Internet connection. A typical Internet access application for your G-570U is shown as follows.

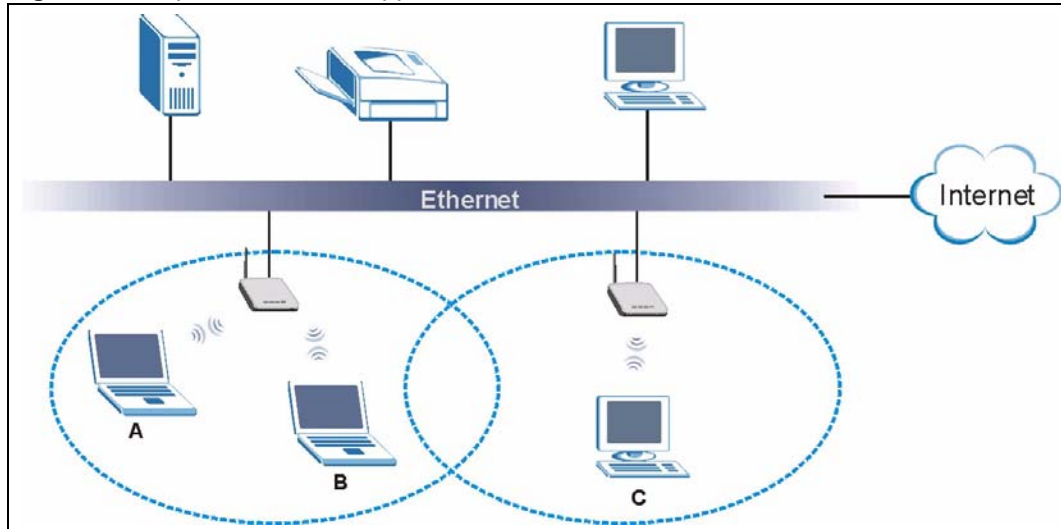
**Figure 2** Internet Access Application



### 1.3.2 Corporate Network Access Application

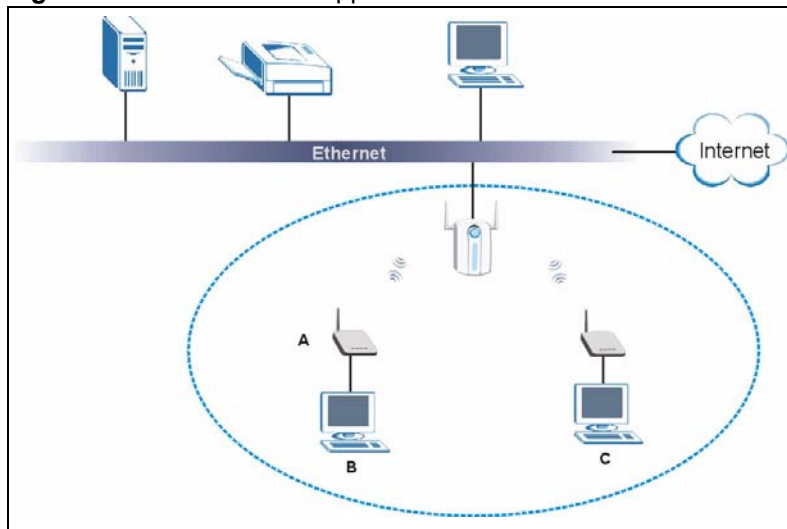
In situations where users need to access corporate network resources and the Internet, the G-570U is an ideal solution for wireless stations to connect to the corporate network without expensive network cabling. Stations A, B and C can access the wired network through the G-570Us.

The following figure depicts a typical application of the G-570U in an enterprise environment. The three computers with wireless adapters are allowed to access the network resource through the G-570U after account validation by the network authentication server.

**Figure 3** Corporate Network Application

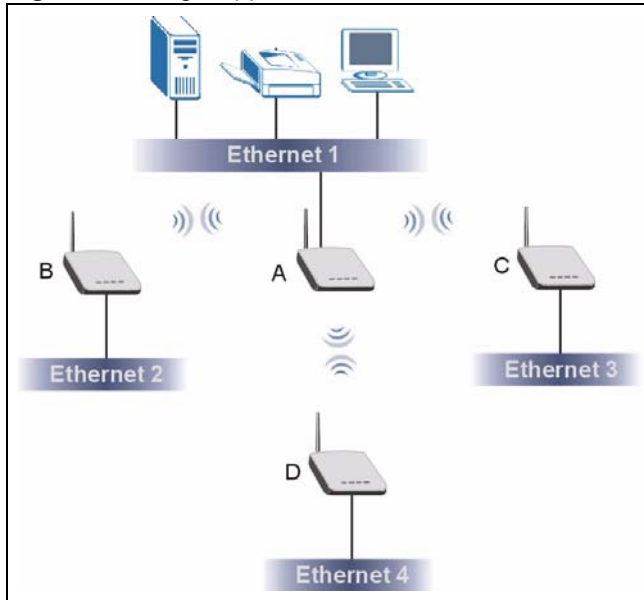
### 1.3.3 Wireless Client Application

The G-570U can function as a wireless client to connect to a network via an Access Point (AP). The AP provides access to the wired network and the Internet.

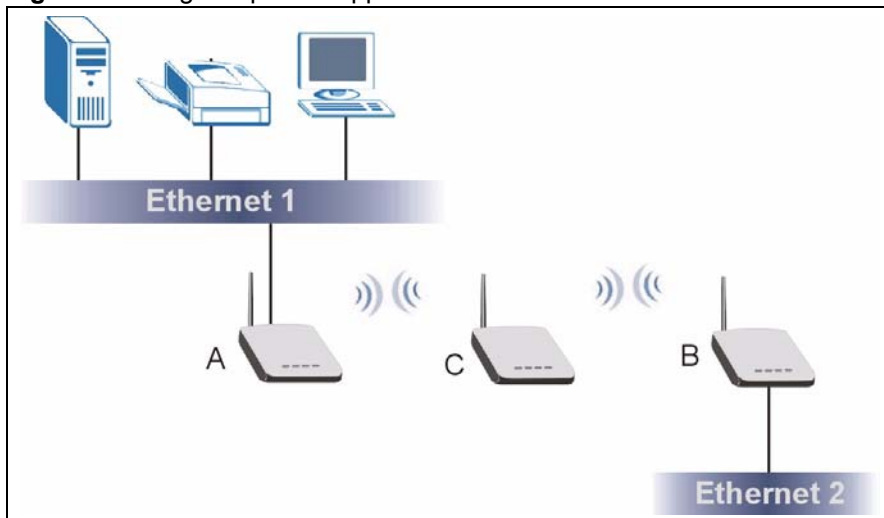
**Figure 4** Wireless Client Application

### 1.3.4 Bridge / Repeater

The G-570U can act as a wireless network bridge and establish wireless links with other APs. The G-570Us in the following example are using bridge mode with a star configuration. A, B, C and D are connected to independent wired networks and have bridge connections at the same time (B, C and D can communicate with A).

**Figure 5** Bridge Application

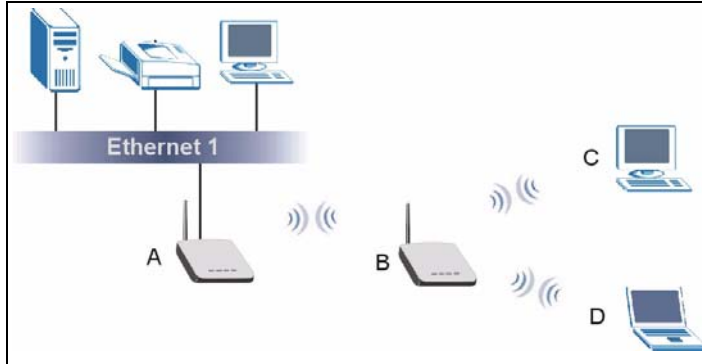
A G-570U in bridge mode without an Ethernet connection can function as a repeater. It transmits traffic from one AP to another AP without using a wired connection. C in the following graphic repeats wireless traffic between A and B.

**Figure 6** Bridge Repeater Application

### 1.3.5 Access Point and Repeater

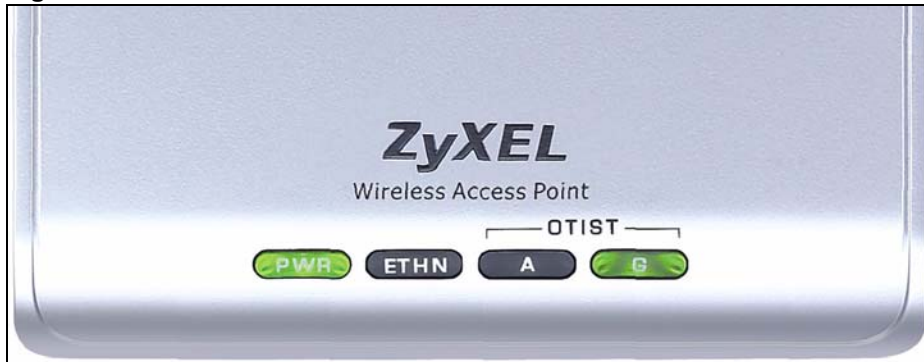
Set the G-570U to **AP+Repeater** mode to have it simultaneously provide access for wireless clients and use the repeater function. This allows you to extend the coverage of your wireless network without installing Ethernet cable to connect the G-570U. In the following figure, B is in **AP+Repeater** mode. B functions as an AP for wireless clients C and D. B also repeats traffic between the wireless clients and AP A which is connected to the wired network. You could also set AP A to **AP+Repeater** mode so that wireless clients could connect to A as well.

**Figure 7** AP+Repeater Application



## 1.4 The LED Display

**Figure 8** Front Panel



The following table describes the LEDs on the G-570U.

**Table 1** Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
PWR/ SYS	Green	Blinking	The G-570U is not ready or rebooting.
		On	The G-570U has a successful reboot and is receiving power.
		Off	The G-570U is not receiving power.
ETHN	Green	Blinking	The G-570U is sending/receiving data.
		On	The G-570U has a successful 10Mbps Ethernet connection.
		Off	The G-570U does not have an Ethernet connection.
	Amber	Blinking	The G-570U is sending/receiving data.
		On	The G-570U has a successful 100Mbps Ethernet connection.
A	Green	On	The G-570U has an active IEEE 802.11a wireless connection, but is not transmitting or receiving data.
		Off	The G-570U does not have an active IEEE 802.11a wireless connection.
		Blinking	The G-570U has an active IEEE 802.11a wireless connection and is transmitting or receiving data.

**Table 1** Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
G	Green	On	The G-570U has an active IEEE 802.11b/g wireless connection, but is not transmitting or receiving data.
		Off	The G-570U does not have an active IEEE 802.11b/g wireless connection.
		Blinking	The G-570U has an active IEEE 802.11b/g wireless connection and is transmitting or receiving data.
A and G	Green	Both LEDs blinking in series	OTIST (One-Touch Intelligent Security Technology) is in progress.
		Both LEDs blinking simultaneously	OTIST (One-Touch Intelligent Security Technology) is complete and the G-570U is attempting to connect to an access point.

## 1.5 The Rear Panel

**Figure 9** G-570U: Rear Panel

The following table describes the rear panel of the G-570U.

**Table 2** G-570U: Rear Panel

LABEL	DESCRIPTION	
A	POWER port	
B	RESET button	Hold this button in for 1-2 seconds to restart the G-570U. Your settings will be saved. Hold this button in for 10 seconds or more to reset the device. All settings will be returned to factory defaults.
C	OTIST button	When the G-570U is in AP mode, click this button once to activate OTIST. In any mode, double-click this button to enter Wireless Client mode and activate OTIST.
D	ETHERNET port	
E	Detachable 2dBi antenna	

# CHAPTER 2

## Management Computer Setup

This chapter describes how to prepare your computer to access the G-570U web configurator.

### 2.1 Introduction

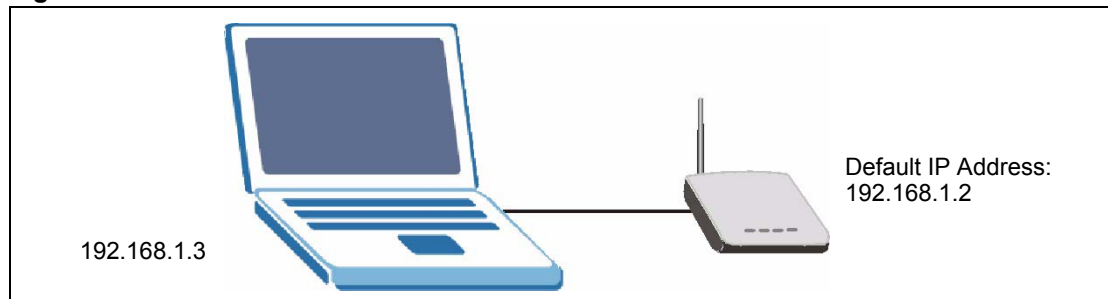
You can connect a computer to the G-570U for management purposes either using an Ethernet connection (recommended for a first time management session) or wirelessly.

### 2.2 Wired Connection

You must prepare your computer/computer network to connect to the G-570U if you are using a wired connection. Your computer's IP address and subnet mask must be on the same subnet as the G-570U. This can be done by setting up your computer's IP address.

The following figure shows you an example of accessing your G-570U via a wired connection with an Ethernet cable.

**Figure 10** Wired Connection



#### 2.2.1 Setting Up Your Computer's IP Address

**Note:** Skip this section if your computer's IP address is already between 192.168.1.3 and 192.168.1.254 with subnet mask 255.255.255.0.

Your computer must have a network card and TCP/IP installed. TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems. Refer to the appendix about setting up your computer's IP address for other operating systems.

### 2.2.1.1 Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

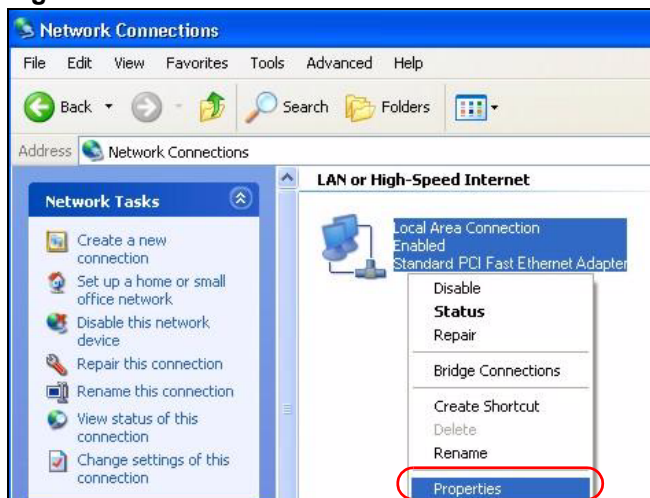
- 1 Click **start (Start in Windows 2000/NT) > Settings > Control Panel**.
- 2 In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections in Windows 2000/NT)**.

**Figure 11** Control Panel



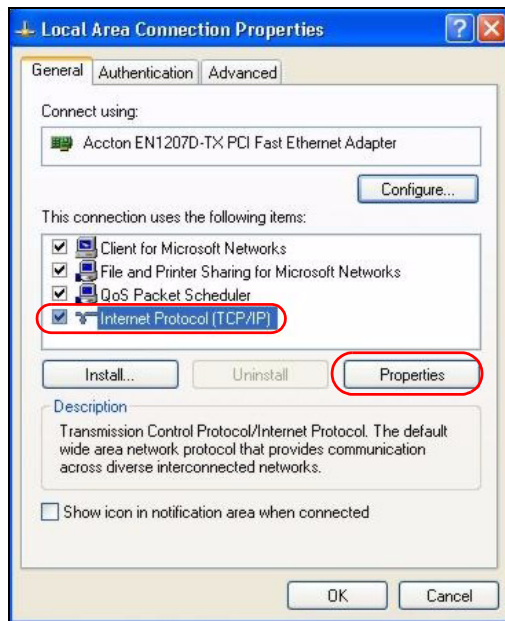
- 3 Right-click **Local Area Connection** and then **Properties**.

**Figure 12** Network Connection

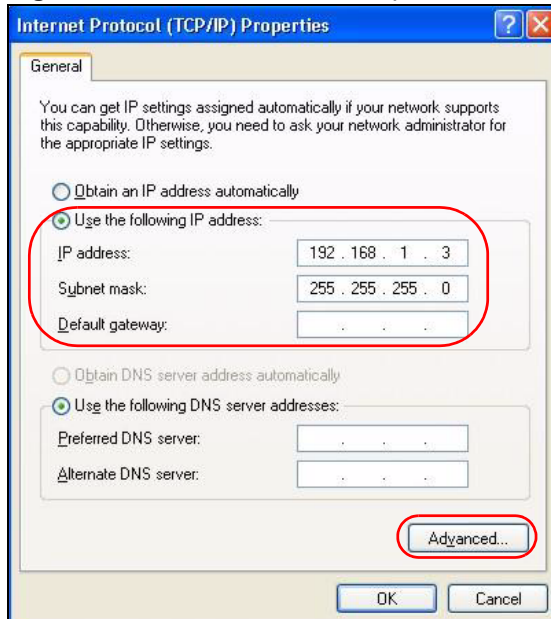


- 4 Select **Internet Protocol (TCP/IP)** and then click **Properties**.



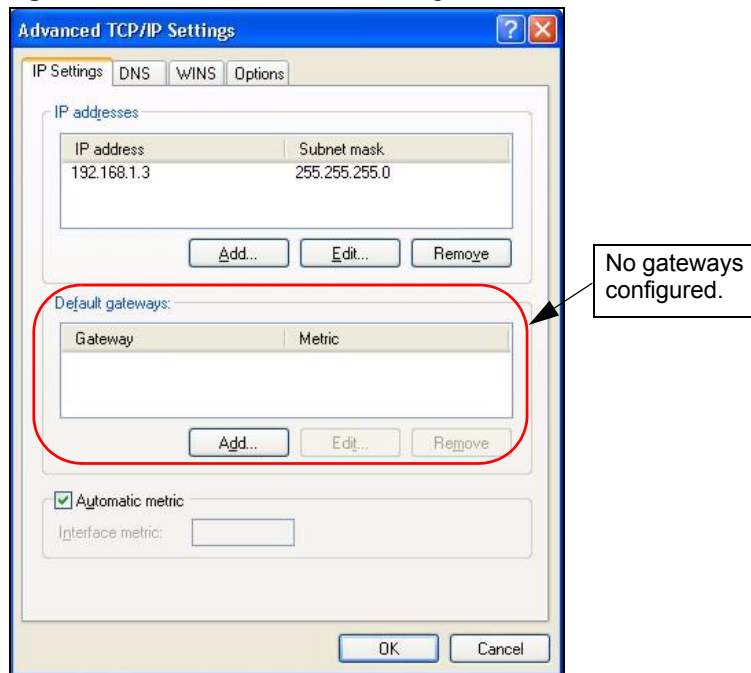
**Figure 13** Local Area Connection Properties

- 5** Select **Use the following IP Address** and fill in an **IP address** (between 192.168.1.3 and 192.168.1.254).
- Type 255.255.255.0 as the **Subnet mask**.
  - Click **Advanced**<sup>1</sup>.

**Figure 14** Internet Protocol Properties

- 6** Remove any previously installed gateways in the **IP Settings** tab and click **OK** to go back to the **Internet Protocol TCP/IP Properties** screen.

1. See the appendices for information on configuring DNS server addresses.

**Figure 15** Advanced TCP/IP Settings

- 7** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 9** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

## 2.3 Wireless Connection

Ensure that the wireless stations have a compatible wireless card/adaptor with the same wireless settings as the G-570U. The following figure shows how you can access your G-570U wirelessly.

**Figure 16** Wireless Connection

**Note:** The wireless stations and G-570U must use the same SSID, channel and wireless security settings for wireless communication.

If you do not enable any wireless security on your G-570U, your network traffic is visible to any wireless networking device that is within range.

## 2.4 Restarting the G-570U

Press and immediately release the **RESET** button to restart the G-570U.

**Note:** Holding the RESET button in for ten seconds or longer resets the device to the factory-default settings.

## 2.5 Resetting the G-570U

If you forget the G-570U's IP address or your password, to access the G-570U you will need to reload the factory-default using the **RESET** button. Resetting the G-570U replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The following parameters will be reset to the default values.

**Table 3** Factory Defaults

PARAMETER	DEFAULT VALUE
IP Address	192.168.1.2
Password	1234
Wireless Security	Disabled
SSID	ZyXEL G-570U

### 2.5.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in two ways:

- 1** Use the **RESET** button on the G-570U to upload the default configuration file (hold this button in for at least ten seconds).
- 2** Use the web configurator to restore defaults. Click **Management > Configuration File**. From here you can restore the G-570U to factory defaults.



# CHAPTER 3

## Introducing the Web Configurator

This chapter describes how to configure the G-570U using the Wizard.

### 3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy G-570U setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

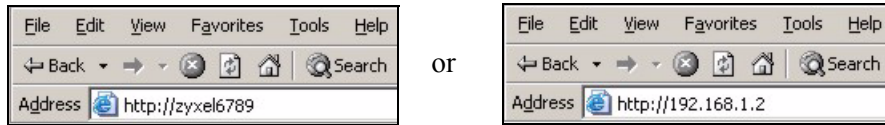
See the **Troubleshooting** chapter if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

### 3.2 Accessing the G-570U Web Configurator

Follow the steps below to access the web configurator, select a language, change your login password and choose a configuration method from the status screen.

- 1** Make sure your G-570U hardware is properly connected (refer to the Quick Start Guide).
- 2** Prepare your computer/computer network to connect to the G-570U (refer to [Section 2.2.1 on page 31](#) for instructions on how to do this).
- 3** Launch your web browser.
- 4** Type the device name of your G-570U as the URL. ZyXELXXXX is the default where “XXXX” is the last four digits of the MAC address. The MAC address is on the bottom of the device). You could also use the IP address of the G-570U (192.168.1.2 is the default). Press **Enter**.

**Figure 17** Web Configurator Address



5 Type "1234" (default) as the password and click **Login**.

**Figure 18** Login Screen

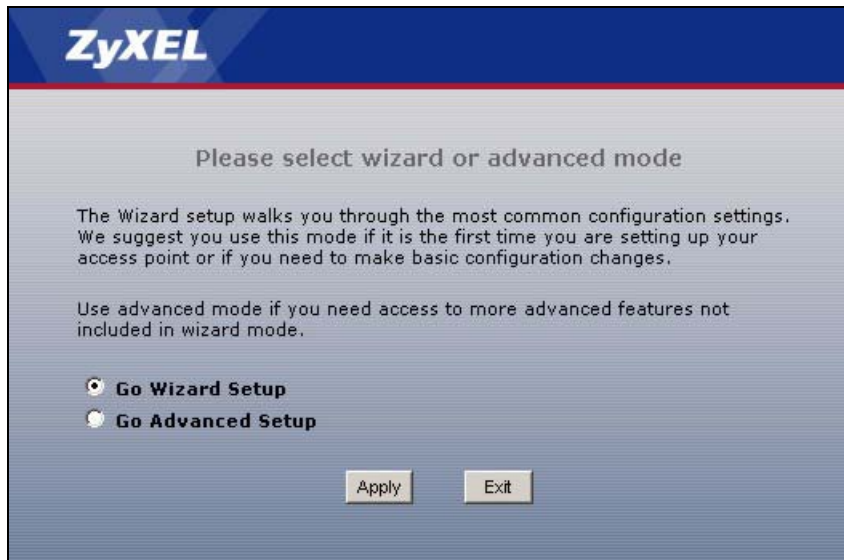


6 Select your language and click **Apply**.

**Figure 19** Language Screen



7 The following screen displays. Select **Go Wizard Setup** and click **Apply** to use the wizard setup screens for initial configuration (see [Section 3.3 on page 39](#)). Select **Go Advanced Setup** and click **Apply** to go directly to the advanced screens (see [Section 3.4 on page 45](#)).

**Figure 20** Select Wizard or Advanced Setup Screen

### 3.3 Configuring the G-570U Using the Wizard

The wizard consists of a series of screens to help you configure your G-570U for wireless stations to access your wired LAN.

Use the following buttons to navigate the Wizard:

Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue to the next screen.

No configuration changes will be saved to the G-570U until you click **Finish**.

#### 3.3.1 Wizard: Basic Settings

Click **SETUP WIZARD** to display the first wizard screen shown next. Refer to the **System Screens** chapter for more background information.

- 1** Enter a descriptive name to identify the device in the Ethernet network.
- 2** Select **Obtain IP Address Automatically** if you want to put the device behind a router that assigns an IP address. If you select this by mistake, use the **RESET** button to restore the factory default IP address.
- 3** Select **Use fixed IP Address** to give the device a static IP address. The IP address you configure here is used for management of the device (accessing the web configurator).
- 4** Enter a **Subnet Mask** appropriate to your network and the **Gateway IP Address** of the neighboring device, if you know it. If you do not, leave the **Gateway IP Address** field as **0.0.0.0**.

Figure 21 Wizard: Basic Settings

**SETUP WIZARD** **ZyXEL**

Basic Settings

**Device Name**

Device Name:

**IP Address Assignment**

Obtain IP Address Automatically

Use Fixed IP Address

IP Address:  .  .  .

Subnet Mask:  .  .  .

Gateway IP Address:  .  .  .

### 3.3.2 Wizard: Wireless Settings

Use this wizard screen to set up the wireless LAN. See the chapter on the wireless screens for background information.

- 1** The SSID is a unique name to identify the device in a wireless network. Enter up to 32 printable characters. Spaces are allowed. If you change this field on the device, make sure all wireless stations use the same SSID in order to access the network.
- 2** IEEE 802.11a, 802.11b and 802.11g wireless modes are different wireless communications standards. If you choose **802.11a only**, **802.11b only** or **802.11g only** in the Wireless Mode field you will be able to communicate with other wireless devices using that mode only, and if you select **Auto (11b/11g)** you can communicate with wireless devices using either 802.11b mode or 802.11g mode.
- 3** A wireless device uses a channel to communicate in a wireless network. Select a channel that is not already in use by a neighboring wireless device.

**Note:** The wireless stations and this device must use the same SSID, wireless mode, channel and wireless security settings for wireless communication.



Figure 22 Wizard: Wireless Settings

**SETUP WIZARD** **ZyXEL**

STEP 1 → **STEP 2** → STEP 3 → STEP 4

**Wireless Settings**

**Wireless Settings**

Enter an unique SSID for your wireless network. To associate with this access point, all wireless clients must use the same SSID entered here below

**SSID:**

**Wireless Mode:**

**Channel:**

**Note:**  
Unless you're concerned with the interference from other access points, you do not need to change the following default channel

### 3.3.3 Wizard: Security Settings

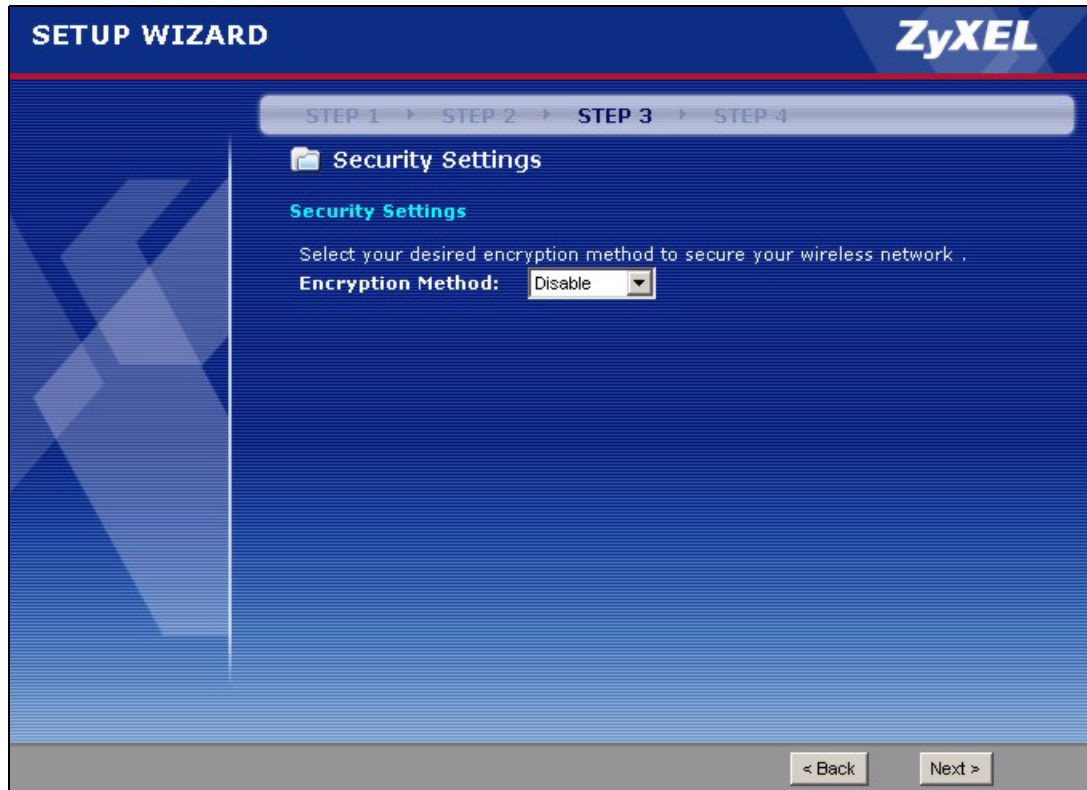
Use this screen to configure security for your wireless LAN. The screen varies depending on what you select in the **Encryption Method** field. Select **Disable** to have no wireless security configured, select **WEP**, or select **WPA-PSK** if your wireless clients support WPA-PSK. Select **WPA2-PSK** if your wireless clients support WPA2-PSK. Go to **Wireless > Security** if you want to use WPA2, WPA or 802.1x. See [Chapter 6 on page 57](#) for background information.

#### 3.3.3.1 Disable

Select **Disable** to have no wireless LAN security configured. If you do not enable any wireless security on your device, your network is accessible to any wireless networking device within range.

**Note:** With no wireless security a neighbor can access and see traffic in your network.

Figure 23 Setup Wizard 3: Disable



### 3.3.3.2 WEP

- 1 WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select **64-bit**, or **128-bit** from the **WEP Encryption** drop-down list box. The higher the WEP encryption, the higher the security but the slower the throughput.
- 2 You can generate or manually enter a WEP key.
  - Enter a **Passphrase** (up to 32 printable characters) and click **Generate**. The device automatically generates WEP keys. One key displays in the **Key 1** field. Go to **Wireless > Security** if you want to see the other WEP keys.
  - or
  - Enter a manual key in the **Key 1** field.

Figure 24 Wizard 3: WEP

**SETUP WIZARD** **ZyXEL**

STEP 1 ▶ STEP 2 ▶ **STEP 3** ▶ STEP 4

**Security Settings**

**Security Settings**

WEP key is the basic encryption method. Choose the encryption level below.

**Encryption Method:**

**WEP Encryption:**

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.

**Passphrase:**   (max. 16 characters)

**Key 1:**

**Note:**

**Manual WEP Key :**

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F").

### 3.3.3.3 WPA(2)-PSK

Select **WPA-PSK** or **WPA2-PSK** only if your wireless clients support it.

Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.

**Figure 25** Wizard 3: WPA(2)-PSK

**SETUP WIZARD** **ZyXEL**

STEP 1 → STEP 2 → **STEP 3** → STEP 4

**Security Settings**

**Security Settings**

WPA-PSK is an advanced encryption method. By sharing the Pre-Shared Key you entered below, the wireless clients or other access points can securely associate.

**Encryption Method:**

**Pre-Shared Key:**  (8-63 ASCII characters)

### 3.3.4 Wizard: Confirm Your Settings

This read-only screen shows the status of the current settings. Use the summary table to check whether what you have configured is correct. Click **Finish** to complete the wizard configuration and save your settings.

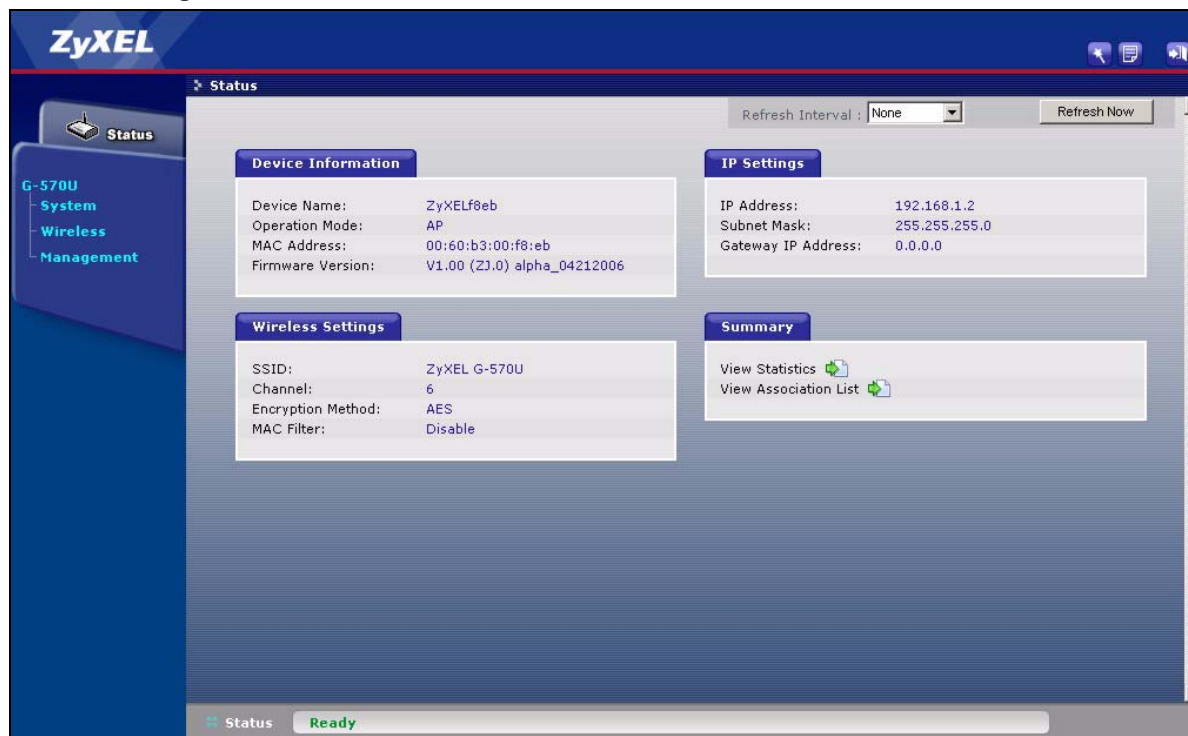
**Figure 26** Wizard: Confirm Your Settings

For more detailed background information, see the rest of this User's Guide.

### 3.4 Navigating the Advanced Screens




The **STATUS** screen is the first advanced screen that displays. This section explains how to navigate the advanced configuration screens. See the chapter on the **Status** screen for details about the individual screen.

Figure 27 Status Screen



The following table describes the global web configurator icons (in the upper right corner of most screens).

Table 4 Global Icon Key

ICON	DESCRIPTION
	Click the <b>Wizard</b> icon to open the setup wizard.
	Click the <b>About</b> icon to view copyright information.
	Click the <b>Logout</b> icon at any time to exit the web configurator. Make sure you save any changes before you log out.

### 3.4.1 Navigation Panel

After you enter the password, use the links on the navigation panel to go to the various advanced screens.

The following table describes the sub-menus.

**Table 5** Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the G-570U's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
System		Use this screen to configure the device name and IP address assignment settings.
Wireless	Wireless Settings	Use this screen to configure the wireless LAN.
	Security	Use this screen to configure wireless LAN security settings.
	MAC Filter	Use the MAC filter screen to configure the G-570U to allow access to devices or block the devices from accessing the G-570U.
	OTIST	This screen allows you to assign the G-570U's wireless security settings to the wireless clients.
Management	Password	Use this screen to configure the administrator password.
	Logs	Use this screen to view logs and alert messages.
	Configuration File	Use this screen to backup and restore the configuration or reset the factory defaults to your G-570U.
	F/W Upload	Use this screen to upload firmware to your G-570U.

**Note:** See the rest of this User's Guide for configuration details and background information on all G-570U features using the web configurator.





# CHAPTER 4

## Status Screens

This chapter describes the Status screens.

### 4.1 System Status

Click **Status** to open the following screen. The Status screen displays a snapshot of your device's settings. You can also view network statistics and a list of wireless stations currently associated with your device. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

**Figure 28** Status



The following table describes the labels in this screen.

**Table 6** Status

LABEL	DESCRIPTION
Refresh Interval	Use the drop-down list box to select how often you want the device to renew the information on this screen.
Refresh Now	Click this button to have the device renew the information on this screen.
Device Information	
Device Name	This is the same as the device name you entered in the first wizard screen, if you entered one there. It is for identification purposes.
Operation Mode	This field shows whether the device is functioning as an access point, a wireless client, a bridge or an access point and repeater.

**Table 6** Status

<b>LABEL</b>	<b>DESCRIPTION</b>
MAC Address	This field displays the MAC address of the device. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer. A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Firmware Version	This is the firmware version and the date the firmware was created.
IP Settings	
IP Address	This is the Ethernet port IP address.
Subnet Mask	This is the Ethernet port subnet mask.
Gateway IP Address	This is the IP address of a gateway. Leave this field as <b>0.0.0.0</b> if you do not know it.
Wireless Settings	
SSID	This is the descriptive name used to identify the device in a wireless network.
Channel	This field displays the radio channel the device is currently using.
Encryption Method	This field shows whether data encryption is activated ( <b>WEP</b> (WEP or 802.1x with WEP), <b>TKIP</b> (WPA, WPA-PSK), <b>AES</b> (WPA2, WPA2-PSK), <b>AES+TKIP</b> (WPA & WPA2, WPA-PSK & WPA2-PSK)) or inactive ( <b>Disable</b> ).
MAC Filter	This field shows whether MAC filter is enabled or not. With MAC filtering, you can allow or deny access to the device based on the MAC addresses of the wireless stations.
Summary	
View Statistics	Click <b>View Statistics</b> to see performance statistics such as number of packets sent and number of packets received.
View Association List	Click <b>View Association List</b> to show the wireless stations that are currently associated to the device.

### 4.1.1 Statistics

Click **View Statistics** in the **Status** screen. This screen displays read-only information including port status and packet-specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 29** Status: View Statistics

View Status		
<b>Ethernet</b>		
	Received	Transmitted
Packets	1980	2081
Bytes	225615	917508
<b>Wireless</b>		
	Received	Transmitted
Unicast Packets	0	2
Broadcast Packets	0	6
Multicast Packets	0	0
Total Packets	0	8
Total Bytes	0	1109
System Up Time : 0:57:40		
Poll Interval : 5 sec <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>		

The following table describes the labels in this screen.

**Table 7** Status: View Statistics

LABEL	DESCRIPTION
Ethernet	
Packets	This row displays the numbers of packets received and transmitted by the Ethernet port.
Bytes	This row displays the numbers of bytes received and transmitted by the Ethernet port.
Wireless	
Unicast Packets	This row displays the numbers of unicast packets received and transmitted by the wireless adapter.
Broadcast Packets	This row displays the numbers of broadcast packets received and transmitted by the wireless adapter.
Multicast Packets	This row displays the numbers of multicast packets received and transmitted by the wireless adapter.
Total Packets	This row displays the numbers of all types of packets received and transmitted by the wireless adapter.
Total Bytes	This row displays the numbers of bytes received and transmitted by the wireless adapter.
System Up Time	This is the total time the device has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

## 4.1.2 Association List

Click **Status** and then the **View Association List** button to display the **Association List** screen. When the device is not in wireless client mode, this screen displays which wireless stations are currently associated to the device in the **Association List** screen. When the device is in Wireless Client mode, it displays details of the access point to which the device is associated.

**Figure 30** Status: View Association List



The following table describes the labels in this screen.

**Table 8** Status: View Association List

LABEL	DESCRIPTION
No.	This is the index number of an associated device.
MAC Address	This field displays the MAC address of an associated device.
IP Address	This field displays the IP address of an associated device.
Signal Strength	This field displays the signal strength of each associated device.
Status	This field displays <b>Associated</b> for associated devices.
Rescan	Click <b>Rescan</b> to check for associated devices.

# CHAPTER 5

## System Screen

This chapter provides information on the **System** screen.

### 5.1 TCP/IP Parameters

#### 5.1.1 IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

**Table 9** Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

**Note:** Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

#### 5.1.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the device unless you are instructed to do otherwise.

## 5.2 System Settings

Click **System** to open the **System Settings** screen.

**Figure 31** System Settings

The following table describes the labels in this screen.

**Table 10** System Settings

LABEL	DESCRIPTION
Device Settings	
Device Name	This name can be up to 15 printable characters long. Spaces are not allowed.
IP Address Assignment	

**Table 10** System Settings

<b>LABEL</b>	<b>DESCRIPTION</b>
Obtain IP Address Automatically	Select this option to have your device use a dynamically assigned IP address from a router each time.
Use fixed IP address	Select this option to have your device use a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your device in dotted decimal notation.
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the device. The gateway helps forward packets to their destinations. Leave this field as <b>0.0.0.0</b> if you do not know it.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.





# CHAPTER 6

## Wireless Screens

This chapter discusses how to configure wireless settings and wireless security on your G-570U.

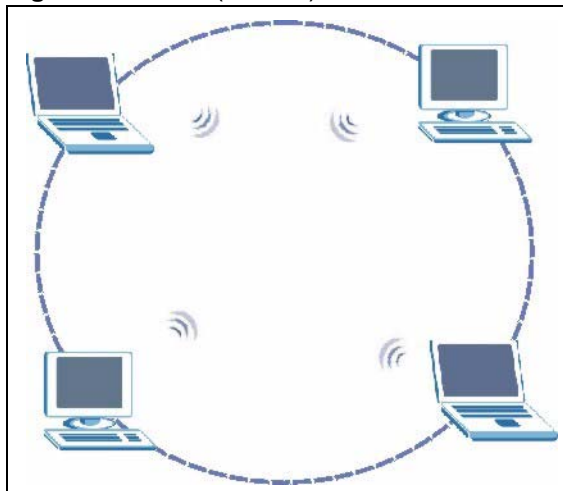
### 6.1 Wireless LAN Overview

This section introduces the wireless LAN (WLAN) and some basic scenarios.

#### 6.1.1 IBSS

An Independent Basic Service Set (IBSS), also called an Ad-hoc network, is the simplest WLAN configuration. An IBSS is defined as two or more computers with wireless adapters within range of each other that form an independent (wireless) network without the need of an access point (AP).

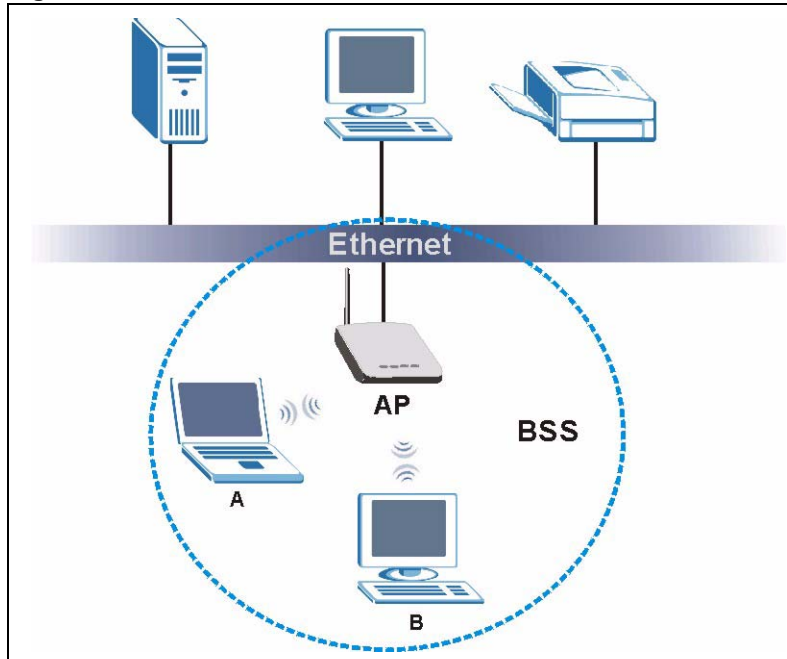
**Figure 32** IBSS (Ad-hoc) Wireless LAN



#### 6.1.2 BSS

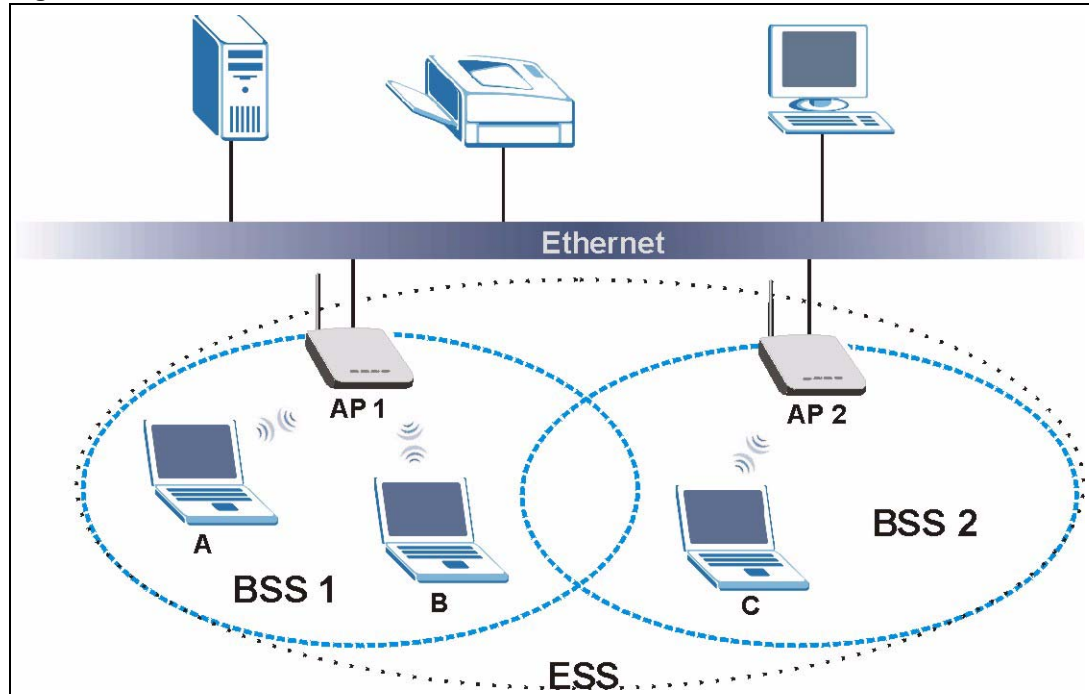
A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless stations **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station **A** and **B** can still access the wired network but cannot communicate with each other.

**Figure 33** Basic Service set

### 6.1.3 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

**Figure 34** Extended Service Set

## 6.2 Wireless LAN Basics

This section describes the wireless LAN network terms.

### 6.2.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

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

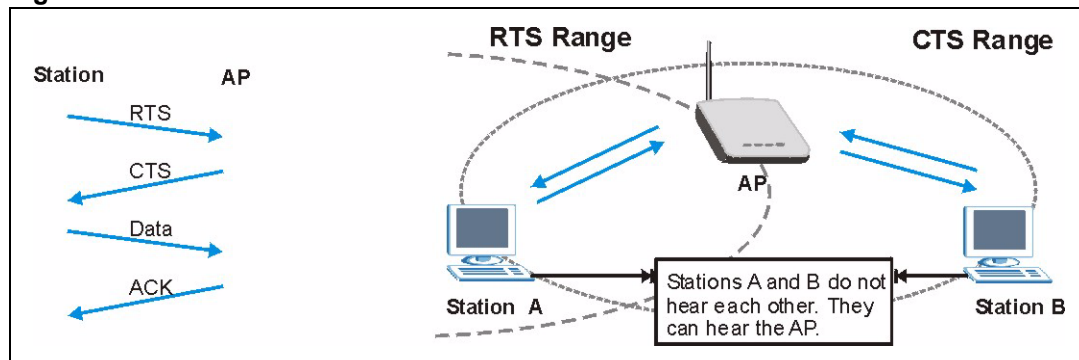
### 6.2.2 SSID

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

### 6.2.3 RTS/CTS

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

**Figure 35** RTS/CTS



When station A sends data to the G-570U, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

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

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

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

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

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

**Note:** Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## 6.2.4 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the G-570U will fragment the packet into smaller data frames.

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

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

## 6.3 Configuring Wireless

Click **Wireless** to display the **Wireless Settings** screen. The screen varies depending upon the operation mode you select.

### 6.3.1 Access Point Mode

Select **AP** (access point) in the **Operation Mode** field to display the screen shown next. This mode has the device act as an access point (AP) through which wireless stations can communicate and/or access a wired network.

**Figure 36** Wireless Settings: Access Point

Basic Settings	
Operation Mode	<input type="text" value="AP"/>
SSID	<input type="text" value="ZyXEL G-570U"/> (max.32 printable characters) <input type="checkbox"/> Hide SSID
Wireless Mode	<input type="text" value="Auto (11g/11b)"/>
Channel	<input type="text" value="6"/>
Advanced Settings	
Beacon Interval	<input type="text" value="100"/> (20-1000)
Intra-BSS Traffic	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Interval	<input type="text" value="1"/> (1~255)
Number of Wireless Stations Allowed to Associate	<input type="text" value="32"/> (1~32)
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Data Rate Management	<input type="text" value="Best"/>
Preamble Type	<input type="text" value="Dynamic"/>
RTS/CTS Threshold	<input type="text" value="2346"/> (0~2346)
Fragmentation	<input type="text" value="2346"/> (256~2346)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

**Table 11** Wireless Settings: Access Point

LABEL	DESCRIPTION
Operation Mode	Select the operating mode from the drop-down list. The options are <b>AP</b> , <b>Wireless Client</b> , <b>Bridge</b> and <b>AP+Repeater</b> .
SSID	Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable characters) for the wireless LAN. Spaces are allowed.  <b>Note:</b> If you are configuring the device from a computer connected to the wireless LAN and you change the device's SSID, channel or security settings, you will lose your wireless connection when you press <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the device's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Refer to the chapter on wizard setup for more information about channels.
Wireless Mode	Select <b>802.11a only</b> to allow only IEEE 802.11a compliant WLAN devices to associate with the device. Select <b>802.11b only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the device. Select <b>802.11g only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the device. Select <b>Auto (11g/11b)</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the device. The transmission rate of your device might be reduced.
Advanced Settings	
Beacon Interval	Set the number of milliseconds that should pass between the sending out of beacons.
Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Enable Intra-BSS traffic to allow wireless stations connected to the device to communicate with each other. Disable Intra-BSS traffic to only allow wireless stations to communicate with the wired network, not with each other.
DTIM Interval	Set the interval for wireless clients in sleep mode to wake up and check for multicast or broadcast traffic.  The AP includes a Delivery Traffic Indication Message (DTIM) in the beacon to notify wireless clients in sleep mode that there is a multicast or broadcast packet awaiting delivery. The interval is a multiple of the beacon interval. For example, if the beacon interval is 100 milliseconds and the DTIM interval is 2, the AP includes a DTIM with every second beacon (or every 200 milliseconds).
Number of Wireless Stations Allowed to Associate:	Use this field to set a maximum number of wireless stations that may connect to the device. Enter the number (from 1 to 32) of wireless stations allowed.

**Table 11** Wireless Settings: Access Point (continued)

LABEL	DESCRIPTION
Radio Enable	Turn on the wireless adapter to allow wireless communications between the device and other wireless devices. Turn off the wireless adapter to stop wireless communications between the device and other wireless devices.
Data Rate Management	Use this field to select a maximum data rate for the wireless connection(s). Please note that this is a total rate to be shared by all of the device's wireless connections.
Preamble Type	<p>Preamble is used to signal that data is coming to the receiver. <b>Short</b> and <b>Long</b> refer to the length of the synchronization field in a packet.</p> <p>Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble.</p> <p>Select <b>Long</b> preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.</p> <p>Select <b>Dynamic</b> to have the device automatically use short preamble when all wireless clients support it, otherwise the device uses long preamble.</p> <p><b>Note:</b> The device and the wireless stations <b>MUST</b> use the same preamble mode in order to communicate.</p>
RTS/CTS Threshold	Enter a value between 0 and 2346. The default is <b>2346</b> .
Fragmentation	Enter a value between 256 and 2346. The default is <b>2346</b> . It is the maximum data fragment size that can be sent.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.3.2 Wireless Client Mode

Select **Wireless Client** in the **Operation Mode** field to display the screen shown next. This mode has the device act as wireless client to connect to a wireless network.

**Note:** WPA, WPA2 and IEEE 802.1x wireless security are not available when you use Wireless Client, Bridge or AP+Repeater mode.

**Figure 37** Wireless Settings: Wireless Client

The screenshot shows a web-based configuration interface for a ZyXEL G-570U wireless device. It is titled 'Wireless Settings: Wireless Client'. The interface is organized into two main sections: 'Basic Settings' and 'Advanced Settings'.  
 In the 'Basic Settings' section, there are two fields: 'Operation Mode' is a dropdown menu currently showing 'Wireless Client', and 'SSID' is a text input field containing 'ZyXEL G-570U' with a note '(max.32 printable characters)'.  
 In the 'Advanced Settings' section, there are four settings: 'Radio Enable' has two radio buttons, with 'Yes' selected; 'Preamble Type' is a dropdown menu set to 'Dynamic'; 'RTS/CTS Threshold' is a text input field with '2346' and a range '(0~2346)'; and 'Fragmentation' is a text input field with '2346' and a range '(256~2346)'.  
 At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 12** Wireless Settings: Wireless Client

LABEL	DESCRIPTION
Operation Mode	Select the operating mode from the drop-down list. The options are <b>AP</b> , <b>Wireless Client</b> , <b>Bridge</b> and <b>AP+Repeater</b> .
SSID	Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable characters) for the wireless LAN. Spaces are allowed.  <b>Note:</b> If you are configuring the device from a computer connected to the wireless LAN and you change the device's SSID, channel or security settings, you will lose your wireless connection when you click <b>Apply</b> to save your settings. You must then change the wireless settings of your computer to match the device's new settings.
Advanced Settings	
Radio Enable	Turn on the wireless adapter to allow wireless communications between the device and other wireless devices. Turn off the wireless adapter to stop wireless communications between the device and other wireless devices.
Preamble Type	Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble.  Select <b>Long</b> preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.  Select <b>Dynamic</b> to have the device automatically use short preamble when all wireless clients support it, otherwise the device uses long preamble.  <b>Note:</b> The device and the wireless stations <b>MUST</b> use the same preamble mode in order to communicate.



**Table 12** Wireless Settings: Wireless Client (continued)

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2346. The default is <b>2346</b> .
Fragmentation	Enter a value between 256 and 2346. The default is <b>2346</b> . It is the maximum data fragment size that can be sent.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

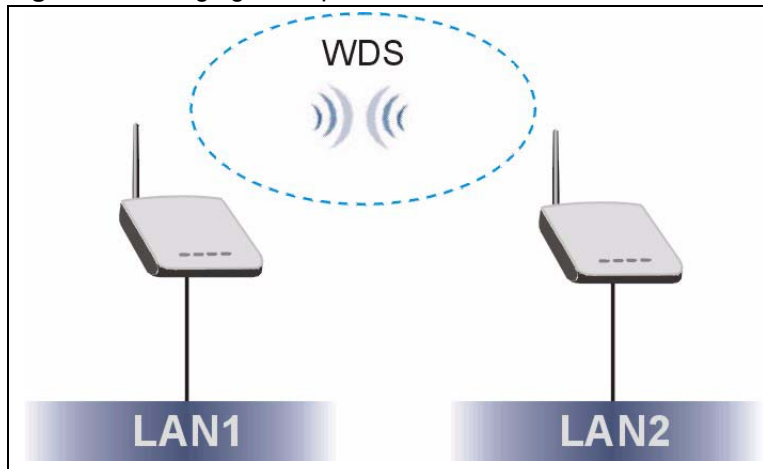
### 6.3.3 Bridge Mode

The device can act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

When two devices connect in **Bridge** mode, they form a WDS (Wireless Distribution System) allowing the computers in one LAN to connect to the computers in another LAN. See the following example.

**Note:** WPA, WPA2 and IEEE 802.1x wireless security are not available when you use Wireless Client, Bridge or AP+Repeater mode.

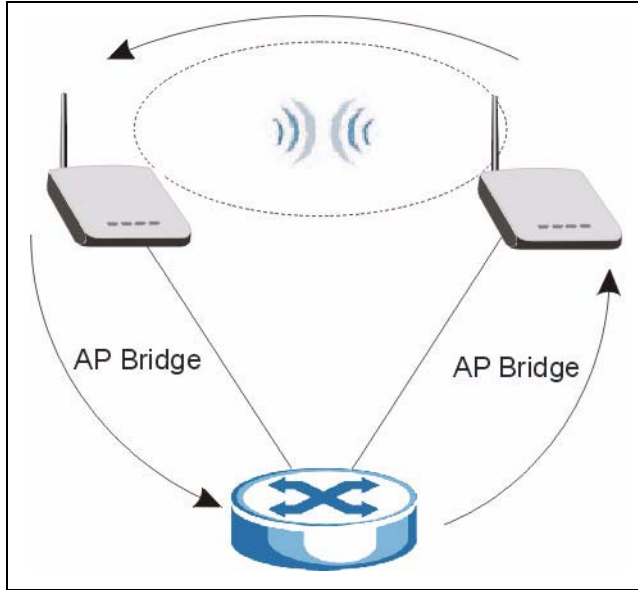
You can only use WEP keys to encrypt traffic between APs.

**Figure 38** Bridging Example

Be careful to avoid bridge loops when you enable bridging in the G-570U. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

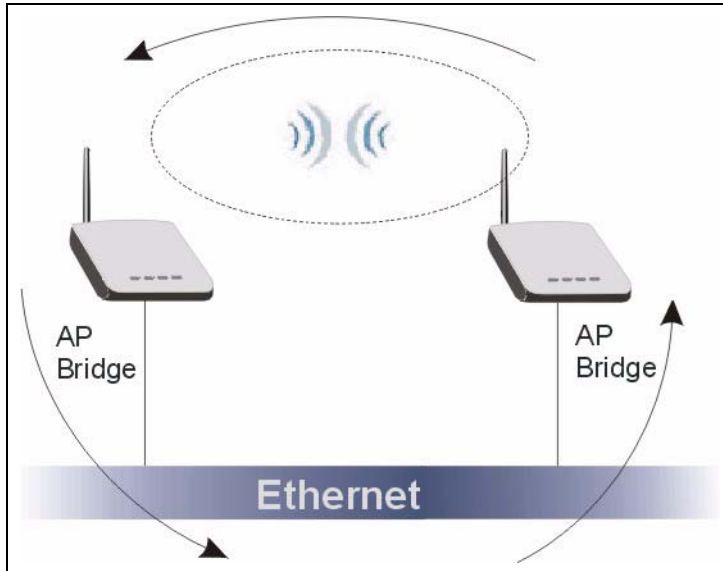
If two or more G-570Us (in bridge mode) are connected to the same hub as shown next.

**Figure 39** Bridge Loop: Two Bridges Connected to Hub



If your G-570U (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN as shown next.

**Figure 40** Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that your G-570U is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

Select **Bridge** as the **Operation Mode** to have the device act as a wireless bridge only.

**Figure 41** Wireless Settings: Bridge

Basic Settings	
Operation Mode	Bridge
Wireless Mode	Auto (11g/11b)
Channel	6
WDS Settings	
Local MAC Address	00 : 60 : b3 : 00 : f8 : eb
Remote MAC Address 1	: : : : : :
Remote MAC Address 2	: : : : : :
Remote MAC Address 3	: : : : : :
Remote MAC Address 4	: : : : : :
Advanced Settings	
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Data Rate Management	Best
Preamble Type	Dynamic
RTS/CTS Threshold	2346 (0~2346)
Fragmentation	2346 (256~2346)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

**Table 13** Wireless Settings: Bridge

LABEL	DESCRIPTION
Operation Mode	<p>Select the operating mode from the drop-down list. The options are <b>AP</b>, <b>Wireless Client</b>, <b>Bridge</b> and <b>AP+Repeater</b>.</p> <p><b>Note:</b> If you are configuring the device from a computer connected to the wireless LAN and you change the device to use bridge mode, you will lose your wireless connection when you click <b>Apply</b> to save your settings. You must then connect to the device through the wired network.</p>
Channel	<p>Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.</p> <p>Refer to the chapter on wizard setup for more information about channels.</p>

**Table 13** Wireless Settings: Bridge (continued)

LABEL	DESCRIPTION
Wireless Mode	<p>Select <b>802.11a</b> only to allow only IEEE 802.11a compliant WLAN devices to associate with the device.</p> <p>Select <b>802.11b only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the device.</p> <p>Select <b>802.11g only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the device.</p> <p>Select <b>Auto (11g/11b)</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the device. The transmission rate of your device might be reduced.</p>
Local MAC Address	This is the MAC address of the device.
Remote MAC Address 1~4	Type the MAC address of the peer device in a valid MAC address format; six hexadecimal character pairs (for example, 12:34:56:78:9a:bc).
Advanced Settings	
Radio Enable	Turn on the wireless adapter to allow wireless communications between the device and other wireless devices. Turn off the wireless adapter to stop wireless communications between the device and other wireless devices.
Data Rate Management	Use this field to select a maximum data rate for the wireless connection(s). Please note that this is a total rate to be shared by all of the device's wireless connections.
Preamble Type	<p>Preamble is used to signal that data is coming to the receiver.</p> <p>Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble.</p> <p>Select <b>Long</b> preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.</p> <p>Select <b>Dynamic</b> to have the device automatically use short preamble when all wireless clients support it, otherwise the device uses long preamble.</p> <p><b>Note:</b> The device and the wireless stations <b>MUST</b> use the same preamble mode in order to communicate.</p>
RTS/CTS Threshold	Enter a value between 0 and 2346. The default is <b>2346</b> .
Fragmentation	Enter a value between 256 and 2346. The default is <b>2346</b> . It is the maximum data fragment size that can be sent.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.3.4 AP+Repeater Mode

Select **AP+Repeater** as the **Operation Mode** to have the device act as an access point and a wireless bridge.

**Figure 42** Wireless Settings: AP+Repeater

Basic Settings	
Operation Mode	AP+Repeater
SSID	ZyXEL G-570U (max.32 printable characters) <input type="checkbox"/> Hide SSID
Wireless Mode	Auto (11g/11b)
Channel	6
WDS Settings	
Local MAC Address	00 : b0 : b3 : 00 : f8 : eb
Remote MAC Address 1	: : : : : :
Remote MAC Address 2	: : : : : :
Remote MAC Address 3	: : : : : :
Remote MAC Address 4	: : : : : :
Advanced Settings	
Beacon Interval	100 (20-1000)
Intra-BSS Traffic	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Interval	1 (1-255)
Number of Wireless Stations Allowed to Associate	32 (1-32)
Radio Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Data Rate Management	Best
Preamble Type	Long
RTS/CTS Threshold	2346 (0-2346)
Fragmentation	2346 (256-2346)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

**Table 14** Wireless Settings: AP + Repeater

LABEL	DESCRIPTION
Operation Mode	Select the operating mode from the drop-down list. The options are <b>AP</b> , <b>Wireless Client</b> , <b>Bridge</b> and <b>AP+Repeater</b> .
SSID	Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable characters) for the wireless LAN. Spaces are allowed.  <b>Note:</b> If you are configuring the device from a computer connected to the wireless LAN and you change the device's SSID, channel or security settings, you will lose your wireless connection when you click <b>Apply</b> to save your settings. You must then change the wireless settings of your computer to match the device's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Refer to the chapter on wizard setup for more information about channels.

**Table 14** Wireless Settings: AP + Repeater (continued)

LABEL	DESCRIPTION
Wireless Mode	<p>Select <b>802.11a</b> only to allow only IEEE 802.11a compliant WLAN devices to associate with the device.</p> <p>Select <b>802.11b only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the device.</p> <p>Select <b>802.11g only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the device.</p> <p>Select <b>Auto (11g/11b)</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the device. The transmission rate of your device might be reduced.</p>
Local MAC Address	This is the MAC address of the device.
Remote MAC Address 1~4	Type the MAC address of the peer device in a valid MAC address format; six hexadecimal character pairs (for example, 12:34:56:78:9a:bc).
Advanced Settings	
Beacon Interval	Set the number of milliseconds that should pass between the sending out of beacons.
Intra-BSS Traffic	<p>Intra-BSS traffic is traffic between wireless stations in the same BSS.</p> <p>Enable Intra-BSS traffic to allow wireless stations connected to the device to communicate with each other.</p> <p>Disable Intra-BSS traffic to only allow wireless stations to communicate with the wired network, not with each other.</p>
DTIM Interval	<p>Set the interval for wireless clients in sleep mode to wake up and check for multicast or broadcast traffic.</p> <p>The AP includes a Delivery Traffic Indication Message (DTIM) in the beacon to notify wireless clients in sleep mode that there is a multicast or broadcast packet awaiting delivery. The interval is a multiple of the beacon interval. For example, if the beacon interval is 100 milliseconds and the DTIM interval is 2, the AP includes a DTIM with every second beacon (or every 200 milliseconds).</p>
Radio Enable	Turn on the wireless adapter to allow wireless communications between the device and other IEEE 802.11b and IEEE 802.11g compliant wireless devices. Turn off the wireless adapter to stop wireless communications between the device and other IEEE 802.11b and IEEE 802.11g compliant wireless devices.
Data Rate Management	Use this field to select a maximum data rate for the wireless connection(s). Please note that this is a total rate to be shared by all of the device's wireless connections.
Preamble Type	<p>Preamble is used to signal that data is coming to the receiver.</p> <p>Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble.</p> <p>Select <b>Long</b> preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.</p> <p>Select <b>Dynamic</b> to have the device automatically use short preamble when all wireless clients support it, otherwise the device uses long preamble.</p> <p><b>Note:</b> The device and the wireless stations <b>MUST</b> use the same preamble mode in order to communicate.</p>
RTS/CTS Threshold	Enter a value between 0 and 2346. The default is <b>2346</b> .
Fragmentation	Enter a value between 256 and 2346. The default is <b>2346</b> . It is the maximum data fragment size that can be sent.

**Table 14** Wireless Settings: AP + Repeater (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.4 Wireless Security Overview

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

The figure below shows the possible wireless security levels on your G-570U. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

**Table 15** Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	Wi-Fi Protected Access (WPA)
	WPA2

If you do not enable any wireless security on your G-570U, your network is accessible to any wireless networking device that is within range.

### 6.4.1 Encryption

- Use WPA(2) security if you have WP(2)A-aware wireless clients and a RADIUS server. WPA(2) has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- If you don't have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use the passphrase feature to automatically generate WEP keys or manually enter WEP keys.

### 6.4.2 Authentication

Use a RADIUS server with WPA or IEEE 802.1x key management protocol.

See the appendix for information on protocols used when a client authenticates with a RADIUS server via the G-570U.

### 6.4.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

### 6.4.4 Hide G-570U Identity

If you hide the ESSID, then the G-570U cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of “hiding” the G-570U may be inconvenience for some valid WLAN clients.

## 6.5 WEP Overview

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

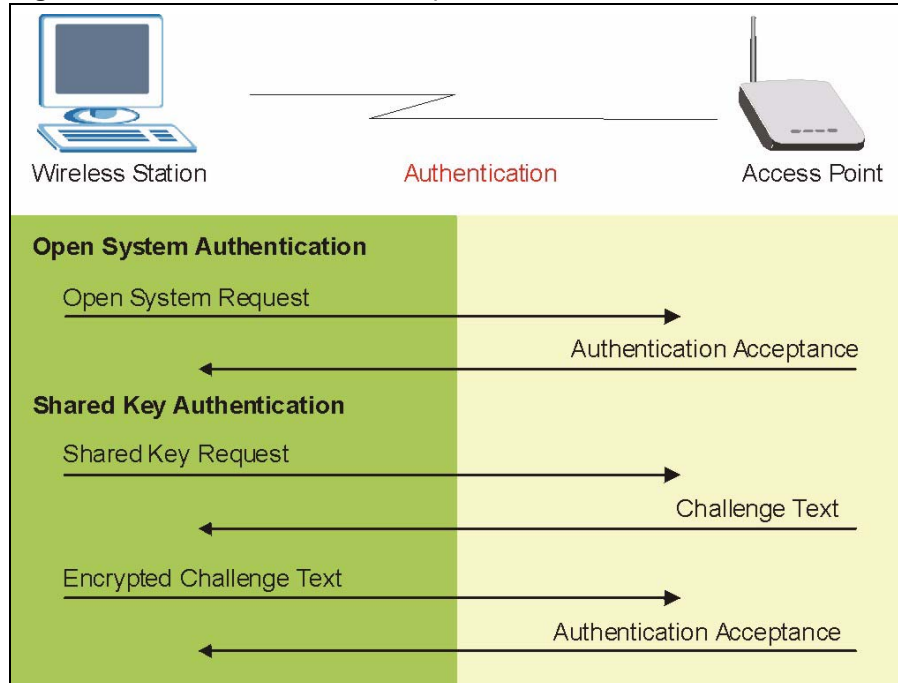
### 6.5.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your G-570U allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

### 6.5.2 Authentication

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared** and **Auto**. The following figure illustrates the steps involved.



**Figure 43** WEP Authentication Steps

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

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

When your G-570U's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the G-570U will accept either type of authentication request and the G-570U will fall back to use open authentication if the shared key does not match.

## 6.6 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the G-570U (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

## 6.7 Introduction to RADIUS

RADIUS is based on a client-server model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication  
Determines the identity of the users.
- Accounting  
Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your G-570U acts as a message relay between the wireless station and the network RADIUS server.

### 6.7.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request  
Sent by an access point, requesting authentication.
- Access-Reject  
Sent by a RADIUS server rejecting access.
- Access-Accept  
Sent by a RADIUS server allowing access.
- Access-Challenge  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request  
Sent by the access point requesting accounting.
- Accounting-Response  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the wired network from unauthorized access.

## 6.8 EAP Authentication Overview

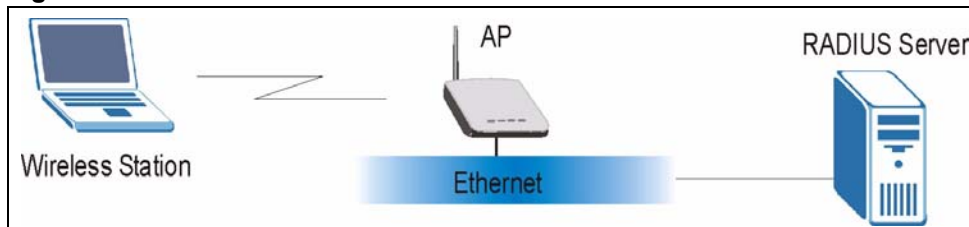
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS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

The type of authentication you use depends on the RADIUS server or the AP. The G-570U supports EAP-TLS, EAP-TTLS, EAP-MD5 and PEAP with RADIUS. Refer to the appendix about the types of EAP authentication for descriptions on the common types.

Your G-570U supports EAP-MD5 (Message-Digest Algorithm 5) and PEAP (Protected EAP) with the built-in RADIUS server.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

**Figure 44** EAP Authentication



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

- 1 The wireless station sends a “start” message to the G-570U.
- 2 The G-570U sends a “request identity” message to the wireless station for identity information.
- 3 The wireless station replies with identity information, including user name and password.
- 4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

## 6.9 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 WEP 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.

To use Dynamic WEP, enable and configure the RADIUS server and enable Dynamic WEP Key Exchange in the **WIRELESS Security 802.1x** screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

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

## 6.10 Introduction to 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.

### 6.10.1 Encryption

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

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

## 6.10.2 User Authentication

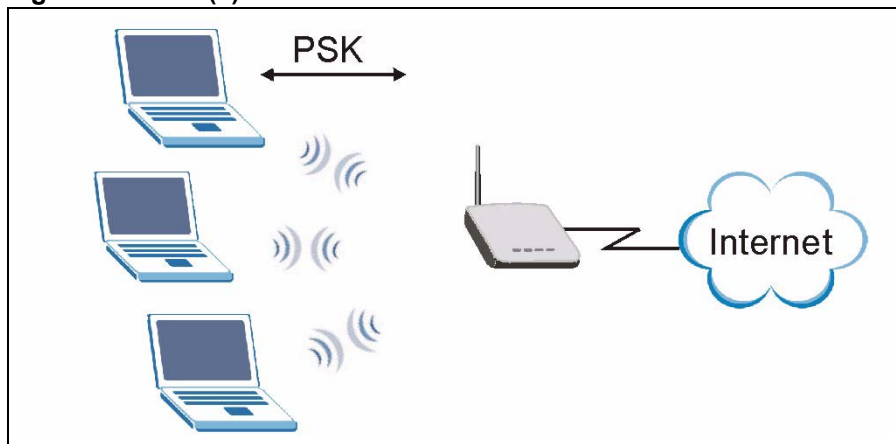
WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

## 6.11 WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2 The AP checks each client's password and (only) allows it to join the network if it matches its password.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 45 WPA(2)-PSK Authentication**



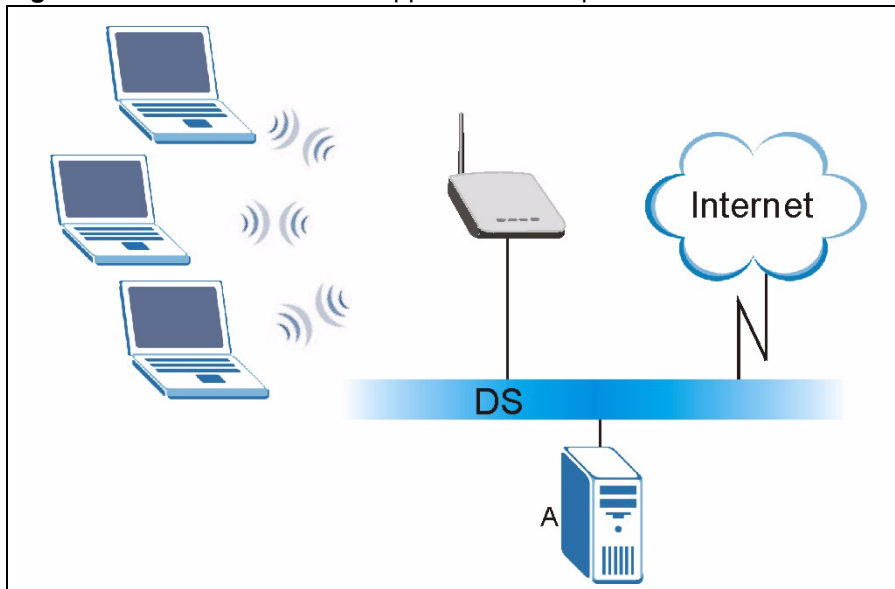
## 6.12 WPA(2) with RADIUS Application Example

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 46** WPA with RADIUS Application Example



## 6.13 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

**Table 16** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
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	No	Enable
WPA-PSK	TKIP	Yes	Enable

**Table 16** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

## 6.14 Configuring Wireless Security

In order to configure and enable wireless security; click **Wireless > Security** to display the **Security** screen. This screen varies according to the encryption method you select.

### 6.14.1 Wireless Security: Disable

If you do not enable any wireless security on your device, your network is accessible to any wireless networking device that is within range.

**Figure 47** Wireless Security: Disable

The following table describes the labels in this screen.

**Table 17** Wireless Security: Disable

LABEL	DESCRIPTION
Encryption Method	Select <b>Disable</b> to have no wireless LAN security configured.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.14.2 Wireless Security: WEP

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. You can configure up to four 64-bit or 128-bit WEP keys, but only one key can be used at any one time.

**Figure 48** Wireless Security: WEP

**Security Settings**

Encryption Method: WEP

Authentication Type: Open

Data Encryption: 128-bit WEP

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key

Passphrase: [\*\*\*\*\*] **Generate** (max. 16 alphanumeric, printable characters)

Key 1 [\*\*\*\*\*]

Key 2 [\*\*\*\*\*]

Key 3 [\*\*\*\*\*]

Key 4 [\*\*\*\*\*]

**Note:**  
**64-bit WEP:** Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)  
**128-bit WEP:** Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)

**Apply** **Reset**

The following table describes the labels in this screen.

**Table 18** Wireless Security: WEP

LABEL	DESCRIPTION
Encryption Method	Select <b>WEP</b> if you want to configure WEP encryption parameters.
Authentication Type	Select <b>Open</b> or <b>Shared</b> from the drop-down list box.
Data Encryption	Select <b>64 bit WEP</b> or <b>128 bit WEP</b> to enable data encryption.
Passphrase	Enter a "passphrase" (password phrase) of up to 16 case-sensitive printable characters and click <b>Generate</b> .
Generate	After you enter the passphrase, click <b>Generate</b> to have the device generate four different WEP keys automatically.
Key 1 to Key 4	If you want to manually set the WEP keys, enter the WEP key in the field provided. Select a WEP key to use for data encryption. The WEP keys are used to encrypt data. Both the device and the wireless stations must use the same WEP key for data transmission. If you chose <b>64 bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128 bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.14.3 Wireless Security: WPA(2)-PSK

Select **WPA-PSK**, **WPA2-PSK** or **WPA-PSK & WPA2-PSK** in the **Encryption Method** drop down list-box to display the screen displays as next.



**Figure 49** Wireless Security: WPA(2)-PSK

The following table describes the labels in this screen.

**Table 19** Wireless Security: WPA-PSK

LABEL	DESCRIPTION
Encryption Method	Select <b>WPA-PSK</b> , <b>WPA2-PSK</b> or <b>WPA-PSK &amp; WPA2-PSK</b> if you want to configure a pre-shared key. Choose this option only if your wireless clients support it.
Pre-Shared Key	The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 ASCII characters (including spaces and symbols). This field is case-sensitive.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

#### 6.14.4 Wireless Security: WPA(2)

WPA (Wi-Fi Protected Access) 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 user authentication and improved data encryption.

**Figure 50** Wireless Security: WPA(2)

The following table describes the labels in this screen.

**Table 20** Wireless Security: WPA(2)

LABEL	DESCRIPTION
Encryption Method	Select <b>WPA</b> , <b>WPA2</b> or <b>WPA &amp; WPA2</b> to configure user authentication and improved data encryption.  <b>Note:</b> WPA, WPA2 and IEEE 802.1x wireless security are not available when you use Wireless Client, Bridge or AP+Repeater mode.  You can only use WEP keys to encrypt traffic between APs.
Authentication Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812.  You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 64 printable characters and no spaces) as the key to be shared between the external authentication server and the device.  The key must be the same on the external authentication server and your device. The key is not sent over the network.
Reauthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 100 and 3600 seconds.  If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

**Table 20** Wireless Security: WPA(2) (continued)

LABEL	DESCRIPTION
Global-Key Update	This is how often the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Specify an interval either in seconds or thousands of packets that the device sends.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 6.14.5 Wireless Security: 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management.

**Note:** Once you enable user authentication, you need to specify an external RADIUS server on the device for authentication.

**Figure 51** Wireless Security: 802.1x

**Security Settings**

Encryption Method

Data Encryption

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key


Passphrase   (max. 16 alphanumeric, printable characters)

Key 1

Key 2

Key 3

Key 4

 **Note:**  
**64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)**  
**128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)**

**Authentication Server**

Authentication Server IP Address  .  .  .

Port Number

Shared Secret  (0-64 alphanumeric, printable characters and no spaces)

**Rekey Options**

Reauthentication Time  Seconds (max. 100 - 3600)

Global-Key Update

every  Seconds (max. 100 - 3600)

every  X1000 Packets (max. 100 - 3600)

The following table describes the labels in this screen.

**Table 21** Wireless Security: 802.1x

LABEL	DESCRIPTION
Encryption Method	<p>Select <b>802.1X</b> to configure authentication of wireless stations and encryption key management.</p> <p><b>Note:</b> WPA, WPA2 and IEEE 802.1x wireless security are not available when you use Bridge or AP+Repeater mode. You can only use WEP keys to encrypt traffic between APs.</p>
Data Encryption	<p>Select <b>None</b> to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.</p> <p>Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.</p> <p>Up to 32 stations can access the device when you configure dynamic WEP key exchange.</p>
Passphrase	<p>Enter a "passphrase" (password phrase) of up to 16 case-sensitive printable characters and click <b>Generate</b>.</p>
Generate	<p>After you enter the passphrase, click <b>Generate</b> to have the device generates four different WEP keys automatically.</p>
Key 1 to Key 4	<p>If you want to manually set the WEP keys, enter the WEP key in the field provided. Select a WEP key to use for data encryption.</p> <p>The WEP keys are used to encrypt data. Both the device and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose <b>64-bit WEP</b>, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose <b>128-bit WEP</b>, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p>
Authentication Server IP Address	<p>Enter the IP address of the external authentication server in dotted decimal notation.</p>
Port Number	<p>Enter the port number of the external authentication server. The default port number is 1812.</p> <p>You need not change this value unless your network administrator instructs you to do so with additional information.</p>
Shared Secret	<p>Enter a password (up to 64 printable characters) as the key to be shared between the external authentication server and the device.</p> <p>The key must be the same on the external authentication server and your device. The key is not sent over the network.</p>
Reauthentication Time	<p>Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 100 and 3600 seconds.</p> <p>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Global-Key Update	<p>This is how often the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.</p> <p>Specify an interval either in seconds or thousands of packets that the device sends.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the device.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 6.15 MAC Filter

The MAC filter screen allows you to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the device (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

The MAC filter works when the device functions as an AP. It allows or denies wireless client access. The MAC filter does not apply to bridge or repeater functions.

The following applies if you set the device to client mode and want to connect to an AP that uses a MAC filter. After the device turns on in client mode, it clones the MAC address of the first packets that it receives from devices connected to the Ethernet port. It uses this MAC address on the packets that it sends to an AP. All of the packets that the device sends to an AP will appear to be from the first device that connected to the Ethernet port. If you turn the device off and on, it again clones the MAC address of the first packets that it receives from devices connected to the Ethernet port. You may be able to check the association list on the AP to determine which MAC address the device is currently using.

To change your device's MAC filter settings, click **Wireless > MAC Filter**. The screen appears as shown.

**Note:** Be careful not to list your computer's MAC address and select **Deny the following MAC address to associate** when managing the device via a wireless connection. This would lock you out.

**Figure 52** MAC Filter

**MAC Address Filter**

Active

Allow the following MAC Address to associate

Deny the following MAC address to associate

#	MAC Address	#	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

**Table 22** MAC Filter

LABEL	DESCRIPTION
Active	Select the check box to enable MAC address filtering and define the filter action for the list of MAC addresses in the MAC address filter table. Select <b>Allow the following MAC address to associate</b> to permit access to the device, MAC addresses not listed will be denied access to the device. Select <b>Deny the following MAC address to associate</b> to block access to the device, MAC addresses not listed will be allowed to access the device.
#	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the device in these address fields.
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.16 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.

**Note:** OTIST replaces the pre-configured wireless settings on the wireless clients.

### 6.16.1 Enabling OTIST: G-570U in AP Mode

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

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

#### 6.16.1.1 AP

You can enable OTIST using the **OTIST** button or the web configurator.

##### 6.16.1.1.1 AP Mode: OTIST Button

If you use the **OTIST** 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 **OTIST** button for one or two seconds to activate OTIST.

##### 6.16.1.1.2 AP Mode: Web Configurator

Click **Wireless > OTIST** to configure and enable OTIST. The screen appears as shown.

**Note:** At the time of writing the device does not support OTIST in **Bridge** or **AP+Repeater** mode.

**Figure 53** AP Mode: OTIST

The screenshot shows the 'OTIST Settings' web page. At the top, there is a header 'OTIST Settings'. Below it, there is a 'Setup Key' field containing the text '01234567' and a note '(8 alphanumeric, printable characters)'. Underneath the field is a checked checkbox with the text: 'Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.' At the bottom of the form, there is a 'Start' button.

The following table describes the labels in this screen.

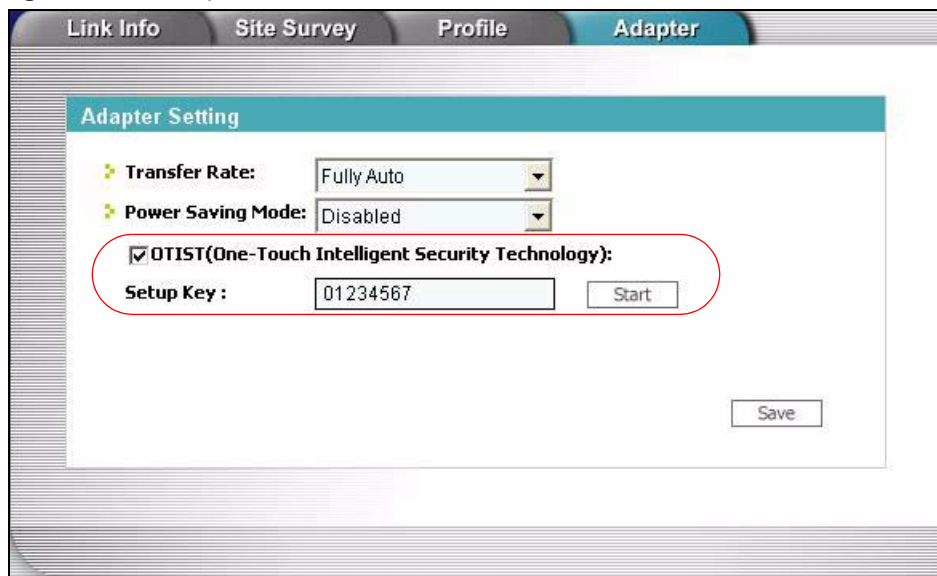
**Table 23** OTIST

LABEL	DESCRIPTION
OTIST Settings	
Setup Key	Enter the setup key of up to eight printable characters. The default OTIST setup key is "01234567".  <b>Note:</b> If you change the OTIST setup key here, you must also make the same change on the wireless client(s).
Yes!	To have OTIST automatically generate a WPA-PSK key, select this check box. If you manually configured a WEP key or a WPA-PSK key and you also select this check box, then the key you manually configured is used.  <b>Note:</b> This option is not available in Wireless Client mode.
Start	Click <b>Start</b> to encrypt the wireless security data using the setup key and have the device set the wireless client to use the same wireless settings as the device. You must also activate and start OTIST on the wireless client at the same time.  The process takes three minutes to complete.

### 6.16.1.2 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**.

**Figure 54** Example Wireless Client OTIST Screen



### 6.16.1.3 G-570U in Wireless Client Mode

If you are using the G-570U in Wireless Client mode, you can enable OTIST using either the OTIST button or the web configurator.



### 6.16.1.3.1 Wireless Client Mode: OTIST Button

If you use the **OTIST** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used.

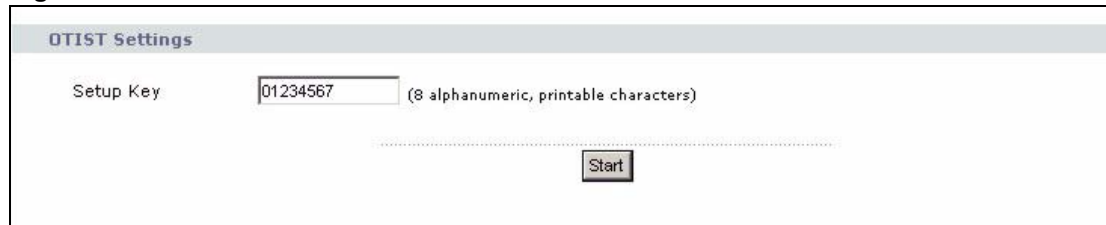
Double-click the **OTIST** button to automatically change the G-570U to wireless client mode and start OTIST.

### 6.16.1.3.2 Wireless Client Mode: Web Configurator

Start the web configurator and click **Wireless**. Select **Wireless Client** in the **Operation Mode** field.

Click on the **OTIST** tab. The screen displays as shown. Enter the same **Setup Key** as your AP's. Click **Start** when you are ready to begin OTIST.

**Figure 55** G-570U in Wireless Client Mode: OTIST Screen

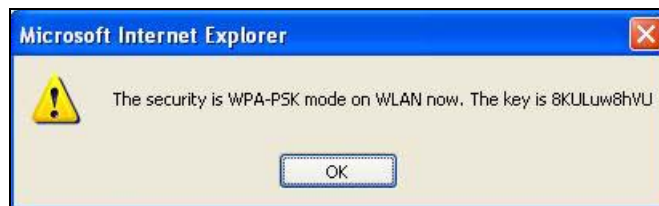


## 6.16.2 Starting OTIST

**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.

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

**Figure 56** Security Key

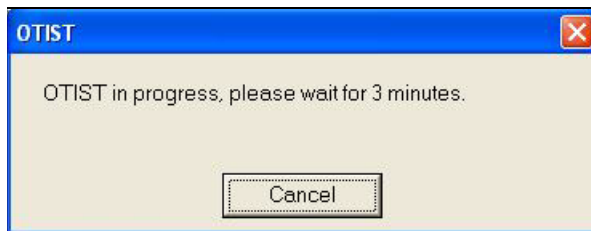


- 2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

**Figure 57** OTIST in Progress (AP)



**Figure 58** OTIST in Progress (Client)



- 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.

**Figure 59** No AP with OTIST Found



- 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.

### 6.16.3 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.

**Figure 60** Start OTIST?

- 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 **OTIST** 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 wireless clients again.



# CHAPTER 7

## Management Screens

This chapter describes the Maintenance screens.

### 7.1 Maintenance Overview

Use these maintenance screens to change the password, view logs, back up or restore the G-570U configuration and change the web configurator language.

### 7.2 Password

To change your device's password (recommended), click **Management**. The screen appears as shown. This screen allows you to change the device's password.

If you forget your password (or the device IP address), you will need to reset the device. See the section on resetting the device for details.

**Figure 61** Management: Password

The screenshot shows a web interface titled "Password Setup". It contains three text input fields stacked vertically. The first is labeled "Current Password". The second is labeled "New Password" and has a small text note to its right that says "(max 19 characters)". The third is labeled "Retype to Confirm". Below the input fields, there are two buttons: "Apply" and "Reset".

The following table describes the labels in this screen.

**Table 24** Management: Password

LABEL	DESCRIPTION
Current Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 19 printable characters). Spaces are not allowed. Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.

**Table 24** Management: Password (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the device.
Reset	Click <b>Reset</b> to clear all fields in this screen.

## 7.3 Logs

Click **Management > Logs** to open the **Logs** screen.

You can view logs and alert messages in this screen. Once the log table is full, old logs are deleted as new logs are created.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

**Figure 62** Management: Logs

Log List			
<input type="button" value="Refresh"/> <input type="button" value="Clear Log"/>			
#	Time ▾	Source	Message
1	783	00:60:B3:45:67:89	WLAN service started
2	785	00:60:B3:45:67:89	WLAN service stopped
3	785	00:60:B3:45:67:89	WLAN service started
4	3463	00:60:B3:45:67:89	WLAN service stopped
5	3463	00:60:B3:45:67:89	WLAN service started
6	5750	00:60:B3:45:67:89	WLAN service stopped
7	5750	00:60:B3:45:67:89	WLAN service started
8	5903	00:60:B3:45:67:89	WLAN service stopped
9	5903	00:60:B3:45:67:89	WLAN service started

The following table describes the labels in this screen.

**Table 25** Management: Logs

LABEL	DESCRIPTION
Display	Select a category of logs to view.
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to clear all the logs.
#	This is the log's index number.
Time	This field displays the time the log was recorded. It is the number of seconds since the last time the system turned on.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet that caused the log.

**Table 25** Management: Logs (continued)

LABEL	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the outgoing packet that caused the log.
Note	This field displays additional information about the log entry.

## 7.4 Configuration File

The configuration file (often called the romfile or rom-0) contains the factory default settings such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a .rom filename extension. Once you have customized the device's settings, they can be saved back to your computer under a filename of your choosing.

Click **Management > Configuration File**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 63** Management: Configuration File

**Backup Configuration**

This page allows you to backup your current configuration to your computer. Click the **"Backup"** button to start the backup process.

---

**Restore Configuration**

To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the **"Upload"** button

File Path:

---

**Back to Factory Defaults**

The **"Reset"** button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again.

- Password: 1234
- LAN IP Address: 192.168.1.2

### 7.4.1 Backup Configuration

Backup configuration allows you to back up (save) the device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the device's current configuration to your computer.

## 7.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your device.

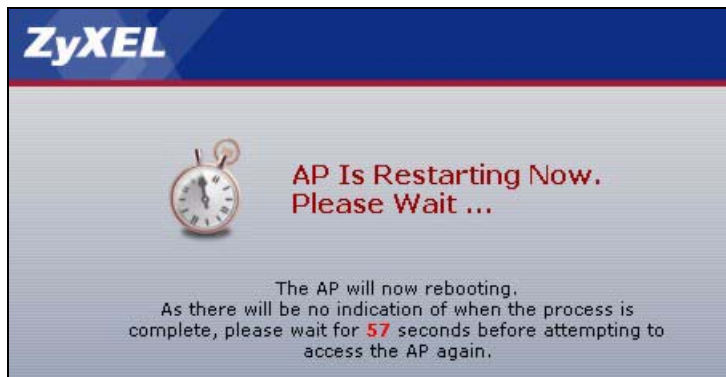
**Table 26** Management: Configuration File: Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.

**Note:** Do not turn off the device while configuration file upload is in progress.

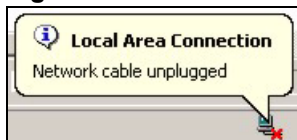
The following screen displays. You must wait one minute before logging into the device again.

**Figure 64** Configuration Upload Successful



The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 65** Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.2).

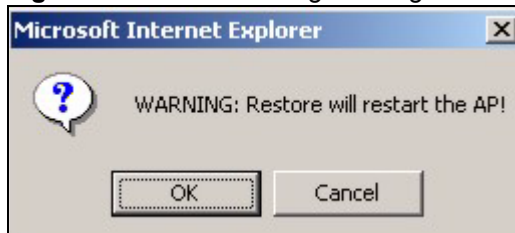
If the upload was not successful, the following screen will appear. Click **Return** to go back to the Configuration File screen.



**Figure 66** Configuration Upload Error

### 7.4.3 Back to Factory Defaults

Clicking the **RESET** button in this section clears all user-entered configuration information and returns the device to its factory defaults. The following warning screen will appear.

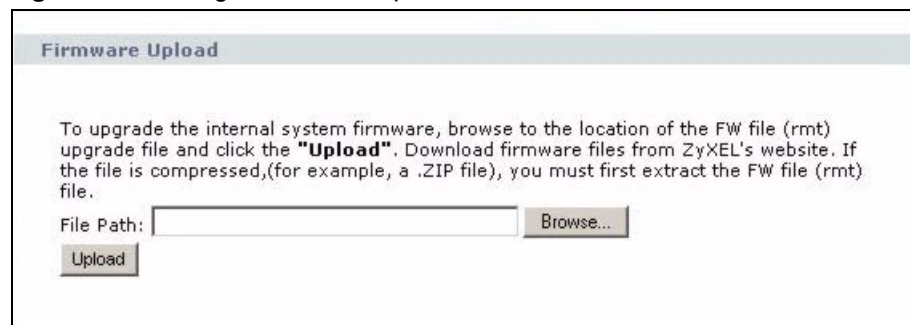
**Figure 67** Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your device. Refer to the section on resetting the device for more information on the **RESET** button.

## 7.5 F/W Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a .rmt extension, for example, "zyxel.rmt". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Management > F/W Upload** to display the screen as shown. Follow the instructions in this screen to upload firmware to your device.

**Figure 68** Management: F/W Upload

The following table describes the labels in this screen.

**Table 27** Management: F/W Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .rmt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

**Note:** Do not turn off the device while firmware upload is in progress!

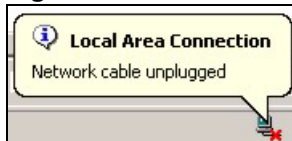
The following screen appears. Wait two minutes before logging into the device again.

**Figure 69** Firmware Upgrading Screen



The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 70** Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following status message displays at the bottom of the screen.

**Figure 71** Firmware Upload Error



# CHAPTER 8

## Troubleshooting

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

### 8.1 Problems Starting Up the G-570U

**Table 28** Troubleshooting the Start-Up of Your G-570U

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adapter.	Make sure you are using the supplied power adapter and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
The G-570U reboots automatically sometimes.	The supplied power to the G-570U is too low. Check that the G-570U is receiving enough power. Make sure the power source is working properly.

### 8.2 Problems with the Password

**Table 29** Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the G-570U.	The <b>Password</b> field is case-sensitive. Make sure that you enter the correct password using the proper casing. Use the <b>RESET</b> button on the rear panel of the G-570U to restore the factory default configuration file (hold this button in for about 10 seconds or release the button when the <b>PWR/SYS</b> LED starts blinking). This will restore all of the factory defaults including the password.

## 8.3 Problems with the WLAN Interface

**Table 30** Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the G-570U from the WLAN.	Make sure the wireless adapter on the wireless station is working properly. Check that both the G-570U and your wireless station are using the same ESSID, channel and security settings.
I cannot ping any computer on the WLAN.	Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the G-570U and wireless station(s) are using the same ESSID, channel and security settings.
I have tried to set up OTIST, but cannot connect to an access point.	When OTIST is complete, the <b>A</b> and <b>G</b> LEDs flash simultaneously while the G-570U tries to connect to an AP. If the LEDs continue to flash, the G-570U has not made a connection. Make sure that OTIST is set up correctly on both the AP and the G-570U. All settings must be the same on both devices. Ensure that the AP and the G-570U are not receiving radio signal interference and are within range. Move the devices closer together and away from any sources of interference, such as microwave ovens, Bluetooth devices and other radio transmitters. Restart OTIST on both devices.

## 8.4 Problems with the Ethernet Interface

**Table 31** Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the G-570U from the LAN.	If the <b>ETHN</b> LED on the front panel is off, check the Ethernet cable connection between your G-570U and the Ethernet device connected to the <b>ETHERNET</b> port. Check for faulty Ethernet cables. Make sure your computer's Ethernet adapter is installed and working properly. Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of the G-570U, the Ethernet device and your computer are on the same subnet.
I cannot ping any computer on the LAN.	If the <b>ETHN</b> LED on the front panel is off, check the Ethernet cable connections between your G-570U and the Ethernet device. Check the Ethernet cable connections between the Ethernet device and the LAN computers. Check for faulty Ethernet cables. Make sure the LAN computer's Ethernet adapter is installed and working properly. Verify that the IP address and the subnet mask of the G-570U, the Ethernet device and the LAN computers are on the same subnet.

**Table 31** Troubleshooting the Ethernet Interface (continued)

PROBLEM	CORRECTIVE ACTION
Cannot access the web configurator.	<p>Your computer's and the G-570U's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the G-570U's IP address, then enter the new one as the URL.</p> <p>If you don't know the G-570U's IP address, type the device name of your G-570U as the URL. ZyXELXXXX is the default where "XXXX" is the last four digits of the MAC address. The MAC address is on the bottom of the device).</p> <p>If you just changed the G-570U's IP address, your computer's cache of machine names may contain an entry that maps the name of the G-570U to its previous IP address.</p> <p>In Windows, use <b>nbtstat -R</b> at the command prompt to delete all entries in your computer's cache of machine names.</p> <p>Open a new browser window.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p> <hr/> <p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click <b>Tools</b> and then <b>Internet Options</b> to open the <b>Internet Options</b> screen.</p> <p>In the <b>General</b> tab, click <b>Delete Files</b>. In the pop-up window, select the <b>Delete all offline content</b> check box and click <b>OK</b>. Click <b>OK</b> in the <b>Internet Options</b> screen to close it.</p> <p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use <b>arp -d</b> at the command prompt to delete all entries in your computer's ARP table.</p> <p>Open a new browser window.</p>

## 8.4.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

**Note:** Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

### 8.4.1.1 Internet Explorer Pop-up Blockers

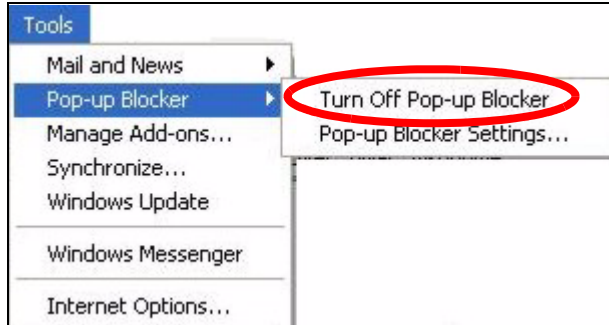
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

#### 8.4.1.1.1 Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

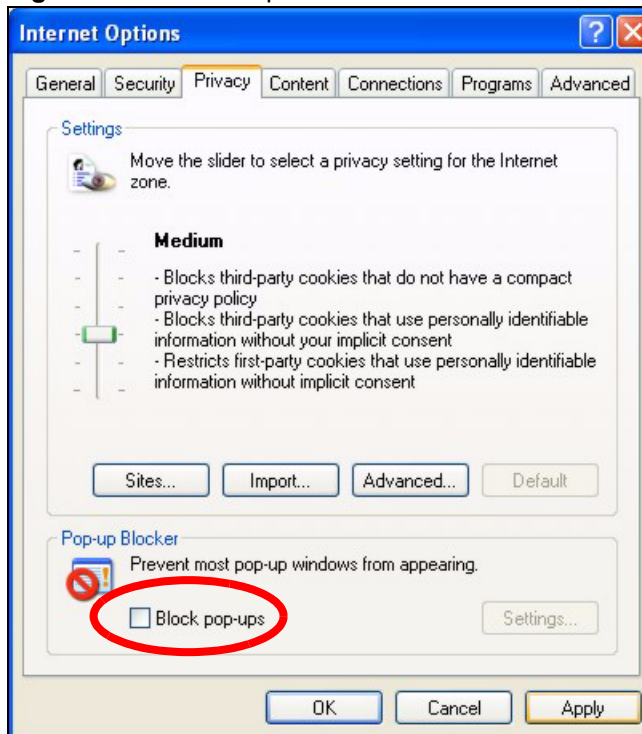
**Figure 72** Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 73** Internet Options



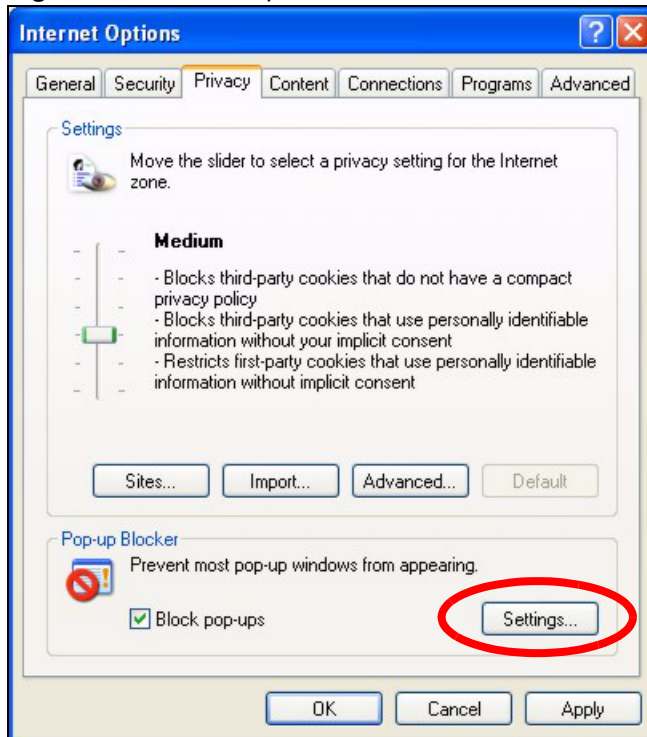
- 3 Click **Apply** to save this setting.

### 8.4.1.1.2 Enable pop-up Blockers with Exceptions

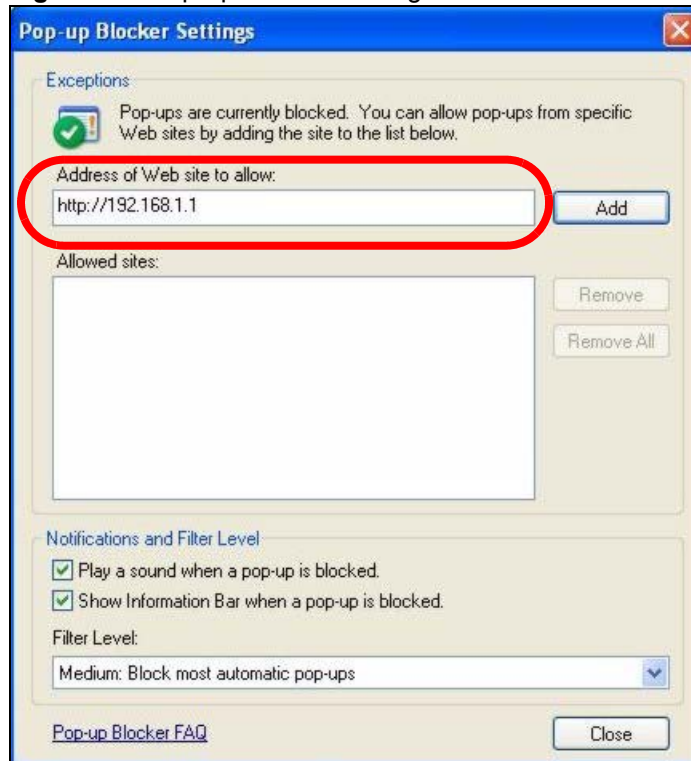
Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 74** Internet Options



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 75** Pop-up Blocker Settings

**5** Click **Close** to return to the **Privacy** screen.

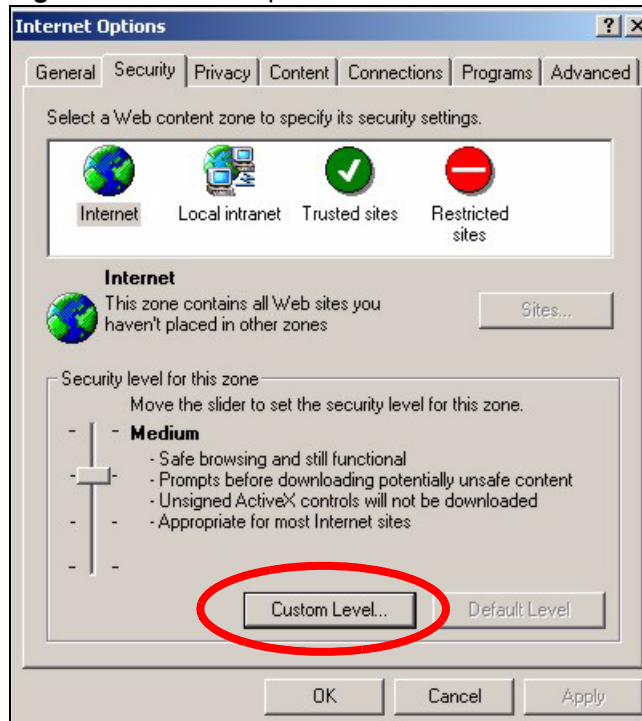
**6** Click **Apply** to save this setting.

### 8.4.1.2 JavaScripts

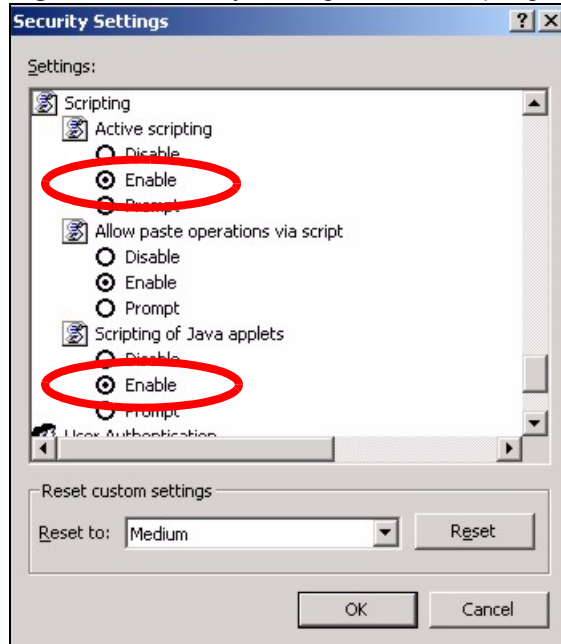
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

**1** In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.



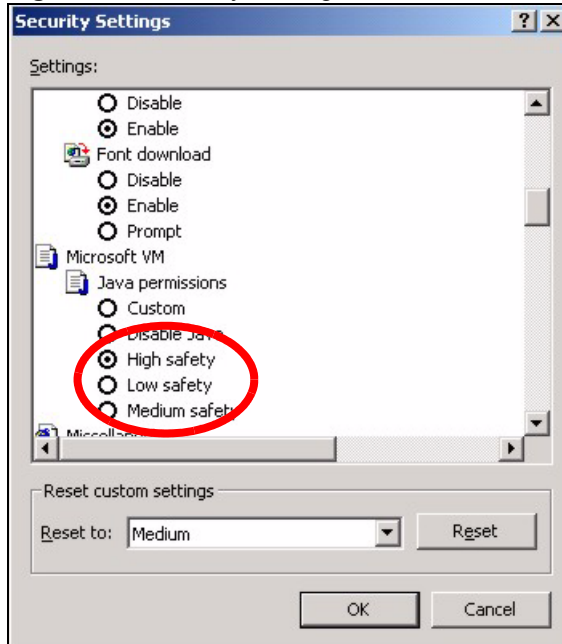
**Figure 76** Internet Options

- 2** Click the **Custom Level...** button.
- 3** Scroll down to **Scripting**.
- 4** Under **Active scripting** make sure that **Enable** is selected (the default).
- 5** Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6** Click **OK** to close the window.

**Figure 77** Security Settings - Java Scripting

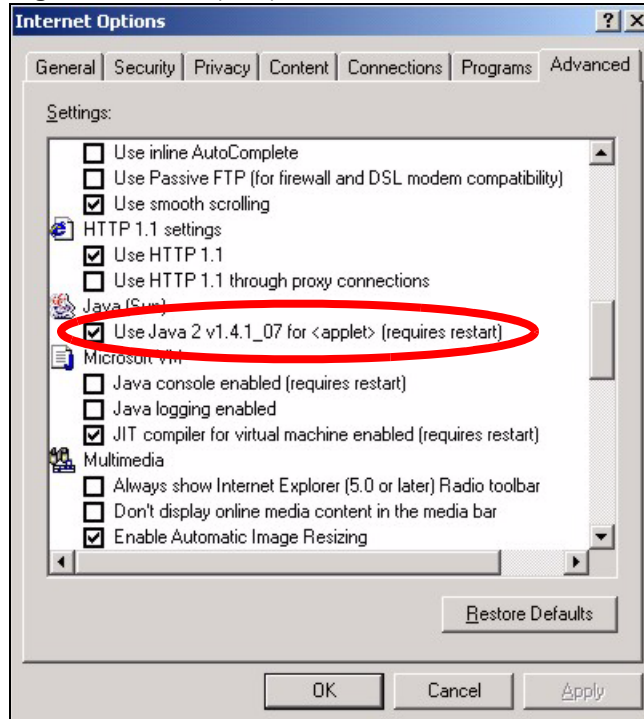
### 8.4.1.3 Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

**Figure 78** Security Settings - Java

#### 8.4.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

**Figure 79** Java (Sun)

## 8.5 Testing the Connection to the G-570U

- 1 Click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type “ping” followed by a space and the IP address of the G-570U (192.168.1.2 is the default).
- 3 Press **ENTER**. The following screen displays.

**Figure 80** Pinging the G-570U

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254
Reply from 192.168.1.2: bytes=32 time<10ms TTL=254

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2m
```

Your computer can now communicate with the G-570U via the **ETHERNET** port.

# APPENDIX A

## Product Specifications

See also the introduction chapter for a general overview of the key features.

### Specification Tables

**Table 32** Device Specifications

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Dimensions	112 mm (Wide) × 106 mm (Deep) × 28.5 mm (High)
Weight	203 g
Ethernet Port	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Antenna	1 external detachable 2dBi dual band dipole antenna with R-SMA connector
Power Requirements	12VDC @ 1 Amp maximum
Operation Temperature	0° C ~ 50° C
Storage Temperature	-30° ~ 60° C
Operation Humidity	20% ~ 95% RH
Storage Humidity	20% ~ 95% RH

**Table 33** Feature Specifications

Protocol Support	Transparent bridging for unsupported network layer protocols DHCP Client DHCP relay
Standard Compliance	IEEE 802.3 and 802.3u 10Base-T and 100Base-TX physical layer specification IEEE 802.11a specification compliance for wireless LAN IEEE 802.11b specification compliance for wireless LAN IEEE 802.11g specification compliance for wireless LAN IEEE 802.1x security standard support Wi-Fi certificate
Roaming	IEEE 802.11a compliant IEEE 802.11b compliant IEEE 802.11g compliant IEEE 802.11f partially compliant (without re-authentication)

**Table 33** Feature Specifications (continued)

Operating Modes	Access Point Client Bridge Access Point and Repeater
Wireless Links	Up to four bridge links. Two or more repeater links are supported. It is suggested that you only use up to three repeater links.
Management	Embedded Web Configurator Command-line interface Telnet support (Password-protected telnet access to internal configuration manager). FTP/Web for firmware downloading and configuration backup and restore. Limitation of client connections (# is configurable, default: unlimited) Intra BSS Block (enable/disable)
Security	WPA and IEEE 802.1x security (EAP-TLS, EAP-TTLS, LEAP, EAP-PEAP and Win XP PEAP included) 64/128-bits WEP WPA/WPA2 support based on 802.11i standard Dynamic WEP key exchange MAC address filtering through WLAN (supports up to 32 MAC address entries) AES Support
Diagnostics Capabilities	Built-in Diagnostic Tools for FLASH memory, RAM, Ethernet port and wireless port. Syslog Error log Trace Log Packet Log
Hardware Features	Restore Factory Defaults (reset) Button OTIST Button Status LEDs <ul style="list-style-type: none"> <li>• PWR</li> <li>• ETHN</li> <li>• A</li> <li>• G</li> </ul>

**Table 34** Wireless RF Specifications

Data Rate	11a/11g: 54/48/36/24/18/12/9/6 Mbps auto fallback 11b: 11/5.5/2/1 Mbps auto fallback
Communication Method	Half Duplex
Transmission/Emission Type	Direct Sequence Spread Spectrum (DSSS)

**Table 34** Wireless RF Specifications

Security	Wired Equivalent Privacy (WEP) data encryption Dynamic WEP key exchange WiFi Protected Access (WPA) IEEE 802.1x
RF frequency range	2.412~2.462GHz: North America 2.412MHz~2.472 GHz: Japan 2.412-2.472 GHz: Europe ETSI 5.15 - 5.25 GHz 5.25 - 5.35 GHz 5.470 - 5.725 GHz 5.725 - 5.825/5.850 GHz
Data modulation type	OFDM/BPSK/QPSK/CCK/DQPSK/DBPSK
Peak Output Power	11a: 19.61 dBm 11b: 18.81dBm 11g: 22.64dBm
Sensitivity	11a: 54M: -68dBm 11b/g: 54M: -70dBm 11M: -85dBm
Coverage	11a: Indoor: Up to 80 meters, Outdoor: Up to 250 meters; 11g: Indoor: up to 100 meters, Outdoor: up to 300 meters
Antenna	1 external detachable 2dBi dipole antenna with R-SMA connector

## Approvals

**Table 35** Approvals

<b>SAFETY</b>	North America	ANSI/UL-1950 3rd CSA C22.2 No. 950 3rd
	European Union (CE mark)	EN60950 (1992+A1+A2+A3+A4+A11) IEC 60950 3rd EN 50371 (MPE)
<b>EMI</b>	North America	FCC Part 15 Class B
	European Union (CE mark)	EN55022 Class B EN61000-3-2 EN61000-3-3
<b>EMS</b>	European Union (CE mark)	

**Table 35** Approvals (continued)

<b>ELECTROSTATIC DISCHARGE</b>		EN61000-4-2
<b>RADIO-FREQUENCY ELECTROMAGNETIC FIELD</b>		EN61000-4-3
<b>EFT/BURST</b>		EN61000-4-4
<b>SURGE</b>		EN61000-4-5
<b>CONDUCTED SUSCEPTIBILITY</b>		EN61000-4-6
<b>POWER MAGNETIC</b>		EN61000-4-8
<b>VOLTAGE DIPS/ INTERRUPTION</b>		EN61000-4-11
<b>EM FIELD FROM DIGITAL TELEPHONES</b>		ENV50204
<b>LAN COMPATIBILITY</b>		SmartBit
<b>FOR WIRELESS PC CARD</b>		FCC Part15C, Sec15.247
		ETS300 328 ETS300 826
		CE mark

## Power Adapter Specifications

**Table 36** Power Adapter Specifications

<b>AUSTRALIAN PLUG STANDARDS</b>	
AC Power Adapter Model	AD-121AE
Input Power	240 Volts AC 50Hz
Output Power	12 Volts DC $\pm 5\%$ 1 Amp
Power Consumption	12 Watts
Safety Standards	C-Tick
<b>EUROPEAN PLUG STANDARDS</b>	
AC Power Adapter Model	AD-121AB
Input Power	230 Volts AC 50Hz
Output Power	12 Volts DC $\pm 5\%$ , 1 Amp
Power Consumption	12 Watts
Safety Standards	CE mark, EN60950 (2001)
<b>NORTH AMERICAN PLUG STANDARDS</b>	



**Table 36** Power Adapter Specifications (continued)

AC Power Adapter Model	AD-121A
Input Power	120 Volts AC 60Hz
Output Power	12 Volts DC $\pm 5\%$ , 1 Amp
Power Consumption	12 Watts
Safety Standards	UL
<b>UK PLUG STANDARDS</b>	
AC Power Adapter Model	AD-121AD
Input Power	240 Volts AC 50Hz
Output Power	12 Volts DC $\pm 5\%$ 1 Amp
Power Consumption	12 Watts
Safety Standards	CE mark, EN60950 (2001)



# APPENDIX B

## 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.

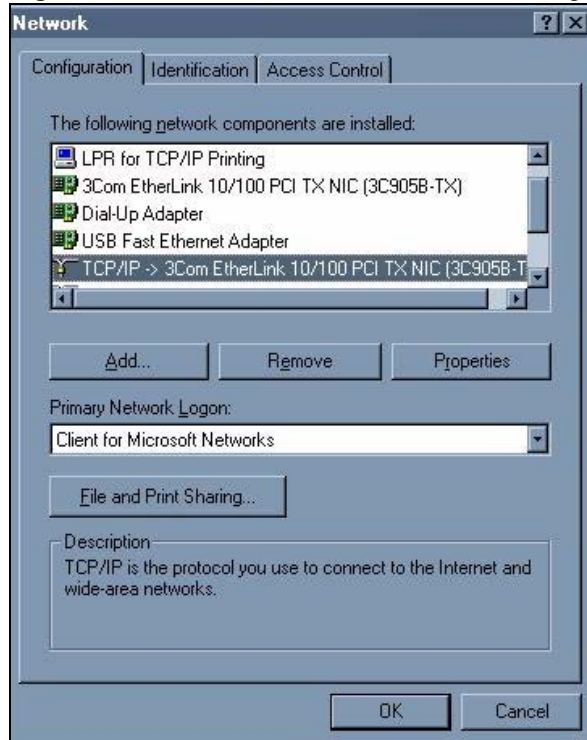
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the G-570U's LAN port.

### Windows 95/98/Me

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

**Figure 81** 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:

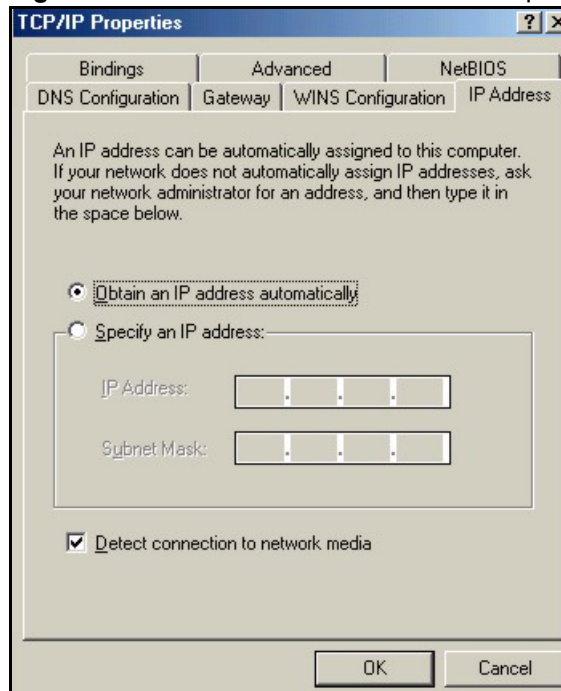
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

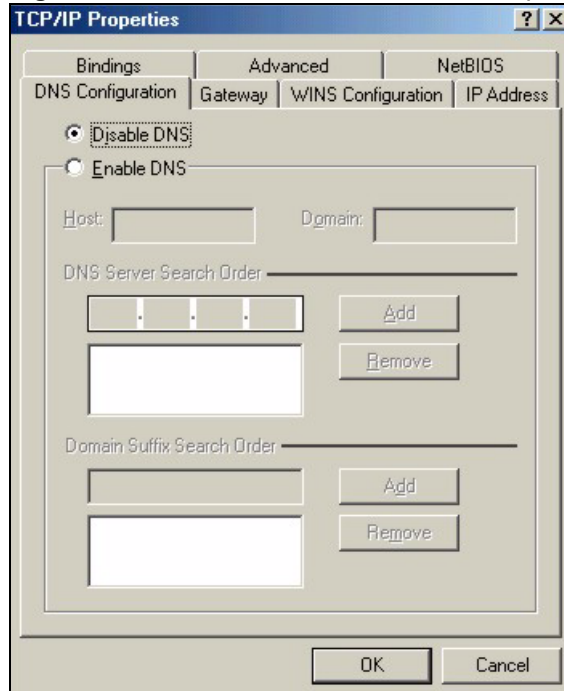
## Configuring

- 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 82** 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 83** 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** Turn on your G-570U and restart your computer when prompted.

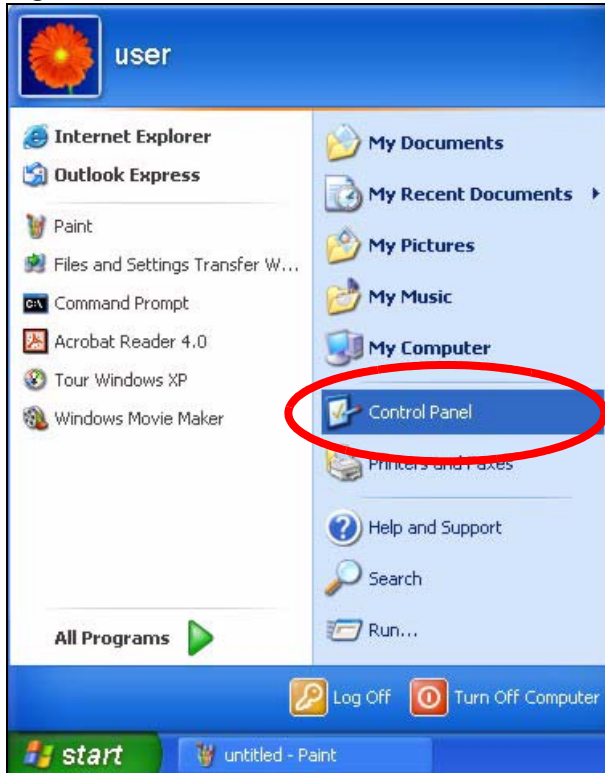
## Verifying Settings

**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.

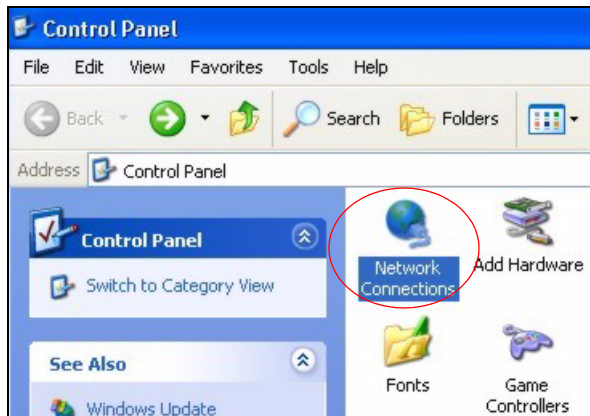
## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

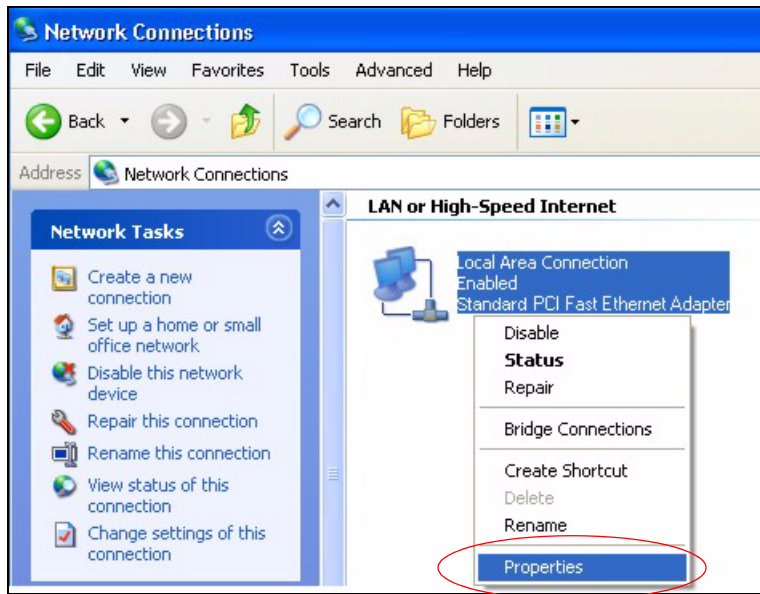
**1** Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 84** Windows XP: Start Menu

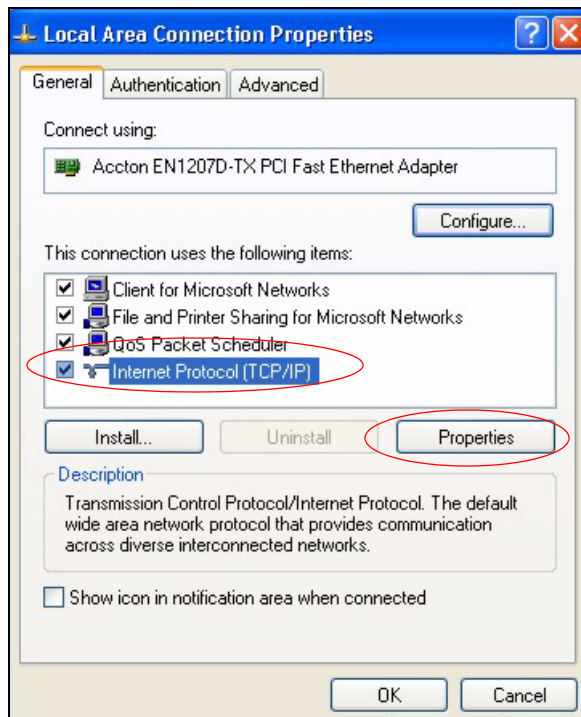
- 2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 85** Windows XP: Control Panel

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

**Figure 86** Windows XP: Control Panel: Network Connections: Properties

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

**Figure 87** Windows XP: Local Area Connection Properties

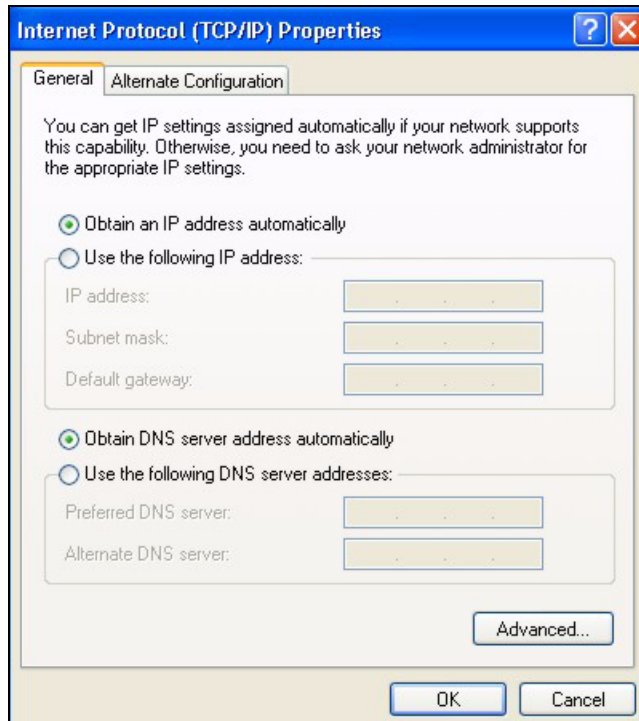
- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- 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**.

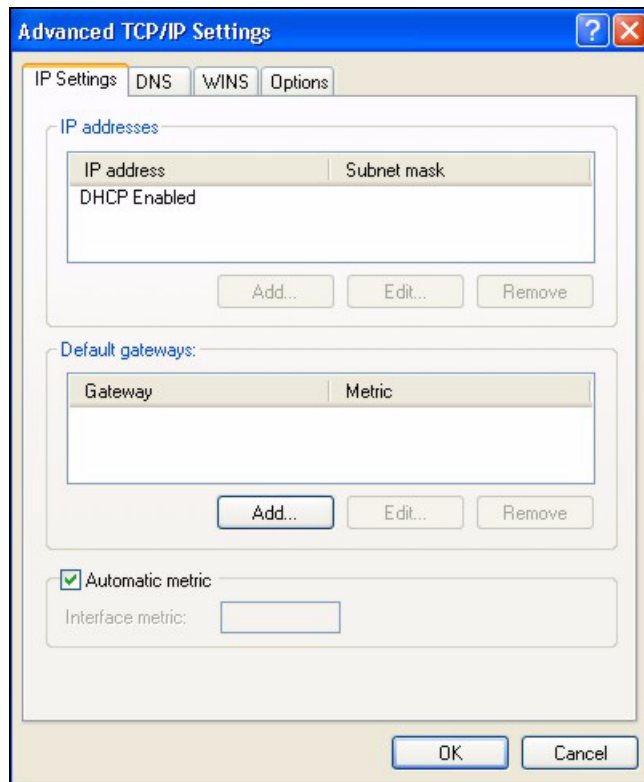
**Figure 88** Windows XP: Internet Protocol (TCP/IP) Properties



- 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:

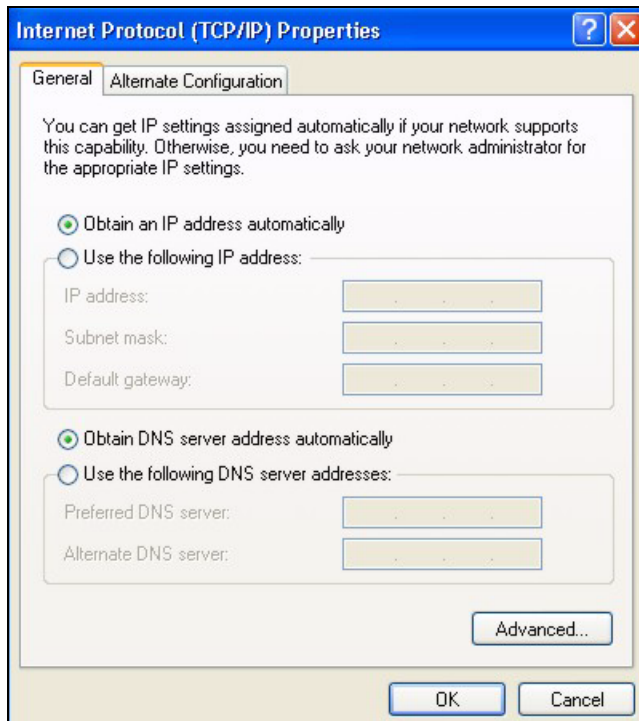
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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.

**Figure 89** Windows XP: Advanced TCP/IP Properties

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

- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Turn on your G-570U and restart your computer (if prompted).

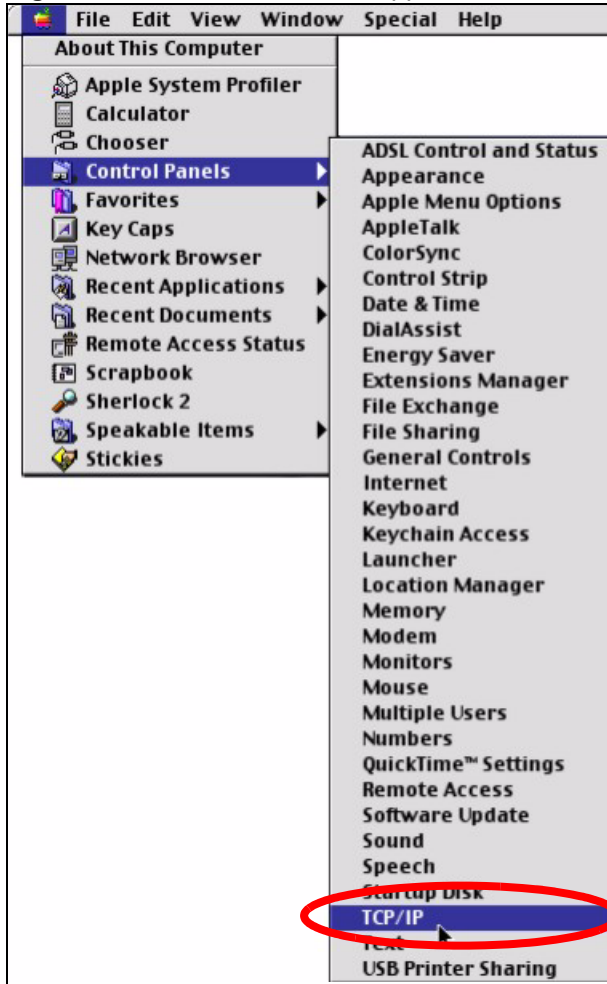
## Verifying Settings

- 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

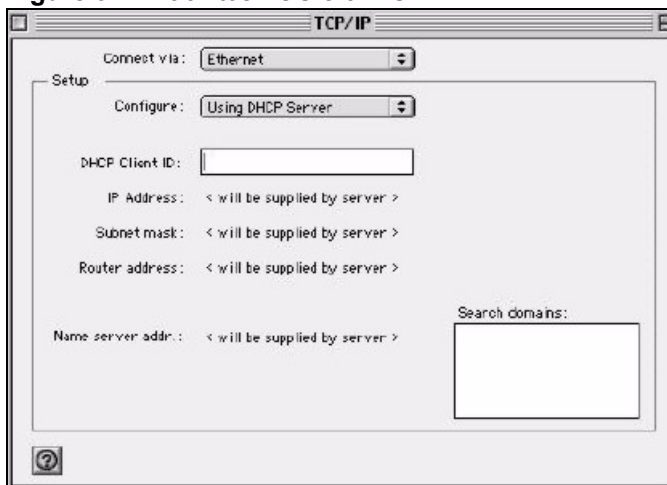
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 91** Macintosh OS 8/9: Apple Menu



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

**Figure 92** 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 G-570U in the **Router address** box.

**5** Close the **TCP/IP Control Panel**.

**6** Click **Save** if prompted, to save changes to your configuration.

**7** Turn on your G-570U and restart your computer (if prompted).

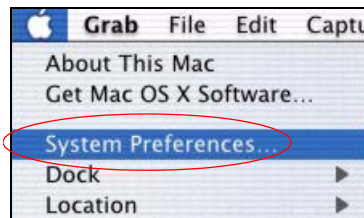
## Verifying Settings

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.

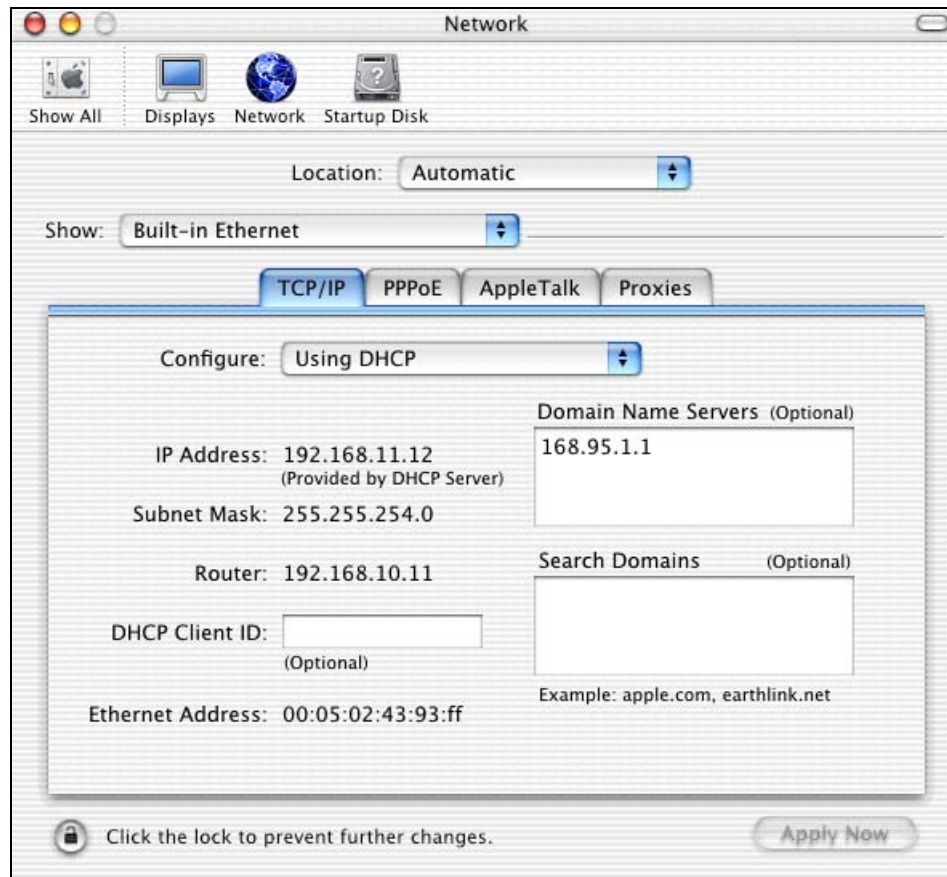
**Figure 93** Macintosh OS X: Apple Menu



**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 94** 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 G-570U in the **Router address** box.

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

**6** Turn on your G-570U and restart your computer (if prompted).

## Verifying Settings

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

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

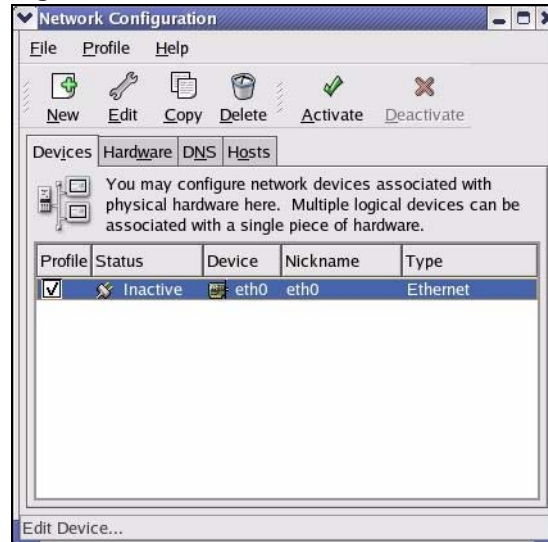
**Note:** Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 95** Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 96** Red Hat 9.0: KDE: Ethernet Device: General

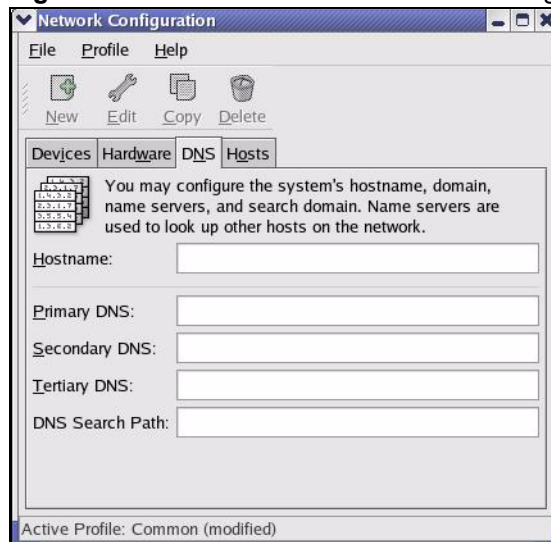


- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.

- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
- 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 97** Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

**Figure 98** Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.



- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 99** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 100** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 101** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 102** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:           [OK]
Setting network parameters:                 [OK]
Bringing up loopback interface:             [OK]
Bringing up interface eth0:                 [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 103** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# APPENDIX C

## Wireless LANs

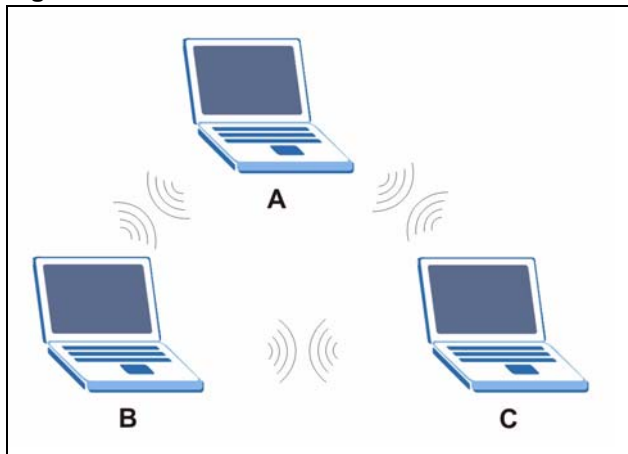
### Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

#### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

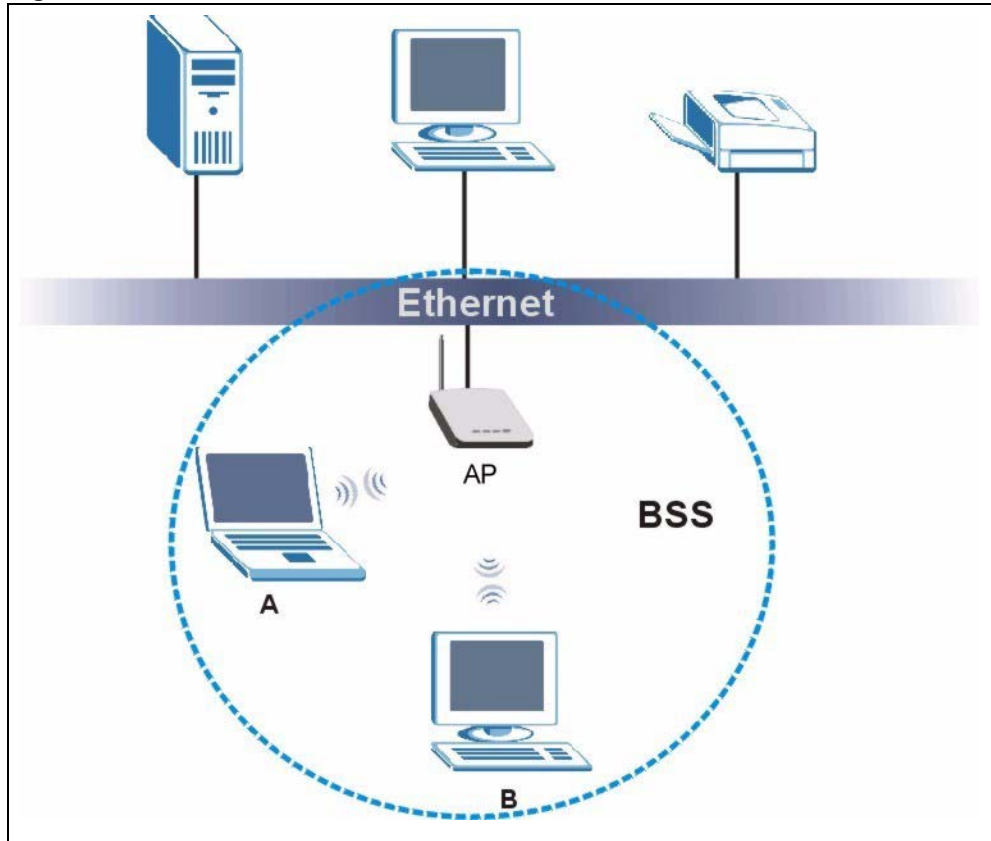
**Figure 104** Peer-to-Peer Communication in an Ad-hoc Network



#### BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

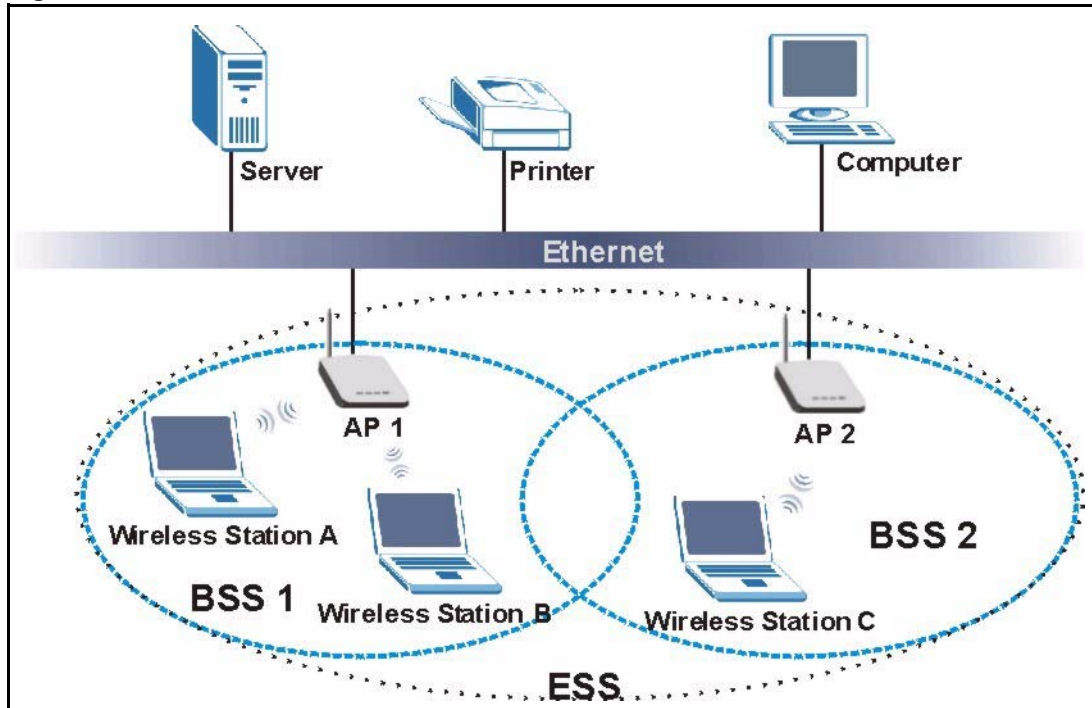
**Figure 105** Basic Service Set

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

**Figure 106** Infrastructure WLAN

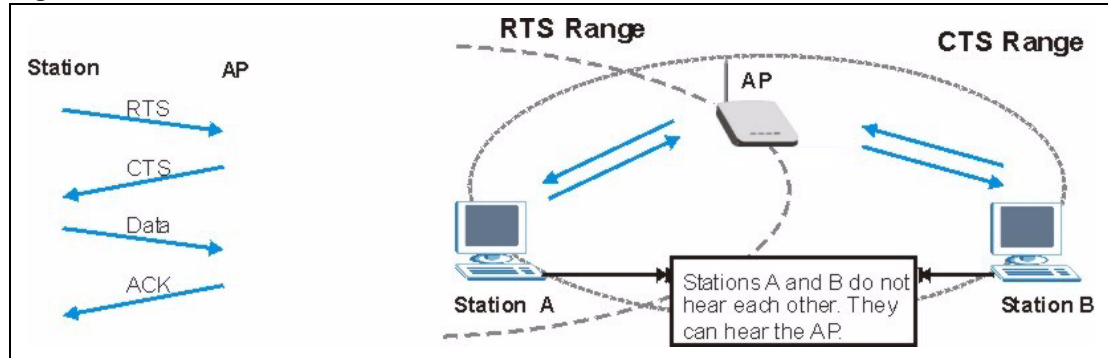
## Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

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

## RTS/CTS

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

**Figure 107** RTS/CTS

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

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

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

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

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

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

**Note:** Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

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

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

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

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 37** IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## IEEE 802.1x

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

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

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- **Authentication**  
Determines the identity of the users.
- **Authorization**  
Determines the network services available to authenticated users once they are connected to the network.
- **Accounting**  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

## **Types of RADIUS Messages**

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**  
Sent by an access point requesting authentication.
- **Access-Reject**  
Sent by a RADIUS server rejecting access.
- **Access-Accept**  
Sent by a RADIUS server allowing access.
- **Access-Challenge**  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**  
Sent by the access point requesting accounting.
- **Accounting-Response**  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.



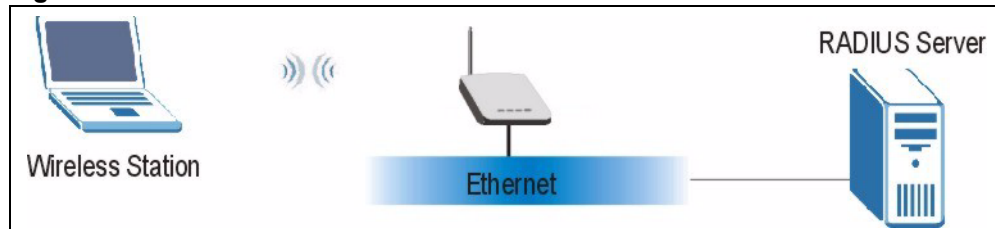
## EAP Authentication

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

The type of authentication you use depends on the RADIUS server or the AP.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

**Figure 108** EAP Authentication



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

- 1 The wireless station sends a “start” message to the device.
- 2 The device sends a “request identity” message to the wireless station for identity information.
- 3 The wireless station replies with identity information, including username and password.
- 4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

## Types of Authentication

This section discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### EAP-MD5 (Message-Digest Algorithm 5)

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

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

## **EAP-TLS (Transport Layer Security)**

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

## **EAP-TTLS (Tunneled Transport Layer Service)**

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

## **PEAP (Protected EAP)**

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

## **LEAP**

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

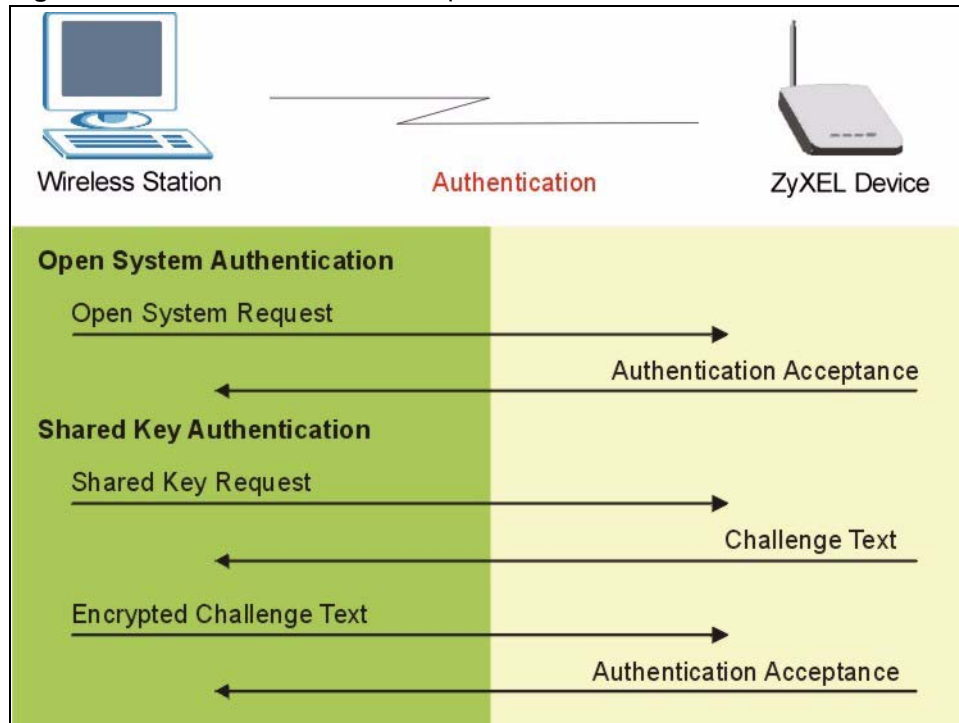
## **WEP Encryption**

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

## WEP Authentication Steps

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

**Figure 109** WEP Authentication Steps



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

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

When your device authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

## 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 38** 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(2)

### User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

### Encryption

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

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

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the 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.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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

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

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

## Roaming

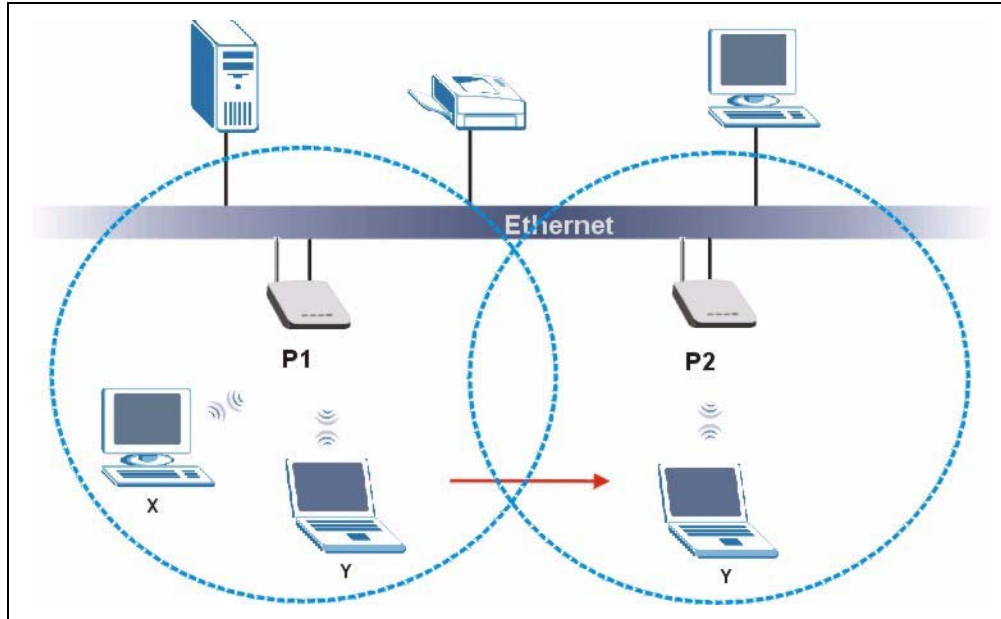
A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in [Figure 110](#).

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

**Figure 110** Roaming Example



The steps below describe the roaming process.

- 1 As wireless station **Y** moves from the coverage area of access point **P1** to that of access point
- 2 **P2**, it scans and uses the signal of access point **P2**.
- 3 Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.
- 4 Access point **P1** updates the new position of wireless station.
- 5 Wireless station **Y** sends a request to access point **P2** for re-authentication.

## Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

- 1 All the access points must be on the same subnet and configured with the same ESSID.
- 2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
- 3 The adjacent access points should use different radio channels when their coverage areas overlap.
- 4 All access points must use the same port number to relay roaming information.

- 5** The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.





# APPENDIX D

## IP Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

### Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

### IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

The following table shows the network number and host ID arrangement for classes A, B and C.

**Table 39** Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	<b>Network number</b>	Host ID	Host ID	Host ID
Class B	<b>Network number</b>	<b>Network number</b>	Host ID	Host ID
Class C	<b>Network number</b>	<b>Network number</b>	<b>Network number</b>	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have  $2^8 - 2$ , or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have  $2^{16} - 2$ , or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have  $2^{24} - 2$  hosts, or approximately 16 million hosts.

## IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

**Table 40** Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239
Class E (reserved)	11110000 to 11111111	240 to 255

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation).

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The “natural” masks for class A, B and C IP addresses are as follows.

**Table 41** “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits.

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

**Table 42** Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

**Table 42** Alternative Subnet Mask Notation (continued)

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

## Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

**Table 43** Two Subnets Example

IP/SUBNET MASK	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C").

To make two networks, divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

**Note:** In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to make network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

**Table 44** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>

**Table 44** Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 45** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is  $2^7 - 2$  or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (all zeroes is the subnet itself, all ones is the broadcast address on the subnet).

**Table 46** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

**Table 46** Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 47** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 48** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 49** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example Eight Subnets

Similarly use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows class C IP address last octet values for each subnet.

**Table 50** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class “C” subnet planning.

**Table 51** Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

## Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see [Table 39 on page 146](#)) available for subnetting.

The following table is a summary for class “B” subnet planning.

**Table 52** Class B Subnet Planning

<b>NO. “BORROWED” HOST BITS</b>	<b>SUBNET MASK</b>	<b>NO. SUBNETS</b>	<b>NO. HOSTS PER SUBNET</b>
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1



# Appendix E

## Open Software Announcements

### Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This product include eCos redboot under eCose License (GPL-compatible).

### eCos LICENSE Overview

As of May 2002, eCos is released under a modified version of the well known GNU General Public License (GPL). The eCos license is officially recognised as a GPL-compatible Free Software License. An exception clause has been added which limits the circumstances in which the license applies to other code when used in conjunction with eCos. The exception clause is as follows:

As a special exception, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other works to produce a work based on this file, this file does not by itself cause the resulting work to be covered by the GNU General Public License. However the source code for this file must still be made available in accordance with section (3) of the GNU General Public License.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

The goal of the license is to serve the eCos user community as a whole. It allows all eCos users to develop products without paying anybody anything, no matter how many developers are working on the product or how many units will be shipped. The license also guarantees that the eCos source code will always be freely available. This applies not only to the core eCos code itself but also to any changes that anybody makes to the core. In particular, it should prevent any company or individual contributing code to the system and then later claiming that all eCos users are now guilty of copyright or patent infringements and have to pay royalties. It should also prevent any company from making some small improvements, calling the result a completely new system, and releasing this under a new and less generous license.

The license does not require users to release the source code of any applications that are developed with eCos. However, if anybody makes any changes to code covered by the eCos license, or writes new files derived in any way from eCos code, then we believe that the entire user community should have the opportunity to benefit from this. The license stipulates that these changes must be made available in source code form to all recipients of binaries based

on the modified code, either by including the sources along with the binaries you deliver (or with any device containing such binaries) or with a written offer to supply the source code to the general public for three years. It is perhaps most practical for eCos developers to make the source code available online and inform those who are receiving binaries containing eCos code, and probably also the eCos maintainers, about the location of the code. See the full text of the GPL for the most authoritative definition of the obligations.

Although it is not strictly necessary to contribute the modified code back to the eCos open source project, we are always pleased to receive code contributions and hope that developers will also be keen to give back in return for what they received from the eCos project completely free of charge. The eCos maintainers are responsible for deciding whether such contributions should be applied to the public repository. In addition, a copyright assignment is required for any significant changes to the core eCos packages.

The result is a royalty-free system with minimal obligations on the part of application developers. This has resulted in the rapid uptake of eCos. At the same time, eCos is fully open source with all the benefits that implies in terms of quality and innovation. We believe that this is a winning combination.

This product include glibc, busybox and linux under GPL License.

## **GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c)

Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies

the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS. All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

NOTE: Some components of the "ZyXEL G-570U "software incorporate source code covered under the eCos License and GPL License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: [support@zyxel.com.tw](mailto:support@zyxel.com.tw)

# Index

## A

Access Point  
  see AP  
Address Assignment [53](#)  
Ad-hoc [57](#)  
Advanced Encryption Standard  
  see AES  
AES [140](#)  
Alternative subnet mask notation [147](#)  
Antenna [111](#)  
antenna [30](#)  
AP [23](#), [26](#), [133](#)  
AP + Repeater mode [28](#)  
Applications [26](#)  
Approvals [111](#)  
Association [26](#)  
Association List [52](#)  
Authentication [25](#), [72](#), [139](#)  
Auto MDI/MDI-X [109](#)  
Auto-crossover [24](#)  
Auto-negotiating [24](#), [109](#)

## B

Basic Service Set  
  see BSS  
Bridge [23](#), [27](#)  
BSS [57](#), [131](#)

## C

CA [138](#)  
CD [21](#)  
Certificate Authority  
  see CA  
Certifications [4](#)  
  Notices [5](#)  
  Viewing [5](#)  
Channel [59](#), [133](#)  
  Interference [133](#)

Channel ID [62](#), [67](#), [69](#)  
Clear to Send  
  see CTS  
Client Connections [26](#)  
Connection  
  Clients [26](#)  
  Testing [108](#)  
Contact information [9](#)  
Copyright [3](#)  
Coverage [111](#)  
Crossover [24](#)  
CTS [134](#)  
Customer support [9](#)

## D

Data Encryption [25](#), [72](#)  
Data Modulation [111](#)  
Data Rate [110](#)  
Data Transfer Speed [24](#)  
Default IP Address [109](#)  
Default Password [109](#)  
Default Subnet Mask [109](#)  
Defaults [24](#), [35](#)  
Depth [109](#)  
Device Specifications [109](#)  
DHCP Client [109](#)  
Diagnostic Tools [110](#)  
Diagnostics [110](#)  
Dimensions [109](#)  
Direct Sequence Spread Spectrum  
  see DSSS  
Disclaimer [3](#)  
Disk [21](#)  
Distribution System [58](#)  
  see DS  
DS [23](#)  
DSSS [110](#)  
Duplex [24](#), [110](#)  
Dynamic WEP Key Exchange [75](#), [140](#)

## E

EAP [25](#), [71](#), [75](#), [77](#)  
  Authentication [137](#)  
Encryption [25](#), [76](#), [140](#)  
ESS [58](#), [132](#)  
ESSID [58](#)  
Ethernet [24](#), [30](#), [31](#)  
  Cables [24](#)  
  Ports [109](#)  
European Plug Standards [112](#)  
Extended Service Set  
  see ESS  
Extended Service Set Identification  
  see ESSID  
Extensible Authentication Protocol  
  see EAP

## F

Fast Ethernet [24](#)  
FCC interference statement [4](#)  
Feature Specifications [109](#)  
Features [23](#)  
Fragmentation Threshold [61](#), [134](#)  
Frequency Range [111](#)

## H

Half-Duplex [24](#)  
Hardware [110](#)  
Height [109](#)  
Hidden node [133](#)  
Humidity [109](#)

## I

IBSS [57](#), [131](#)  
IEEE 802.11g [24](#), [135](#)  
IEEE 802.11i [25](#)  
IEEE 802.1x [23](#), [25](#)  
Incoming Transmission Speed [24](#)  
Independent Basic Service Set  
  see IBSS  
Initialization Vector

  see IV  
Internet Access [26](#)  
IP Address [31](#), [53](#)  
IP Address, Default [109](#)  
IV [141](#)

## J

Java Permissions [101](#)  
JavaScripts [101](#)

## K

Key Exchange [75](#), [140](#)

## L

LEDs [29](#)  
Lights [29](#)  
Logs [25](#)

## M

MAC [72](#)  
MAC Filter [25](#), [72](#)  
Management [25](#), [31](#), [37](#), [110](#)  
MDI/MDI-X [109](#)  
Media Access Control  
  see MAC  
Message Integrity Check  
  see MIC  
MIC [140](#)  
Modulation [111](#)

## N

Navigation Panel [46](#)  
Network Access [26](#)  
Network Card [31](#)  
Network Expansion [23](#)  
Network Management [25](#)



North American Plug Standards [112](#)

## O

One-Touch Intelligent Security Technology  
see OTIST

Open System [73](#)

Operating Modes [110](#)

Operation Humidity [109](#)

Operation Temperature [109](#)

OTIST [24, 30](#)

Output Power [111](#)

## P

Packet Tracing [25](#)

Pairwise Master Key  
see PMK

Password [24, 109](#)

Ping [108](#)

Plug Standards [112](#)

PMK [141](#)

Pop-up Windows [101](#)

Ports, Ethernet [109](#)

Power [111](#)

power [30](#)

Power Adapter Specifications [112](#)

Private IP Address [53](#)

product registration [8](#)

Protocol Support [109](#)

## R

Radio Specifications [110](#)

RADIUS [25, 135](#)

Message Types [136](#)

Messages [136](#)

Shared Secret Key [136](#)

Read Me First [21](#)

registration

product [8](#)

Related Documentation [21](#)

Remote Authentication Dial-In User Service  
see RADIUS

Repeater [23, 27](#)

Request To Send  
see RTS

Reset [24, 30, 35](#)

Restart [30, 35](#)

Restore Defaults [24](#)

RF [110, 111](#)

RJ-45 [109](#)

Roaming [109, 141](#)

Example [142](#)

Requirements [142](#)

RTS [134](#)

RTS Threshold [60, 133, 134](#)

RTS/CTS [60](#)

## S

Safety Warnings [6](#)

Secure Sockets Layer  
see SSL

Security [110](#)

Security Parameters [78](#)

Security Settings [24](#)

Sensitivity [111](#)

Service Set Identity  
see SSID

Setup [38](#)

Shared Key [73](#)

Signal Strength [52](#)

Specifications [109](#)

SSID [24, 59](#)

SSL

Passthrough [25](#)

Standards [109](#)

Statistics [50](#)

Status [49](#)

Storage Humidity [109](#)

Storage Temperature [109](#)

Subnet [31, 145](#)

Subnet Mask [31, 53](#)

Subnet mask [147](#)

Subnet Mask, Default [109](#)

subnetting [147](#)

Supporting Disk [21](#)

Syntax Conventions [21](#)

System Status [49](#)

## T

TCP/IP [31](#)  
Temperature [109](#)  
Temporal Key Integrity Protocol  
  see TKIP  
Testing [108](#)  
TKIP [140](#)  
Tools, Diagnostic [110](#)  
Tracing [25](#)  
Trademarks [3](#)  
Troubleshooting [99](#)  
  Ethernet Interface [100](#)  
  Password [99](#)  
  Startup [99](#)  
  WLAN [100](#)

Wireless Specifications [110](#)  
Wizard [38](#)  
WLAN [133](#)  
  Interference [133](#)  
WPA [23, 25, 76](#)  
WPA with RADIUS Application [77](#)  
WPA2 [25, 76](#)  
  MAC Filter [23](#)  
WPA-PSK [76](#)  
  Application [77](#)

## U

UK Plug Standards [113](#)  
User Authentication [25, 77, 140](#)

## W

Warranty [8](#)  
  Note [8](#)  
WDS [23, 65](#)  
Web Configurator [31](#)  
  Access [37](#)  
  overview [37](#)  
Weight [109](#)  
WEP [23, 25, 72, 75, 140](#)  
WEP encryption [138](#)  
Width [109](#)  
Wi-Fi Protected Access  
  see WPA  
Wired Equivalent Privacy  
  see WEP  
Wireless Access [34](#)  
Wireless Access Point  
  see AP  
Wireless Association List [26](#)  
Wireless Client [27](#)  
Wireless Distribution System  
  see WDS  
Wireless LAN  
  see WLAN  
Wireless Security [111](#)