

G-3000H

802.11g Wireless Access Point

User's Guide

Version 3.50
11/2005

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 effect.

Copyright

Copyright © 2005 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.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

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.



Certifications

Go to www.zyxel.com

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

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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

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

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization 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.

Safety Warnings

- 1** To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
- 2** Do not use this product near water, for example, in a wet basement or near a swimming pool.
- 3** Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

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

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 ^A	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	
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	
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		

METHOD	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48-22-5286603	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
		+48-22-5206701		
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 Alejandro Villegas 33 1º, 28043 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	

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

Table of Contents

Copyright	2
Federal Communications Commission (FCC) Interference Statement	3
ZyXEL Limited Warranty	5
Customer Support	6
Table of Contents	9
List of Figures	17
List of Tables	23
Preface	27
Chapter 1	
Getting to Know Your ZyAIR	31
1.1 Introducing the ZyAIR	31
1.2 ZyAIR Features	31
1.2.1 Physical Features	31
1.2.2 Firmware Features	32
1.3 Applications for the ZyAIR	36
1.3.1 Access Point	37
1.3.2 Multiple ESS	37
1.3.3 AP + Bridge	38
1.3.4 Bridge / Repeater	39
Chapter 2	
Introducing the Web Configurator	41
2.1 Accessing the ZyAIR Web Configurator	41
2.2 Resetting the ZyAIR	43
2.2.1 Procedure To Use The Reset Button	43
2.2.2 Method of Restoring Factory-Defaults	43
2.3 Navigating the ZyAIR Web Configurator	43
Chapter 3	
Wizard Setup	45
3.1 Wizard Setup Overview	45
3.1.1 Channel	45
3.1.2 ESS ID	45

3.1.3 WEP Encryption	45
3.2 Wizard Setup: General Setup	46
3.3 Wizard Setup: Wireless LAN	46
3.4 Wizard Setup: IP Address	48
3.4.1 IP Address Assignment	48
3.4.2 IP Address and Subnet Mask	48
3.5 Basic Setup Complete	50
Chapter 4	
System Screens	51
4.1 System Overview	51
4.2 Configuring General Setup	51
4.3 Configuring Password	52
4.4 Configuring Time Setting	53
Chapter 5	
Wireless Configuration	57
5.1 Wireless LAN Overview	57
5.1.1 BSS	57
5.1.2 ESS	58
5.2 Wireless LAN Basics	59
5.3 WMM QoS	60
5.3.1 WMM QoS Priorities	60
5.3.2 Type Of Service (ToS)	60
5.3.2.1 DiffServ	61
5.3.2.2 DSCP and Per-Hop Behavior	61
5.3.3 ToS (Type of Service) and WMM QoS	61
5.4 Spanning Tree Protocol (STP)	62
5.4.1 Rapid STP	62
5.4.2 STP Terminology	62
5.4.3 How STP Works	63
5.4.4 STP Port States	63
5.5 Wireless Screen Overview	63
5.6 Configuring Wireless	64
5.6.1 Access Point Mode	64
5.6.2 Bridge/Repeater Mode	66
5.6.3 AP+Bridge Mode	70
5.6.4 Multiple ESS Mode	71
Chapter 6	
Wireless Security Configuration	73
6.1 Wireless Security Overview	73
6.1.1 Encryption	73

6.1.2 Authentication	73
6.1.3 Restricted Access	73
6.1.4 Hide ZyAIR Identity	74
6.1.5 WEP Encryption	74
6.2 Configuring WEP Encryption	74
6.3 802.1x Overview	74
6.4 EAP Authentication Overview	74
6.5 Dynamic WEP Key Exchange	75
6.6 Introduction to WPA	75
6.6.1 User Authentication	76
6.6.2 Encryption	76
6.6.3 WPA(2)-PSK Application Example	76
6.7 WPA(2) with RADIUS Application Example	77
6.8 Security Modes	78
6.9 Security Modes and Wireless Client Compatibility	79
6.10 Wireless Client WPA Supplicants	79
6.11 Wireless Security Effectiveness	80
6.12 Configuring Security	80
6.12.1 Security: No Access	81
6.12.2 Security: WEP	82
6.12.3 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP	83
6.12.4 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP	85
6.12.5 Security: WPA, WPA-MIX, WPA2, WPA2-MIX	86
6.12.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX	87
6.13 Introduction to RADIUS	89
6.14 Configuring RADIUS	89
6.15 Configuring Local User Database	91

Chapter 7

Multiple ESS, SSID and VLAN 93

7.1 Wireless LAN Infrastructures	93
7.1.1 Multiple ESS	93
7.1.2 Notes on Multiple-ESS	93
7.1.3 Multiple ESS Example	94
7.1.4 Multi-ESS with VLAN Example	94
7.1.5 Configuring Multiple ESS	94
7.2 SSID	97
7.2.1 Configuring SSID	98
7.2.2 Second Rx VLAN ID	100

Chapter 8

Other Wireless Configurations 103

8.1 Layer-2 Isolation Introduction	103
--	-----

8.2 Configuring Layer-2 Isolation	104
8.2.1 Layer-2 Isolation Examples	105
8.2.2 Layer-2 Isolation Example 1	106
8.2.3 Layer-2 Isolation Example 2	106
8.2.4 Layer-2 Isolation Example 3	107
8.3 Configuring MAC Filter	108
8.4 Configuring Roaming	109
8.4.1 Requirements for Roaming	111
Chapter 9	
VLAN	113
9.1 VLAN	113
9.1.1 Management VLAN ID	113
9.1.2 VLAN Tagging	113
9.2 Configuring VLAN	113
9.2.1 Configuring Management VLAN Example	115
9.2.2 Configuring Microsoft's IAS Server Example	117
9.2.2.1 Configuring VLAN Groups	118
9.2.2.2 Configuring Remote Access Policies	119
Chapter 10	
IP Screen	127
10.1 Factory Ethernet Defaults	127
10.2 TCP/IP Parameters	127
10.2.1 IP Address and Subnet Mask	127
10.2.2 WAN IP Address Assignment	127
10.3 Configuring IP	128
Chapter 11	
Certificates	129
11.1 Certificates Overview	129
11.1.1 Advantages of Certificates	130
11.2 Self-signed Certificates	130
11.3 Configuration Summary	130
11.4 My Certificates	130
11.5 Certificate File Formats	132
11.6 Importing a Certificate	133
11.7 Creating a Certificate	134
11.8 My Certificate Details	136
11.9 Trusted CAs	139
11.10 Importing a Trusted CA's Certificate	141
11.11 Trusted CA Certificate Details	142

Chapter 12	
Remote Management Screens	147
12.1 Remote Management Overview	147
12.1.1 Remote Management Limitations	147
12.1.2 Remote Management and NAT	148
12.1.3 System Timeout	148
12.2 Configuring WWW	148
12.3 Configuring Telnet	150
12.4 Configuring TELNET	150
12.5 Configuring FTP	151
12.6 SNMP	152
12.6.1 Supported MIBs	154
12.6.2 SNMP Traps	154
12.7 SNMP Traps	155
12.7.1 Configuring SNMP	155
Chapter 13	
Log Screens.....	157
13.1 Configuring View Log	157
13.2 Configuring Log Settings	158
Chapter 14	
Maintenance	161
14.1 Maintenance Overview	161
14.2 System Status Screen	161
14.2.1 System Statistics	162
14.3 Association List	163
14.4 Channel Usage	164
14.5 F/W Upload Screen	166
14.6 Configuration Screen	168
14.6.1 Backup Configuration	168
14.6.2 Restore Configuration	169
14.6.3 Back to Factory Defaults	170
14.7 Restart Screen	170
Chapter 15	
Introducing the SMT	171
15.1 Connect to your ZyAIR Using Telnet	171
15.2 Changing the System Password	171
15.3 ZyAIR SMT Menu Overview Example	172
15.4 Navigating the SMT Interface	173
15.4.1 System Management Terminal Interface Summary	174

Chapter 16	
General Setup	177
16.1 General Setup	177
16.1.1 Procedure To Configure Menu 1	177
Chapter 17	
LAN Setup	179
17.1 LAN Setup	179
17.2 TCP/IP Ethernet Setup	179
17.3 Wireless LAN Setup	180
17.3.1 Configuring MAC Address Filter	182
17.3.2 Configuring Roaming	184
17.3.3 Configuring SSID Profiles	186
17.3.4 Configuring Bridge Link	187
17.3.5 Configuring Layer-2 Isolation	189
Chapter 18	
Dial-in User Setup	193
18.1 Dial-in User Setup	193
Chapter 19	
VLAN Setup	195
19.1 VLAN Setup	195
Chapter 20	
SNMP Configuration	197
20.1 SNMP Configuration	197
Chapter 21	
System Security	199
21.1 System Security	199
21.1.1 System Password	199
21.1.2 Configuring Security Profiles	199
Chapter 22	
System Information and Diagnosis	201
22.1 System Status	201
22.2 System Information	203
22.2.1 System Information	203
22.2.2 Console Port Speed	204
22.3 Log and Trace	204
22.3.1 Viewing Error Log	204
22.4 Diagnostic	205

Chapter 23	
Firmware and Configuration File Maintenance	207
23.1 Filename Conventions	207
23.2 Backup Configuration	208
23.2.1 Backup Configuration Using FTP	208
23.2.2 Using the FTP command from the DOS Prompt	209
23.2.3 Backup Configuration Using TFTP	210
23.2.4 Example: TFTP Command	211
23.2.5 Backup Via Console Port	211
23.3 Restore Configuration	212
23.3.1 Restore Using FTP	213
23.4 Uploading Firmware and Configuration Files	213
23.4.1 Firmware Upload	214
23.4.2 Configuration File Upload	214
23.4.3 Using the FTP command from the DOS Prompt Example	215
23.4.4 TFTP File Upload	215
23.4.5 Example: TFTP Command	216
23.4.6 Uploading Via Console Port	216
23.4.7 Uploading Firmware File Via Console Port	216
23.4.8 Example Xmodem Firmware Upload Using HyperTerminal	217
23.4.9 Uploading Configuration File Via Console Port	217
23.4.10 Example Xmodem Configuration Upload Using HyperTerminal	218
Chapter 24	
System Maintenance and Information	219
24.1 Command Interpreter Mode	219
24.1.1 CNM	220
24.1.2 Configuring Vantage CNM	220
24.1.3 Configuration Example	223
24.2 Time and Date Setting	224
24.2.1 Resetting the Time	226
24.3 Remote Management Setup	226
24.3.1 Telnet	226
24.3.2 FTP	226
24.3.3 Web	227
24.3.4 Remote Management Setup	227
24.3.5 Remote Management Limitations	229
24.4 Remote Management and NAT	229
24.5 System Timeout	229
Appendix A	
Troubleshooting	231

Appendix B Specifications	233
Appendix C Power over Ethernet (PoE) Specifications	235
Appendix D Brute-Force Password Guessing Protection	237
Appendix E Setting up Your Computer's IP Address	239
Appendix F IP Address Assignment Conflicts	251
Appendix G Wireless LANs	255
Appendix H IP Subnetting	267
Appendix I Command Interpreter	275
Appendix J Log Descriptions	277
Appendix K Indoor Installation Recommendations	281
Appendix L Power Adaptor Specifications	283
Index	285

List of Figures

Figure 1 PoE Installation Example	32
Figure 2 WDS Functionality Example	33
Figure 3 Access Point Application	37
Figure 4 Multiple ESS Application	38
Figure 5 AP+Bridge Application	39
Figure 6 Bridge Application	40
Figure 7 Repeater Application	40
Figure 8 Change Password Screen	42
Figure 9 Replace Certificate Screen	42
Figure 10 The MAIN MENU Screen of the Web Configurator	44
Figure 11 Wizard 1: General Setup	46
Figure 12 Wizard 2: Wireless LAN Setup	47
Figure 13 Wizard 3: IP Address Assignment	49
Figure 14 Wizard 4: Setup Complete	50
Figure 15 System General Setup	51
Figure 16 Password.	53
Figure 17 Time Setting	54
Figure 18 Basic Service set	58
Figure 19 Extended Service Set	59
Figure 20 DiffServ: Differentiated Service Field	61
Figure 21 Wireless: Access Point	65
Figure 22 Bridging Example	67
Figure 23 Bridge Loop: Two Bridges Connected to Hub	68
Figure 24 Bridge Loop: Bridge Connected to Wired LAN	68
Figure 25 Wireless: Bridge/Repeater	69
Figure 26 Wireless: AP+Bridge	71
Figure 27 EAP Authentication	75
Figure 28 WPA(2)-PSK Authentication	77
Figure 29 WPA(2) with RADIUS Application Example	78
Figure 30 Security	81
Figure 31 Security: No Access or None	82
Figure 32 Security: WEP	82
Figure 33 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP	84
Figure 34 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP	85
Figure 35 Security: WPA, WPA-MIX, WPA2 or WPA2-MIX	87
Figure 36 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX	88
Figure 37 RADIUS	90
Figure 38 Local User Database	91

Figure 39 Multi-ESS with VLAN Example	94
Figure 40 Wireless: Multiple ESS	95
Figure 41 SSID	97
Figure 42 Configuring SSID	99
Figure 43 Second Rx VLAN ID Example	100
Figure 44 Configuring SSID: Second Rx VLAN ID Example	100
Figure 45 Layer-2 Isolation Application	104
Figure 46 Layer-2 Isolation Configuration Screen	105
Figure 47 Layer-2 Isolation Example	106
Figure 48 Layer-2 Isolation Example 1	106
Figure 49 Layer-2 Isolation Example 2	107
Figure 50 Layer-2 Isolation Example 3	108
Figure 51 MAC Address Filter	109
Figure 52 Roaming Example	110
Figure 53 Roaming	111
Figure 54 VLAN	114
Figure 55 Management VLAN Configuration Example	115
Figure 56 VLAN-Aware Switch - Static VLAN	116
Figure 57 VLAN-Aware Switch	116
Figure 58 VLAN-Aware Switch - VLAN Status	116
Figure 59 VLAN Setup	117
Figure 60 New Global Security Group	118
Figure 61 Add Group Members	119
Figure 62 New Remote Access Policy for VLAN Group	120
Figure 63 Specifying Windows-Group Condition	120
Figure 64 Adding VLAN Group	121
Figure 65 Granting Permissions and User Profile Screens	121
Figure 66 Authentication Tab Settings	122
Figure 67 Encryption Tab Settings	122
Figure 68 Connection Attributes Screen	123
Figure 69 RADIUS Attribute Screen	124
Figure 70 802 Attribute Setting for Tunnel-Medium-Type	124
Figure 71 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID	125
Figure 72 VLAN Attribute Setting for Tunnel-Type	125
Figure 73 Completed Advanced Tab	126
Figure 74 IP Setup	128
Figure 75 My Certificates	131
Figure 76 My Certificate Import	133
Figure 77 My Certificate Create	134
Figure 78 My Certificate Details	137
Figure 79 Trusted CAs	140
Figure 80 Trusted CA Import	141
Figure 81 Trusted CA Details	143

Figure 82 Remote Management: WWW	149
Figure 83 Telnet Configuration on a TCP/IP Network	150
Figure 84 Remote Management: Telnet	151
Figure 85 Remote Management: FTP	152
Figure 86 SNMP Management Model	153
Figure 87 Remote Management: SNMP	156
Figure 88 View Log	157
Figure 89 Log Settings	159
Figure 90 System Status	161
Figure 91 System Status: Show Statistics	162
Figure 92 Association List	163
Figure 93 Channel Usage	165
Figure 94 Firmware Upload	166
Figure 95 Firmware Upload In Process	167
Figure 96 Network Temporarily Disconnected	167
Figure 97 Firmware Upload Error	168
Figure 98 Configuration	168
Figure 99 Configuration Upload Successful	169
Figure 100 Network Temporarily Disconnected	169
Figure 101 Configuration Upload Error	170
Figure 102 Reset Warning Message	170
Figure 103 Restart Screen	170
Figure 104 Login Screen	171
Figure 105 Menu 23.1 System Security: Change Password	172
Figure 106 G-3000H SMT Main Menu	174
Figure 107 Menu 1 General Setup	177
Figure 108 Menu 3 LAN Setup	179
Figure 109 Menu 3.2 TCP/IP Setup	180
Figure 110 Menu 3.5 Wireless LAN Setup	181
Figure 111 Menu 3.5 Wireless LAN Setup	183
Figure 112 Menu 3.5.1 WLAN MAC Address Filter	183
Figure 113 Menu 3.5 Wireless LAN Setup	185
Figure 114 Menu 3.5.2 Roaming Configuration	185
Figure 115 Menu 3.5 Wireless LAN Setup	186
Figure 116 Menu 3.5.6 - SSID Profile Edit	187
Figure 117 Menu 3.5 Wireless LAN Setup	188
Figure 118 Menu 3.5.4 Bridge Link Configuration	189
Figure 119 Menu 3.5 Wireless LAN Setup	190
Figure 120 Menu 3.5.5 Layer-2 Isolation	190
Figure 121 Menu 14- Dial-in User Setup	193
Figure 122 Menu 14.1- Edit Dial-in User	194
Figure 123 Menu 16 VLAN Setup	195
Figure 124 Menu 22 SNMP Configuration	197

Figure 125 Menu 23 System Security	199
Figure 126 Menu 23 - System Security	200
Figure 127 Menu 23.5 Security Profile Edit	200
Figure 128 Menu 24 System Maintenance	201
Figure 129 Menu 24.1 System Maintenance: Status	202
Figure 130 Menu 24.2 System Information and Console Port Speed	203
Figure 131 Menu 24.2.1 System Information: Information	203
Figure 132 Menu 24.2.2 System Maintenance: Change Console Port Speed	204
Figure 133 Menu 24.3 System Maintenance: Log and Trace	205
Figure 134 Sample Error and Information Messages	205
Figure 135 Menu 24.4 System Maintenance: Diagnostic	205
Figure 136 Menu 24.5 Backup Configuration	209
Figure 137 FTP Session Example	210
Figure 138 System Maintenance: Backup Configuration	212
Figure 139 System Maintenance: Starting Xmodem Download Screen	212
Figure 140 Backup Configuration Example	212
Figure 141 Successful Backup Confirmation Screen	212
Figure 142 Menu 24.6 Restore Configuration	213
Figure 143 Menu 24.7 System Maintenance: Upload Firmware	213
Figure 144 Menu 24.7.1 System Maintenance: Upload System Firmware	214
Figure 145 Menu 24.7.2 System Maintenance: Upload System Configuration File	214
Figure 146 FTP Session Example	215
Figure 147 Menu 24.7.1 as seen using the Console Port	217
Figure 148 Example Xmodem Upload	217
Figure 149 Menu 24.7.2 as seen using the Console Port	218
Figure 150 Example Xmodem Upload	218
Figure 151 Menu 24 System Maintenance	220
Figure 152 Valid CI Commands	220
Figure 153 CNM CL	221
Figure 154 CNM Configuration Example	224
Figure 155 Menu 24.10 System Maintenance: Time and Date Setting	225
Figure 156 Telnet Configuration on a TCP/IP Network	226
Figure 157 Menu 24.11 Remote Management Control	228
Figure 158 WIndows 95/98/Me: Network: Configuration	240
Figure 159 Windows 95/98/Me: TCP/IP Properties: IP Address	241
Figure 160 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	242
Figure 161 Windows XP: Start Menu	243
Figure 162 Windows XP: Control Panel	243
Figure 163 Windows XP: Control Panel: Network Connections: Properties	244
Figure 164 Windows XP: Local Area Connection Properties	244
Figure 165 Windows XP: Advanced TCP/IP Settings	245
Figure 166 Windows XP: Internet Protocol (TCP/IP) Properties	246
Figure 167 Macintosh OS 8/9: Apple Menu	247

Figure 168 Macintosh OS 8/9: TCP/IP	247
Figure 169 Macintosh OS X: Apple Menu	248
Figure 170 Macintosh OS X: Network	249
Figure 171 IP Address Conflicts: Case A	251
Figure 172 IP Address Conflicts: Case B	252
Figure 173 IP Address Conflicts: Case C	252
Figure 174 IP Address Conflicts: Case D	253
Figure 175 Peer-to-Peer Communication in an Ad-hoc Network	255
Figure 176 Basic Service Set	256
Figure 177 Infrastructure WLAN	257
Figure 178 RTS/CTS	258

List of Tables

Table 1 IEEE 802.11b	34
Table 2 IEEE 802.11g	34
Table 3 Wizard 1: General Setup	46
Table 4 Wizard 2: Wireless LAN Setup	47
Table 5 Private IP Address Ranges	48
Table 6 Wizard 3: IP Address Assignment	49
Table 7 System General Setup	51
Table 8 Password	53
Table 9 Time Setting	54
Table 10 WMM QoS Priorities	60
Table 11 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping	61
Table 12 STP Path Costs	62
Table 13 STP Port States	63
Table 14 Wireless: Access Point	65
Table 15 Wireless: Bridge/Repeater	69
Table 16 Security Modes	78
Table 17 Security Modes for ZyAIR and Windows XP Wireless Client	79
Table 18 ZyAIR Wireless Security Levels	80
Table 19 Security	81
Table 20 Security: No Access or None	82
Table 21 Security: WEP	82
Table 22 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP	84
Table 23 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP	85
Table 24 Security: WPA, WPA-MIX, WPA2 or WPA2-MIX	87
Table 25 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX	88
Table 26 RADIUS	90
Table 27 Local User Database	91
Table 28 Wireless: Multiple ESS	95
Table 29 SSID	97
Table 30 Configuring SSID	99
Table 31 Layer-2 Isolation Configuration	105
Table 32 MAC Address Filter	109
Table 33 Roaming	111
Table 34 VLAN	114
Table 35 Standard RADIUS Attributes	117
Table 36 Private IP Address Ranges	127
Table 37 IP Setup	128
Table 38 My Certificates	131

Table 39 My Certificate Import	133
Table 40 My Certificate Create	134
Table 41 My Certificate Details	137
Table 42 Trusted CAs	140
Table 43 Trusted CA Import	141
Table 44 Trusted CA Details	143
Table 45 Remote Management: WWW	149
Table 46 Remote Management: Telnet	151
Table 47 Remote Management: FTP	152
Table 48 SNMP Traps	154
Table 49 SNMP Interface Index to Physical Port Mapping	155
Table 50 Remote Management: SNMP	156
Table 51 View Log	157
Table 52 Log Settings	159
Table 53 System Status	161
Table 54 System Status: Show Statistics	162
Table 55 Association List	163
Table 56 Channel Usage	165
Table 57 Firmware Upload	166
Table 58 Restore Configuration	169
Table 59 SMT Menus Overview	172
Table 60 Main Menu Commands	173
Table 61 Main Menu Summary	174
Table 62 Menu 1 General Setup	177
Table 63 Menu 3.2 TCP/IP Setup	180
Table 64 Menu 3.5 Wireless LAN Setup	181
Table 65 Menu 3.5.1 WLAN MAC Address Filter	184
Table 66 Menu 3.5.2 Roaming Configuration	185
Table 67 Menu 3.5.6 - SSID Profile Edit	187
Table 68 Menu 3.5.4 Bridge Link Configuration	189
Table 69 Menu 3.5.5 Layer-2 Isolation	191
Table 70 Menu 14.1- Edit Dial-in User	194
Table 71 Menu 16 VLAN Setup	195
Table 72 Menu 22 SNMP Configuration	197
Table 73 Menu 24.1 System Maintenance: Status	202
Table 74 Menu 24.2.1 System Maintenance: Information	203
Table 75 Menu 24.4 System Maintenance Menu: Diagnostic	206
Table 76 Filename Conventions	208
Table 77 General Commands for Third Party FTP Clients	210
Table 78 General Commands for Third Party TFTP Clients	211
Table 79 CNM Commands	221
Table 80 System Maintenance: Time and Date Setting	225
Table 81 Remote Management Port Control	227

Table 82 Menu 24.11 Remote Management Control	228
Table 83 Troubleshooting the Start-Up of Your ZyAIR	231
Table 84 Troubleshooting the Ethernet Interface	231
Table 85 Troubleshooting the Password	232
Table 86 Troubleshooting Telnet	232
Table 87 Troubleshooting the WLAN Interface	232
Table 88 Hardware	233
Table 89 Firmware	233
Table 90 Power over Ethernet Injector Specifications	235
Table 91 Power over Ethernet Injector RJ-45 Port Pin Assignments	235
Table 92 Brute-Force Password Guessing Protection Commands	237
Table 93 IEEE 802.11b	259
Table 94 Comparison of EAP Authentication Types	263
Table 95 Wireless Security Relational Matrix	264
Table 96 Classes of IP Addresses	267
Table 97 Allowed IP Address Range By Class	268
Table 98 "Natural" Masks	268
Table 99 Alternative Subnet Mask Notation	269
Table 100 Two Subnets Example	269
Table 101 Subnet 1	270
Table 102 Subnet 2	270
Table 103 Subnet 1	271
Table 104 Subnet 2	271
Table 105 Subnet 3	271
Table 106 Subnet 4	272
Table 107 Eight Subnets	272
Table 108 Class C Subnet Planning	272
Table 109 Class B Subnet Planning	273
Table 110 System Maintenance Logs	277
Table 111 ICMP Notes	277
Table 112 Sys log	278
Table 113 Log Categories and Available Settings	279
Table 114 North American Plug Standards	283
Table 115 European Plug Standards	283
Table 116 United Kingdom Plug Standards	283
Table 117 Australia and New Zealand Plug Standards	283

Preface

Congratulations on your purchase of the G-3000H - 802.11g Wireless Access Point/Bridge/Repeater.

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

The ZyAIR can function as a wireless network bridge/repeater and establish up to five wireless links with other APs.

The ZyAIR also supports both AP and bridge connections at the same time.

Your ZyAIR is easy to install and configure.

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

About This User's Guide

This User's Guide is designed to guide you through the configuration of your ZyAIR using the web configurator or the SMT. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

Note: Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your ZyAIR. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Compact Guide
The Compact Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.











User Guide Feedback

Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The G-3000H may be referred to simply as the ZyAIR in the user’s guide.

Graphics Icons Key

ZyAIR 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Modem 	Switch 	Router 
Wireless Signal 		

CHAPTER 1

Getting to Know Your ZyAIR

This chapter introduces the main features and applications of the ZyAIR.

1.1 Introducing the ZyAIR

The G-3000H extends the range of your existing wired network without any additional wiring efforts, providing easy network access to mobile users.

The ZyAIR offers highly secured wireless connectivity to your wired network with IEEE 802.1x, Wi-Fi Protected Access, WEP data encryption and MAC address filtering.

The ZyAIR is easy to install and configure. The embedded web-based configurator enables easy operation and configuration.

1.2 ZyAIR Features

The following sections describe the features of the ZyAIR

1.2.1 Physical Features

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

This auto-negotiating feature allows the ZyAIR 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.

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

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Reset Button

The ZyAIR reset button is built into the side panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.2, subnet mask to 255.255.255.0.

ZyAIR LED

The blue ZyAIR LED (also known as the Breathing LED) is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. You may use the web configurator to turn this LED off even when the ZyAIR is on and data is being transmitted/received.

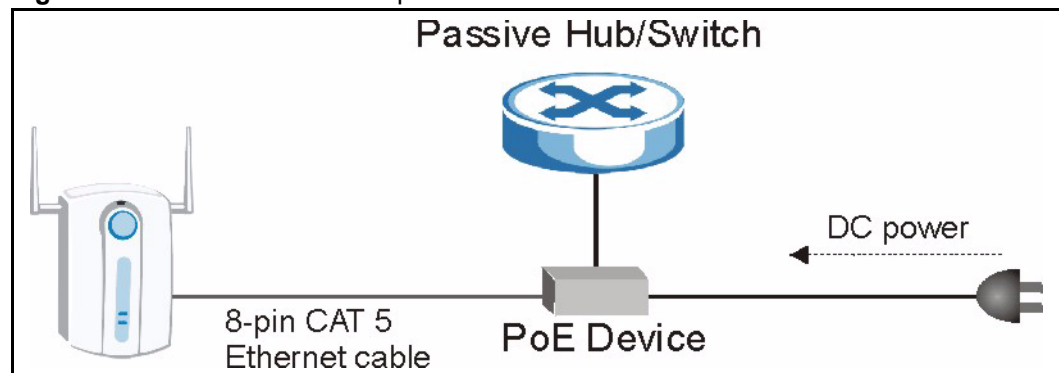
Bridge/Repeater LED

A Bridge/Repeater link LED turns steady on green when your ZyAIR acts as a bridge, establishing up to six wireless links with other APs.

Power over Ethernet (PoE)

Power over Ethernet (PoE) is the ability to provide power to your ZyAIR via an 8-pin CAT 5 Ethernet cable, eliminating the need for a nearby power source. An injector or PoE device (not included) is also needed to supply the Ethernet cable with power. This feature allows increased flexibility in the locating of your ZyAIR. You only need to connect the external power adaptor if you are not using PoE. If you simultaneously use both PoE and the external power adaptor, the ZyAIR will draw power from the PoE connection only. Refer to the appendix for more information about PoE.

Figure 1 PoE Installation Example



1.2.2 Firmware Features

Wi-Fi Protected Access

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

Layer-2 Isolation

Layer-2 isolation is used to prevent wireless clients associated with your ZyAIR from communicating with other wireless clients, AP's, computers or routers in a network.

VLAN

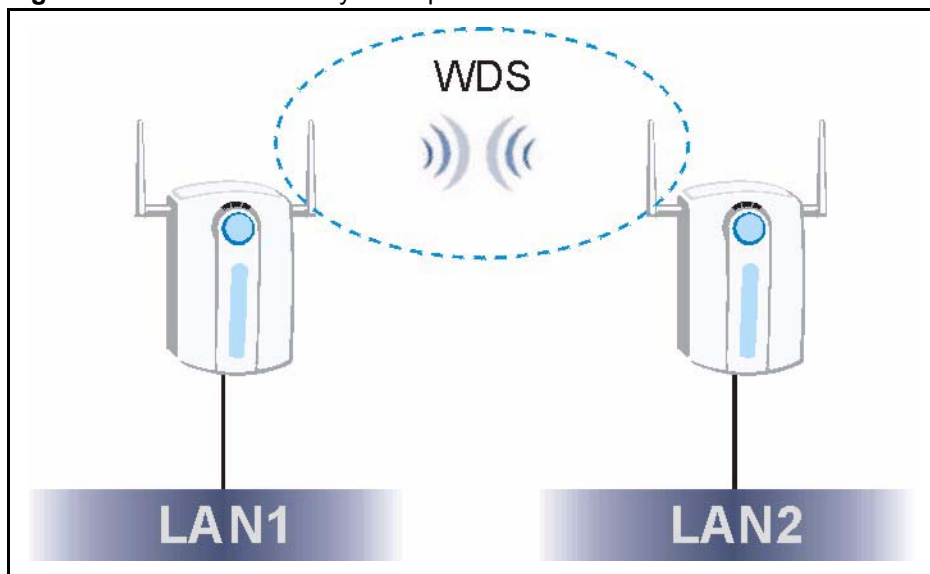
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can talk to each other. Stations on a logical network can belong to one or more groups. The ZyAIR supports 802.1Q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyAIR can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

Configure VLAN (virtual LAN) to extend the wireless logical grouping to the wired network. A ZyAIR that you configure with the built-in wireless card uses the same **Management VLAN ID** as a ZyAIR configured with a removable wireless card.

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 ZyAIR supports WDS, providing a cost-effective solution for wireless network expansion.

Figure 2 WDS Functionality Example



802.11b Wireless LAN Standard

The ZyAIR complies with the 802.11b wireless standard.

The 802.11b data rate and corresponding modulation techniques are shown in the table below. The modulation technique defines how bits are encoded onto radio waves.

Table 1 IEEE 802.11b

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shifted Keying)
2	DQPSK (Differential Quadrature Phase Shifted Keying)
5.5 / 11	CCK (Complementary Code Keying)

802.11g Wireless LAN Standard

The ZyAIR, complies with the 802.11g wireless standard and is also fully compatible with the 802.11b standard. This means an 802.11b radio card can interface directly with an 802.11g device (and vice versa) at 11 Mbps or lower depending on range. 802.11g has several intermediate rate steps between the maximum and minimum data rates. The 802.11g data rate and modulation are as follows:.

Table 2 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Note: The ZyAIR may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network.

WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of the individual and applications.

Certificates

The ZyAIR can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

Limit the number of Client Connections

You may set a maximum number of wireless stations that may connect to the ZyAIR. 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.

SSL Passthrough

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". The ZyAIR allows SSL connections to take place through the ZyAIR.

Brute-Force Password Guessing Protection

The ZyAIR has a special protection mechanism to discourage brute-force password guessing attacks on the ZyAIR's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendix for details about this feature.

Wireless LAN MAC Address Filtering

Your ZyAIR 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 ZyAIR supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. 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.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyAIR's management settings. Most functions of the ZyAIR are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.

Embedded FTP and TFTP Servers

The ZyAIR's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the ZyAIR to access your wired network.

Wireless LAN Channel Usage

The **Wireless Channel Usage** screen displays whether the radio channels are used by other wireless devices within the transmission range of the ZyAIR. This allows you to select the channel with minimum interference for your ZyAIR.

1.3 Applications for the ZyAIR

Here are some ZyAIR application examples.

The ZyAIR can be configured using the following WLAN operating modes

- 1 AP
- 2 AP+Bridge
- 3 Bridge/Repeater

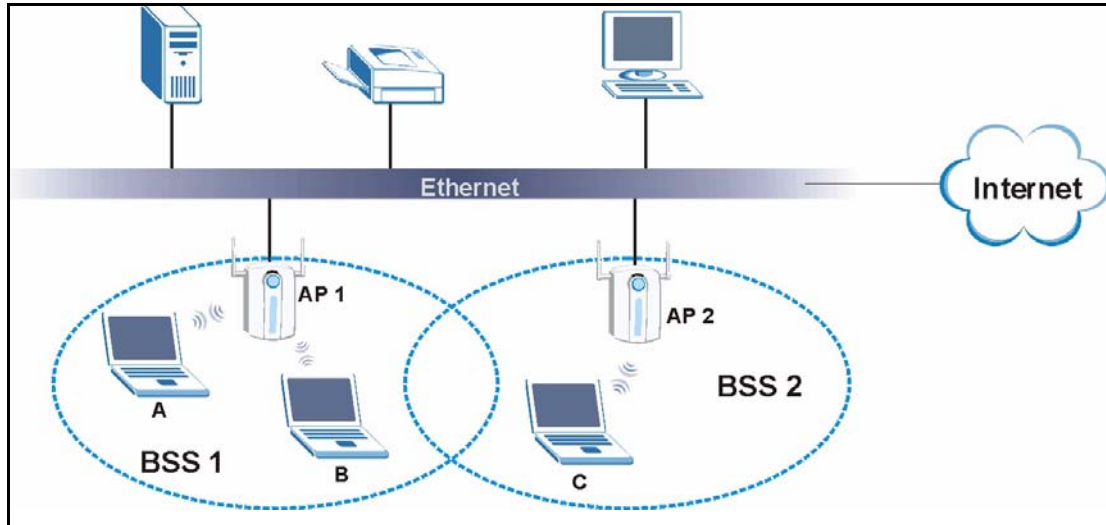
Applications for each operating mode are shown below.

Note: A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

1.3.1 Access Point

The ZyAIR is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyAIR is shown as follows. Stations A, B and C can access the wired network through the ZyAIRs.

Figure 3 Access Point Application



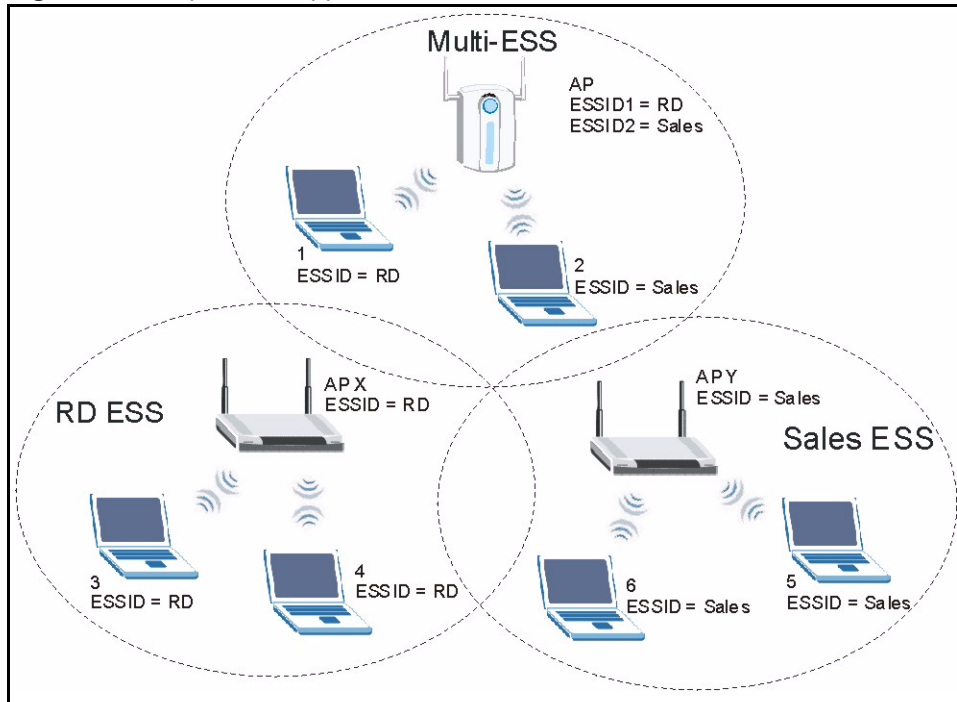
1.3.2 Multiple ESS

The ZyAIR's Multiple ESS function allows multiple ESSs to be configured on just one access point (the ZyAIR). Wireless stations can use different ESSIDs to associate with the same AP. Only wireless stations with the same ESSID can communicate with each other.

In this application example, wireless stations 1 and 2 both associate with the ZyAIR but cannot communicate with each other as they belong to different ESSs. Stations 1, 3 and 4 can communicate with each other. Similarly, stations 2, 5 and 6 can communicate with each other.

Station 1 relays communications via the ZyAIR within the Multi-ESS coverage area and with AP X if it moves to the RD ESS coverage area. Similarly, Station 2 relays communications via the ZyAIR within the Multi-ESS coverage area and with AP Y if it moves to the Sales ESS coverage area.

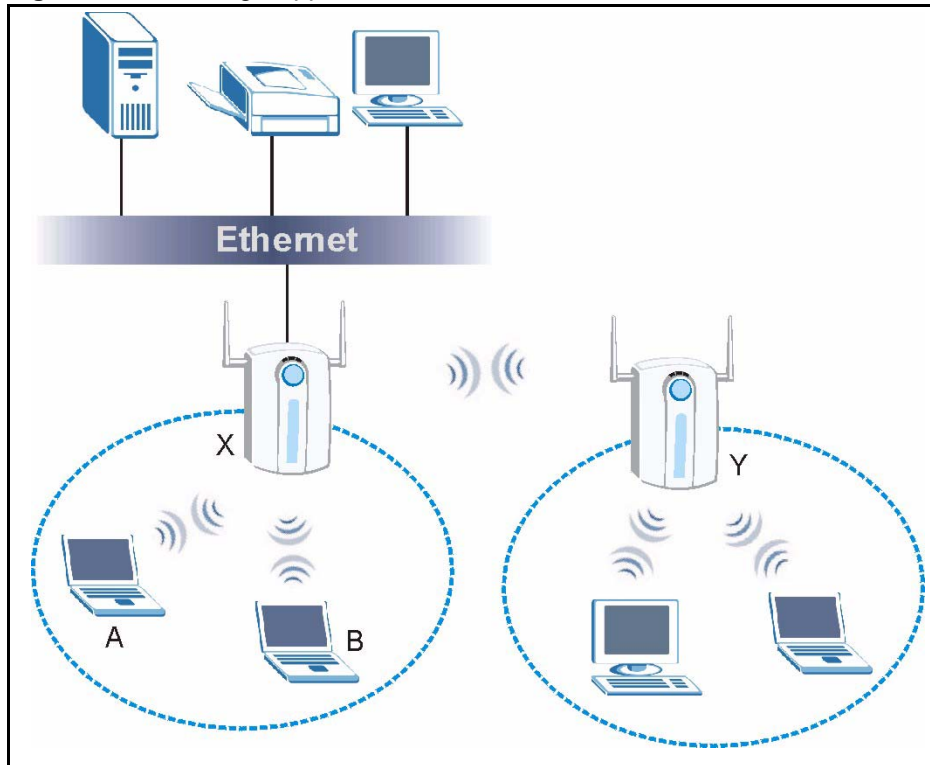
You cannot configure WPA on your ZyAIR in Multiple ESS mode.

Figure 4 Multiple ESS Application

1.3.3 AP + Bridge

In **AP+Bridge** mode, the ZyAIR supports both AP (**A** and **B** can connect to the wired network through **X**) and bridge (**X** can communicate with **Y**) connection at the same time.

When the ZyAIR is in **AP + Bridge** mode, the traffic between ZyAIRs (the WDS) is not encrypted. The security settings on the ZyAIR refer to the traffic between the wireless station and the ZyAIR.

Figure 5 AP+Bridge Application

1.3.4 Bridge / Repeater

The ZyAIR can act as a wireless network bridge and establish wireless links with other APs. In bridge mode, the ZyAIR's (**A** and **B**) are connected to independent wired networks and have a bridge (**A** can communicate with **B**) connection at the same time. A ZyAIR in repeater mode (**C**) has no Ethernet connection. When the ZyAIR is in the bridge mode, you should enable STP to prevent bridge loops.

When the ZyAIR is in **Bridge/Repeater** mode, you don't have to enter a pre-shared key, but the traffic between devices won't be encrypted if you don't. The peer bridge must use the same pre-shared key and encryption method.

The ZyAIR in **AP+Bridge** mode cannot connect to another ZyAIR in **Bridge/Repeater** mode that uses manual WEP keys with 64-bit or 128-bit WEP encryption.

Figure 6 Bridge Application

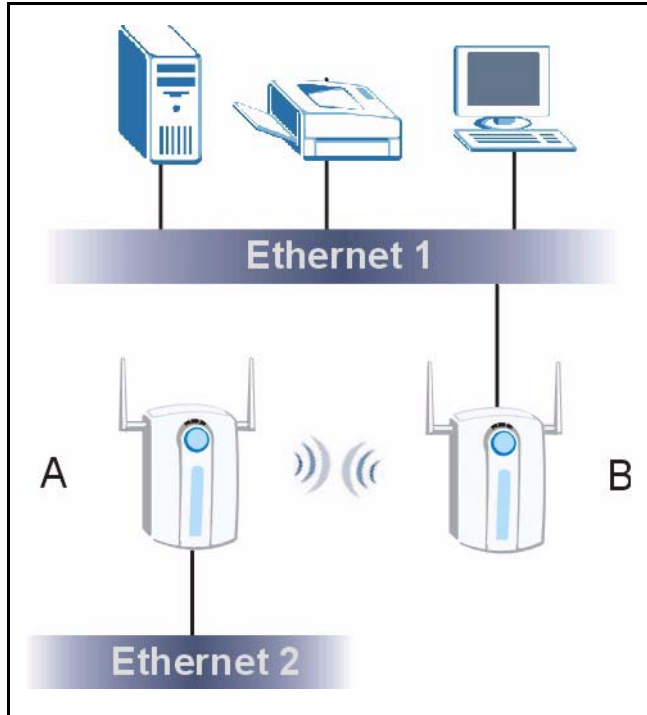
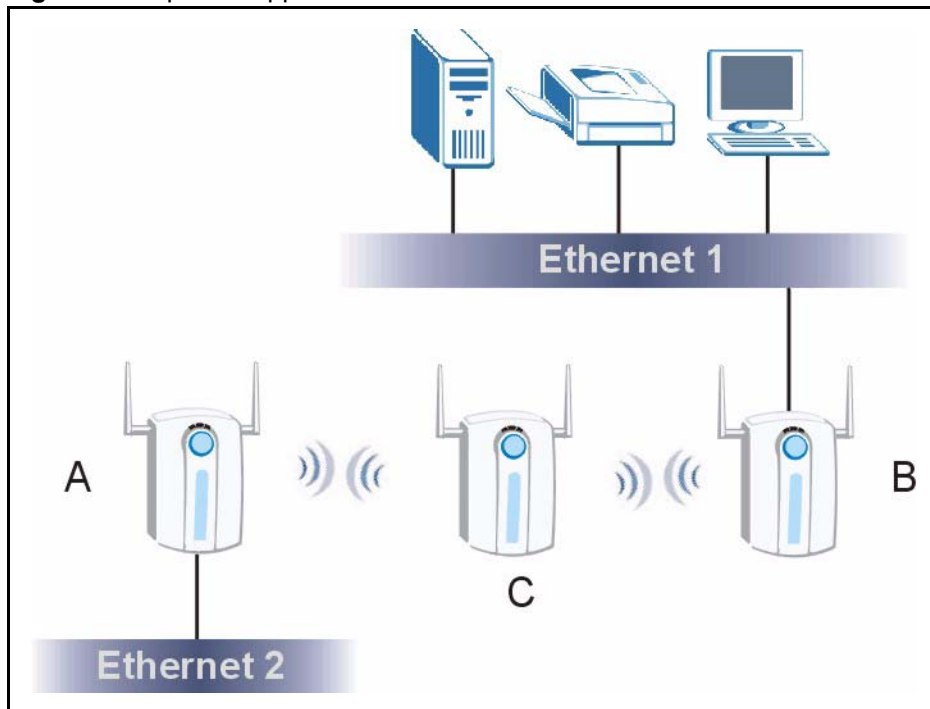


Figure 7 Repeater Application



CHAPTER 2

Introducing the Web Configurator

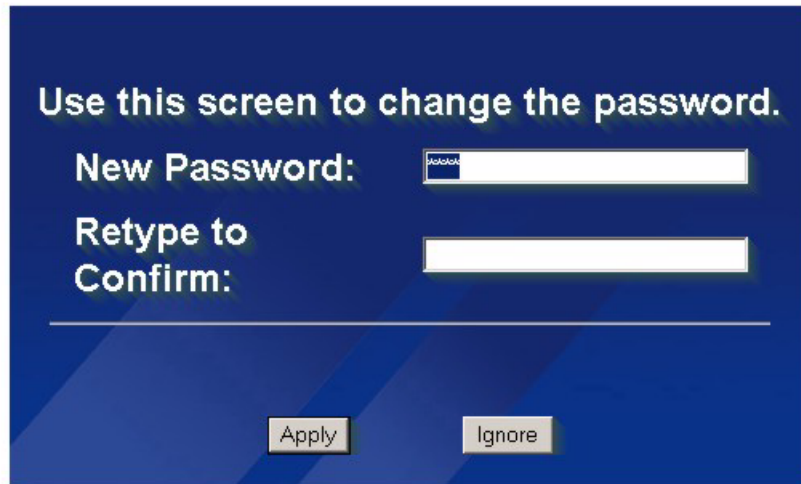
This chapter describes how to access the ZyAIR web configurator and provides an overview of its screens. The default IP address of the ZyAIR is 192.168.1.2.

2.1 Accessing the ZyAIR Web Configurator

- 1 Make sure your ZyAIR hardware is properly connected and prepare your computer/ computer network to connect to the ZyAIR (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.2" as the URL.
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Note: If you do not change the password, the following screen appears every time you login.

Figure 8 Change Password Screen



Use this screen to change the password.

New Password:

Retype to Confirm:

- 6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyAIR's MAC address that will be specific to this device.

Figure 9 Replace Certificate Screen



Replace Factory Default Certificate

The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device.

You should now see the **MAIN MENU** screen.

Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the ZyAIR if this happens to you.

2.2 Resetting the ZyAIR

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the side panel of the ZyAIR. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to 1234.

2.2.1 Procedure To Use The Reset Button

Make sure the **SYS** LED is on (not blinking) before you begin this procedure.

- 1 Press the **RESET** button for ten seconds or until the **SYS** LED, **LINK** LED or **BDG/RPT** LED turns red, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyAIR restarts. Otherwise, go to step 2.
- 2 Turn the ZyAIR off.
- 3 While pressing the **RESET** button, turn the ZyAIR on.
- 4 Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyAIR is now restarting.
- 5 Release the **RESET** button and wait for the ZyAIR to finish restarting.

2.2.2 Method of Restoring Factory-Defaults

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

Use the **RESET** button on the side panel of the ZyAIR to upload the default configuration file (hold this button in for about 10 seconds or until the **SYS** LED, **LINK** LED or **BDG/RPT** LED turns red). Use this method for cases when the password or IP address of the ZyAIR is not known.


Use the web configurator to restore defaults (refer to [Chapter 14, on page 161](#)).

Transfer the configuration file to your ZyAIR using FTP. See later in the part on SMT configuration for more information.

2.3 Navigating the ZyAIR Web Configurator

We use the G-3000H web configurator in this guide as an example. The web configurator screens for your model may vary slightly for different ZyAIR models.

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

Note: Follow the instructions you see in the **MAIN MENU** screen or click the  icon (located in the top right corner of most screens) to view online help.


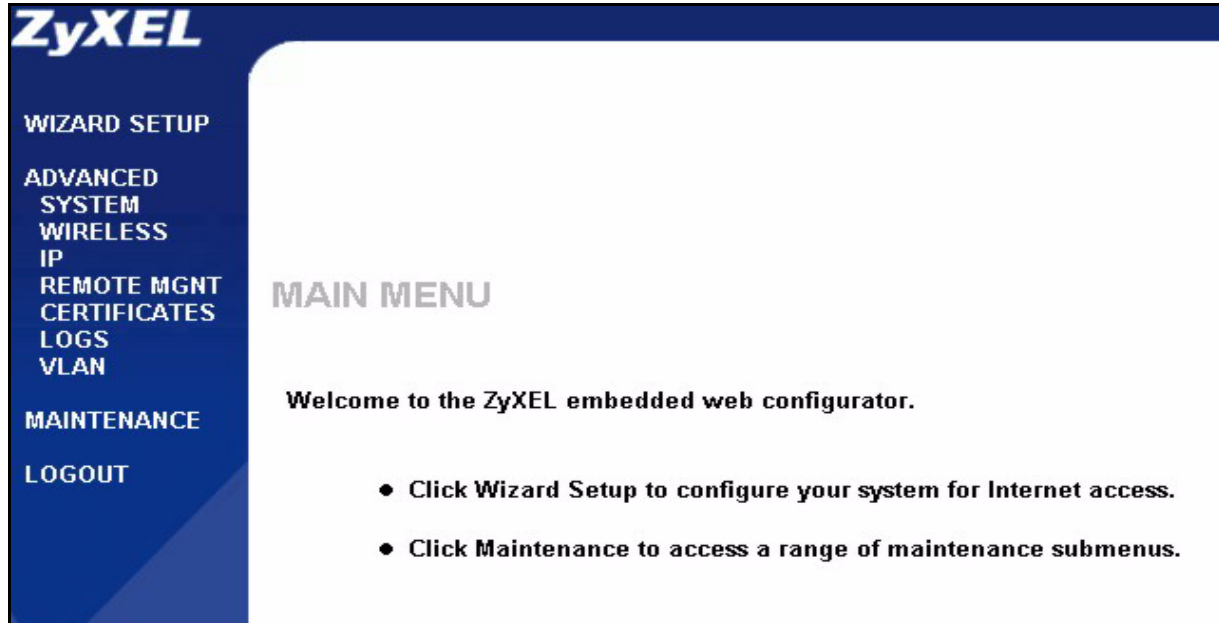
The  icon does not appear in the **MAIN MENU** screen.

Figure 10 The MAIN MENU Screen of the Web Configurator



Click **WIZARD SETUP** for initial configuration including general setup, Wireless LAN setup and IP address assignment.

Click the links under **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Password and Time Zone), **WIRELESS** (Wireless, SSID, Security, RADIUS, Layer-2 Isolation, MAC Filter, Roaming, Local User Database), **IP**, **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **CERTIFICATES** (My Certificates, Trusted CAs), **LOGS** (View reports and Log Settings) and **VLAN**.

Click **MAINTENANCE** to view information about your ZyAIR or upgrade configuration/firmware files. Maintenance includes **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**

Click **LOGOUT** at any time to exit the web configurator

CHAPTER 3

Wizard Setup

This chapter provides information on the Wizard Setup screens in the web configurator.

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your ZyAIR for wireless stations to access your wired LAN.

3.1.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b and IEEE 802.11g 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.

The ZyAIR's "Scan" function is especially designed to automatically scan for a channel with the least interference.

3.1.2 ESS ID

An Extended Service Set (ESS) is a group of access points connected to a wired LAN on the same subnet. An SS ID uniquely identifies each set. All access points and their associated wireless stations in the same set must have the same SSID.

3.1.3 WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. 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 for data encryption and decryption.

3.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.

Figure 11 Wizard 1: General Setup

The screenshot shows a window titled "General Setup:". Inside the window, there is a message: "Enter a descriptive name for identification purposes. We recommend using your computer's name." Below the message are two text input fields. The first is labeled "System Name:" and the second is labeled "Domain Name:". At the bottom right of the window is a button labeled "Next".

The following table describes the labels in this screen.

Table 3 Wizard 1: General Setup

LABEL	DESCRIPTION
System Name	It is recommended you type your computer's "Computer name". In Windows 95/98 click Start, Settings, Control Panel, Network . Click the Identification tab, note the entry for the Computer Name field and enter it as the System Name . In Windows 2000, click Start, Settings, Control Panel and then double-click System . Click the Network Identification tab and then the Properties button. Note the entry for the Computer name field and enter it as the System Name . In Windows XP, click Start, My Computer, View system information and then click the Computer Name tab. Note the entry in the Full computer name field and enter it as the ZyAIR System Name . This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Next	Click Next to proceed to the next screen.

3.3 Wizard Setup: Wireless LAN

Use the second wizard screen to set up the wireless LAN.

Figure 12 Wizard 2: Wireless LAN Setup

The following table describes the labels in this screen.

Table 4 Wizard 2: Wireless LAN Setup

LABEL	DESCRIPTION
Wireless LAN Setup	
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyAIR, make sure all wireless stations use the same Name (SSID) in order to access the network.
Choose Channel ID	To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyAIR automatically select a channel, click Scan instead.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.
WEP Encryption	Select Disable allows all wireless computers to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding 0x is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.

3.4 Wizard Setup: IP Address

The third wizard screen allows you to configure IP address assignment.

3.4.1 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 5 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.

3.4.2 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 ZyAIR, 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 ZyAIR 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 ZyAIR unless you are instructed to do otherwise.

Figure 13 Wizard 3: IP Address Assignment

The following table describes the labels in this screen.

Table 6 Wizard 3: IP Address Assignment

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again.
Use fixed IP address	Select this option if your ZyAIR is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation. Note: If you changed the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyAIR's LAN or WAN port.
Back	Click Back to return to the previous screen.
Finish	Click Finish to proceed to complete the Wizard setup.

3.5 Basic Setup Complete

When you click **Finish** in the **Wizard 3 IP Address Assignment** screen, a warning window display as shown. Click **OK** to close the window and log in to the web configurator again using the new IP address if you change the default IP address (192.168.1.2).

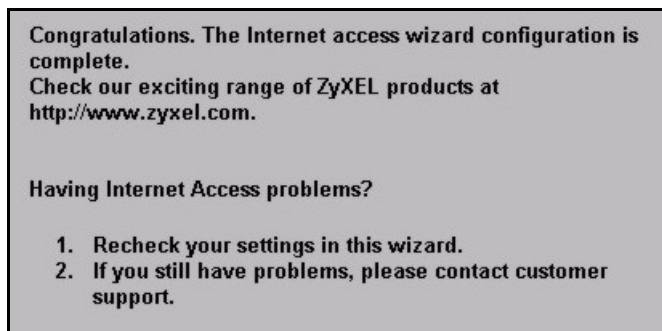


You have successfully set up the ZyAIR. A screen displays prompting you to close the web browser.



Click **Yes**. Otherwise, click **No** and the congratulations screen shows next.

Figure 14 Wizard 4: Setup Complete



Well done! You have successfully set up your ZyAIR to operate on your network and access the Internet.

CHAPTER 4

System Screens

4.1 System Overview

This section provides information on general system setup.

4.2 Configuring General Setup

Click the **SYSTEM** link under **ADVANCED** to open the **General** screen.

Figure 15 System General Setup

The following table describes the labels in this screen.

Table 7 System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Type a descriptive name to identify the ZyAIR in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.

Table 7 System General Setup

LABEL	DESCRIPTION
Administrator Inactivity Timer	<p>Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out.</p> <p>The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.</p> <p>A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).</p>
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	<p>Select From DHCP if your DHCP server dynamically assigns DNS server information (and the ZyAIR's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p> <p>The default setting is None.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

4.3 Configuring Password

To change your ZyAIR's password (recommended), click the **SYSTEM** link under **ADVANCED** and then the **Password** tab. The screen appears as shown. This screen allows you to change the ZyAIR's password.

If you forget your password (or the ZyAIR IP address), you will need to reset the ZyAIR. See the [Resetting the ZyAIR](#) section for details

Figure 16 Password.

The following table describes the labels in this screen.

Table 8 Password

LABEL	DESCRIPTIONS
Old Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 31 characters). 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.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

4.4 Configuring Time Setting

To change your ZyAIR's time and date, click the **SYSTEM** link under **ADVANCED** and then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the ZyAIR's time based on your local time zone.

Figure 17 Time Setting

The following table describes the labels in this screen.

Table 9 Time Setting

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, NTP (RFC 1305) , is similar to Time (RFC 868). Select None to enter the time and date manually.
Time Server Address	Enter the IP address or the URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time (hh:mm:ss)	This field displays the time of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the time with the time server.
New Time (hh:mm:ss)	This field displays the last updated time from the time server. When you select None in the Time Protocol field, enter the new time in this field and then click Apply .
Current Date (yyyy/mm/dd)	This field displays the date of your ZyAIR. Each time you reload this page, the ZyAIR synchronizes the date with the time server.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server. When you select None in the Time Protocol field, enter the new date in this field and then click Apply .

Table 9 Time Setting

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date (mm-dd)	Enter the month and day that your daylight-savings time starts on if you selected Daylight Savings .
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected Daylight Savings .
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to reload the previous configuration for this screen.

CHAPTER 5

Wireless Configuration

This chapter discusses how to configure Wireless screens on the ZyAIR.

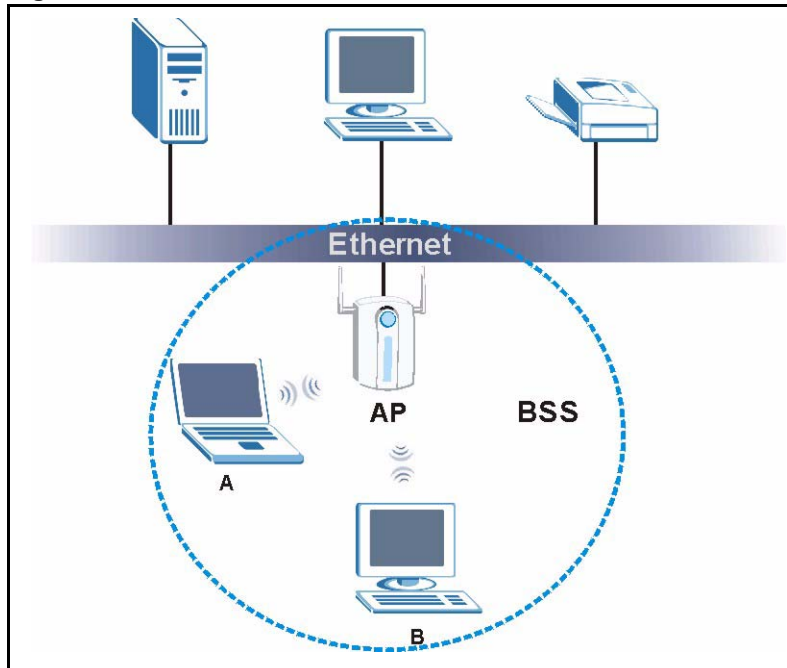
5.1 Wireless LAN Overview

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

5.1.1 BSS

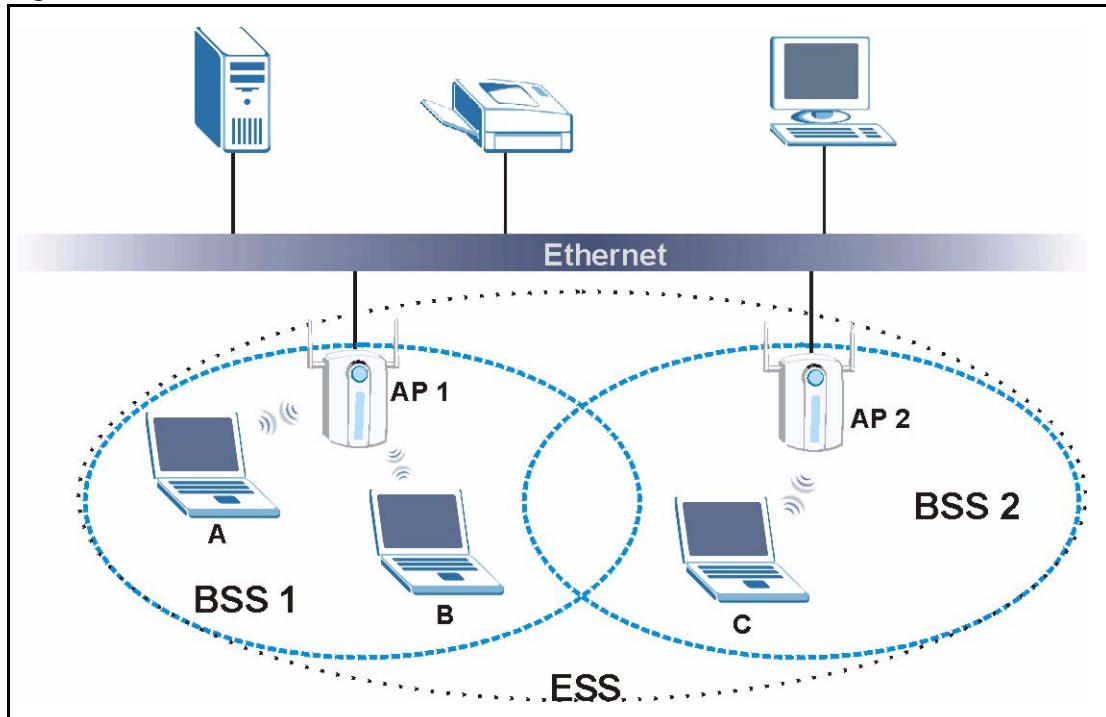
A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

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 18 Basic Service set

5.1.2 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 19 Extended Service Set

5.2 Wireless LAN Basics

Refer also to the [Wizard Setup](#) chapter for more background information on Wireless LAN features, such as channels.

See the Wireless LANs Appendix for information on the following:

- Wireless LAN Topologies
- Channel
- RTS/CTS
- Fragmentation Threshold
- Preamble Type
- IEEE 802.1x
- RADIUS
- Types of Authentication
- WPA
- Security Parameters Summary

5.3 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks for multimedia applications. WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access throughput to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyAIR uses WMM QoS to prioritize traffic streams according to the needs of the application. The ZyAIR automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to jitter (variations in delay).

5.3.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the ZyAIR uses.

Table 10 WMM QoS Priorities

PRIORITY LEVEL	DESCRIPTION
voice	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
besteffort	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

5.3.2 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the Prestige) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

5.3.2.1 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

5.3.2.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 20 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

5.3.3 ToS (Type of Service) and WMM QoS

The DSCP value of outgoing packets is between 0 and 255. 0 is the default priority. WMM QoS checks the DSCP value in the header of data packets. It gives the traffic a priority according to this number.

In order to control which priority level is given to traffic, the device sending the traffic must set the DSCP value in the header. If the DSCP value is not specified, then the traffic is treated as best-effort. This means the wireless clients and the devices with which they are communicating must both set the DSCP value in order to make the best use of WMM QoS. A Voice over IP (VoIP) device for example may allow you to define the DSCP value.

The following table lists which WMM QoS priority level the ZyAIR uses for specific DSCP values.

Table 11 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

DSCP VALUE	WMM QOS PRIORITY LEVEL
224, 192	voice
160, 128	video

Table 11 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

DSCP VALUE	WMM QOS PRIORITY LEVEL
96, 0 ^a	besteffort
64, 32	background

a. The ZyAIR also uses best effort for any DSCP value for which another WMM QoS priority is not specified (255, 158 or 37 for example).

5.4 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

5.4.1 Rapid STP

The ZyAIR uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

5.4.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

Table 12 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

5.4.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

5.4.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 13 STP Port States

PORT STATES	DESCRIPTIONS
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

5.5 Wireless Screen Overview

The following is a list of the screens you can configure on the ZyAIR.

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
----------	------	----------	--------	-------------------	------------	---------	---------------------

- 1** Configure the ZyAIR as an AP, an AP+Bridge, a Bridge/Repeater or to use multiple ESS in the **Wireless** screen. You can also select an **SSID Profile** in the **Wireless** screen.
- 2** Use the **SSID** screens to view and create SSID profiles.
- 3** Use the **Security** screen to configure wireless profiles. For each profile you can configure a name and one of the wireless security modes.
- 4** Use the **RADIUS** screen to configure RADIUS authentication and accounting settings.
- 5** Use the **Layer-2 Isolation** screen to prevent wireless clients associated with your ZyAIR from communicating with other wireless clients, AP's, computers or routers in a network.
- 6** Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.
- 7** Use the **Roaming** screen to configure the ZyAIR so that 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.
- 8** Configure the built-in authentication database in the **Local User Database** screen.

5.6 Configuring Wireless

Click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. The screen varies depending upon the operating mode you select.

5.6.1 Access Point Mode

Select **Access Point** as the **Operating Mode** to display the screen as shown next.

Figure 21 Wireless: Access Point

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
<p>Operating Mode: <input type="text" value="Access Point"/></p> <p>Choose Channel ID: <input type="text" value="Channel-06 2437MHz"/> or <input type="button" value="Scan"/></p> <p>RTS/CTS Threshold: <input type="text" value="2432"/> (800 ~ 2432)</p> <p>Fragmentation Threshold: <input type="text" value="2432"/> (800 ~ 2432)</p> <p>SSID Profile: <input type="text" value="TestSSID"/></p> <p><input type="checkbox"/> Hide Name(SSID)</p> <p><input checked="" type="checkbox"/> Enable Intra-BSS Traffic</p> <p><input checked="" type="checkbox"/> Enable Breathing LED</p> <p><input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)</p> <p>Output Power: <input type="text" value="100% (Full Power)"/></p> <p>Preamble: <input type="text" value="Long"/></p> <p>802.11 Mode: <input type="text" value="Mixed"/></p> <p>Max. Frame Burst: <input type="text" value="650"/> (0 ~1800)</p> <p style="text-align: center;"><input type="button" value="Apply"/> <input type="button" value="Reset"/></p>							

The following table describes the general wireless LAN labels in this screen.

Table 14 Wireless: Access Point

LABEL	DESCRIPTION
Operating Mode	Select the operating mode from the drop-down list. The options are Access Point , Bridge/Repeater , AP+Bridge and MESSID .
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyAIR automatically select a channel, click Scan instead. Refer to the Wizard Setup chapter for more information on channels.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 800 and 2432 .
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 800 and 2432 .
SSID Profile	The SSID (Service Set IDentity) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an SSID Profile from the drop-down list box. Configure SSID profiles in the SSID screen. Note: If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.

Table 14 Wireless: Access Point

LABEL	DESCRIPTION
Hide Name (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.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Select this check box to enable Intra-BSS traffic.
Enable Breathing LED	Select this check box to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyAIR.
Output Power	Set the output power of the ZyAIR in this field. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference with other APs. Select one of the following 100%(Full Power) , 50% , 25% or 12.5% . These percentages represent the following power ranges; <ul style="list-style-type: none"> • 100%(Full Power) <11b>17dBm/<11g>13dBm (<11b>50mW/<11g>20mW), • 50% <11b>15dBm/<11g>11dBm (<11b>32mW/<11g>12.6mW), • 25% <11b>13dBm/<11g>9dBm (<11b>20mW/<11g>7.9mW), • 12.5% <11b>11dBm/<11g>7dBm (<11b>12.6mW/<11g>5mW).
Preamble	Select a preamble type from the drop-down list menu. Choices are Long , Short and Dynamic . See the section on preamble for more information.
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR. Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

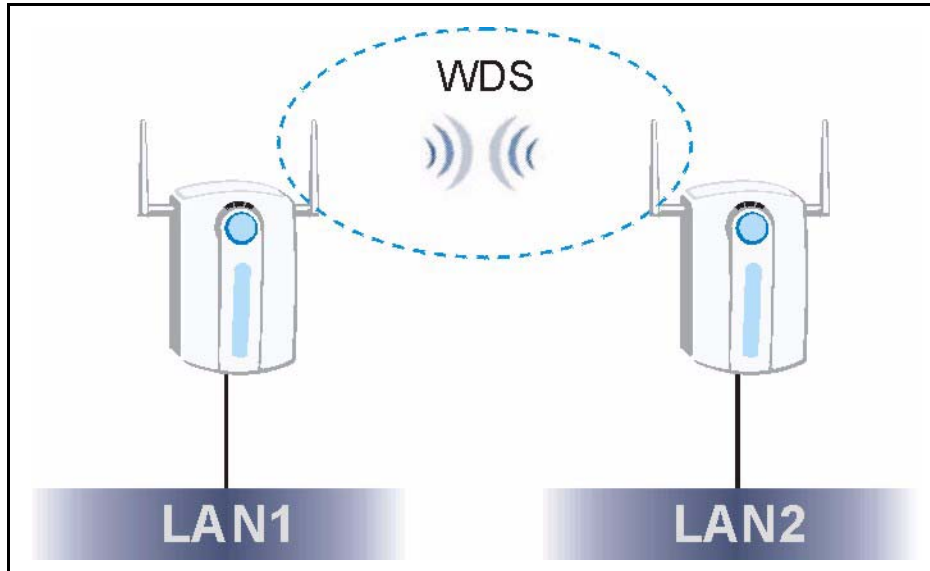
5.6.2 Bridge/Repeater Mode

The ZyAIR 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.

The ZyAIR can establish up to five wireless links with other APs.

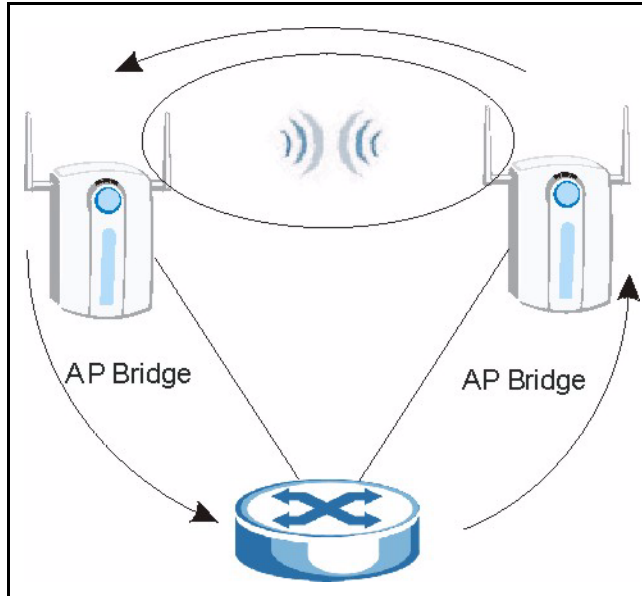
In the example below, when both ZyAIRs are in Bridge/Repeater mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

Figure 22 Bridging Example

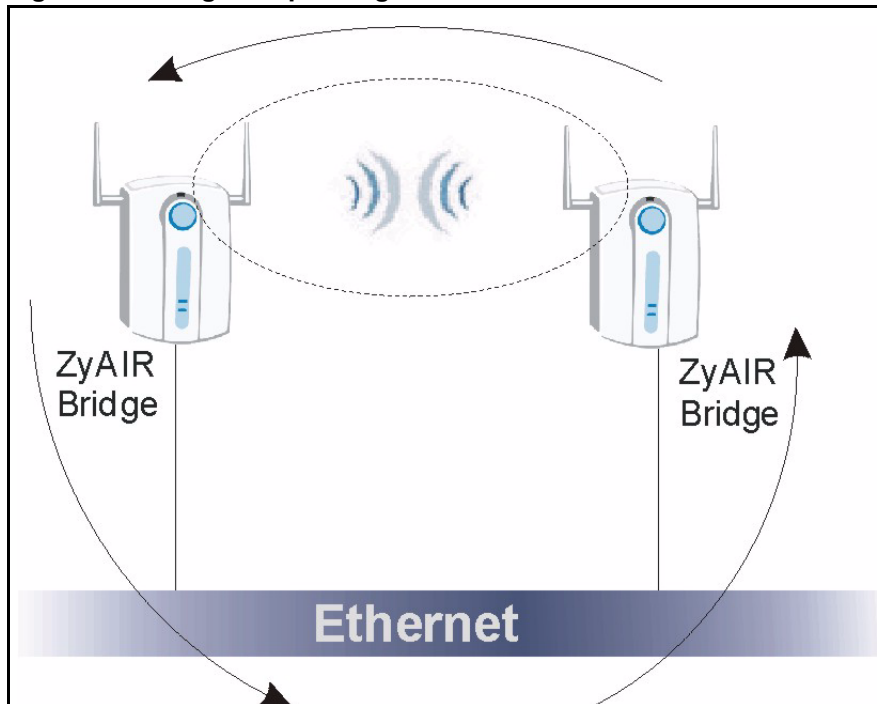


Be careful to avoid bridge loops when you enable bridging in the ZyAIR. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

If two or more ZyAIRs (in bridge mode) are connected to the same hub as shown next.

Figure 23 Bridge Loop: Two Bridges Connected to Hub

If your ZyAIR (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 24 Bridge Loop: Bridge Connected to Wired LAN

To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyAIR is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

Click the **WIRELESS** link under **ADVANCED**. Select **Bridge/Repeater** as the **Operating Mode** to have the ZyAIR act as a wireless bridge only.

Figure 25 Wireless: Bridge/Repeater

The screenshot shows the 'Wireless' configuration page for a Bridge/Repeater. At the top, 'Operating Mode' is set to 'Bridge/Repeater'. Below it, 'Choose Channel ID' is set to 'Channel-06 2437MHz' with a 'Scan' button. 'RTS/CTS Threshold' and 'Fragmentation Threshold' are both set to '2432'. A section for 'WDS Security' is checked, containing a table with 5 rows. Each row has an 'Active' checkbox (all are unchecked), a 'Remote Bridge MAC Address' field (all are '00:00:00:00:00:00'), and a 'PSK' field. Below the table, 'Enable Breathing LED' and 'Enable Spanning Tree Protocol (STP)' are checked. 'Output Power' is set to '100% (Full Power)', 'Preamble' to 'Long', '802.11 Mode' to 'Mixed', and 'Max. Frame Burst' to '650'. 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the bridge labels in this screen.

Table 15 Wireless: Bridge/Repeater

LABEL	DESCRIPTIONS
Operating Mode	Select Bridge/Repeater in this field to display the screen as shown.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyAIR automatically select a channel, click Scan instead. Refer to the Wizard Setup chapter for more information on channels.
Scan	Click this button to have the ZyAIR automatically scan for and select a channel with the least interference.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 800 and 2432 .
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 800 and 2432 .

Table 15 Wireless: Bridge/Repeater

LABEL	DESCRIPTIONS
Enable WDS Security	Select the check box to enable WDS on your ZyAIR. A Wireless Distribution System (WDS) is a wireless connection between two or more APs. When you select the check box, you are prompted to type a Pre-Shared Key (PSK). The ZyAIR uses TKIP to encrypt traffic on the WDS between AP's. Note: Other AP's must use the same encryption method to enable WDS.
#	This is the index number of the bridge connection.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

See [Table 14 on page 65](#) for information on the other labels in this screen.

5.6.3 AP+Bridge Mode

Click the **WIRELESS** link under **ADVANCED**. Select **AP+Bridge** as the **Operating Mode** to display the screen as shown next. In this screen, you can configure the ZyAIR to function as an AP and bridge simultaneously. See the section on ZyAIR applications for more information.

Figure 26 Wireless: AP+Bridge

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database	
Operating Mode		AP+Bridge						
Choose Channel ID		Channel-06 2437MHz					or	Scan
RTS/CTS Threshold		2432 (800 ~ 2432)						
Fragmentation Threshold		2432 (800 ~ 2432)						
SSID Profile		TestSSID						
#	Active	Remote Bridge MAC Address	PSK					
1	<input type="checkbox"/>	00:00:00:00:00:00						
2	<input type="checkbox"/>	00:00:00:00:00:00						
3	<input type="checkbox"/>	00:00:00:00:00:00						
4	<input type="checkbox"/>	00:00:00:00:00:00						
5	<input type="checkbox"/>	00:00:00:00:00:00						
<input type="checkbox"/> Hide Name(SSID)								
<input checked="" type="checkbox"/> Enable Intra-BSS Traffic								
<input checked="" type="checkbox"/> Enable Breathing LED								
<input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)								
Output Power		100% (Full Power)						
Preamble		Long						
802.11 Mode		Mixed						
Max. Frame Burst		650 (0 ~ 1800)						
Apply				Reset				

See the tables describing the fields in the **Access Point** and **Bridge/Repeater** operating modes for descriptions of the fields in this screen.

5.6.4 Multiple ESS Mode

Select **MESSID** as the **Operating Mode** to display the screen. Refer to the chapter on Multiple ESS and VLAN for configuration and detailed information. See the chapter on wireless security for details on the security settings.

Note: The following screens are configurable only in **Access Point** and **AP+Bridge** operating modes only.

CHAPTER 6

Wireless Security Configuration

This chapter describes how to use the **Security**, **RADIUS** and **Local User Database** screens to configure wireless security on your ZyAIR.

6.1 Wireless Security Overview

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

Wireless security methods available on the ZyAIR are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyAIR identity.

6.1.1 Encryption

- Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA 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 manually enter 64-bit, or 128-bit WEP keys.

6.1.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use the built-in database (Local User Database) or a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the ZyAIR.
- Use the Local User Database if you have less than 32 wireless clients in your network. The ZyAIR uses MD5 encryption when a client authenticates with the Local User Database

6.1.3 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**).

6.1.4 Hide ZyAIR Identity

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

6.1.5 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.

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

6.2 Configuring WEP Encryption

In order to configure and enable WEP encryption; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen.

Note: The **WEP Encryption, Authentication Method** and the WEP key fields are not visible when you enable Dynamic WEP Key, WPA or WPA-PSK in the **Security** screen.

6.3 802.1x 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 ZyAIR (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

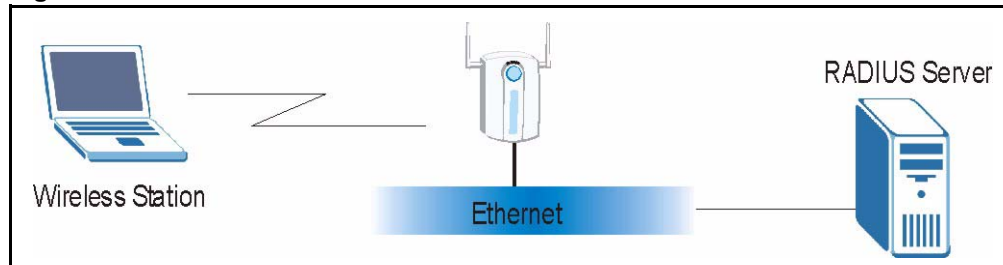
6.4 EAP Authentication Overview

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

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

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

Figure 27 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 ZyAIR.
- 2 The ZyAIR 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.

6.5 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.

To use Dynamic WEP, enable and configure the RADIUS server and enable one of the Dynamic WEP **Security Modes** in the **Security** 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.

6.6 Introduction to WPA

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.

6.6.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS, EAP and PEAP.

If you don't have an external RADIUS server you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

6.6.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

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

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

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

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

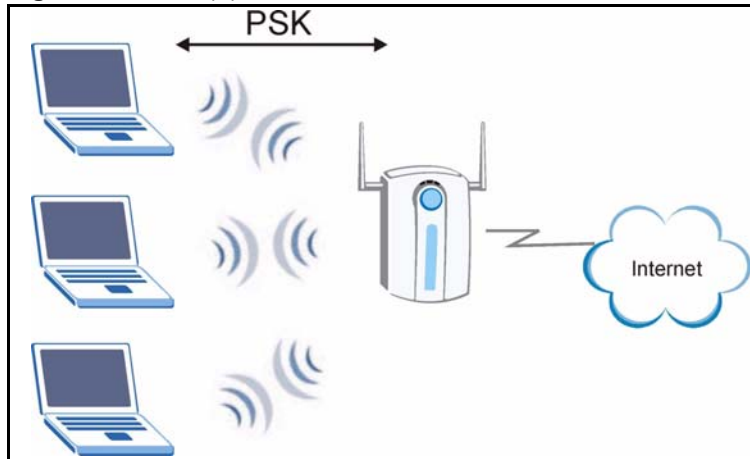
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement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

6.6.3 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 wireless client's password and (only) allows it to join the network if the password matches.
- 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.

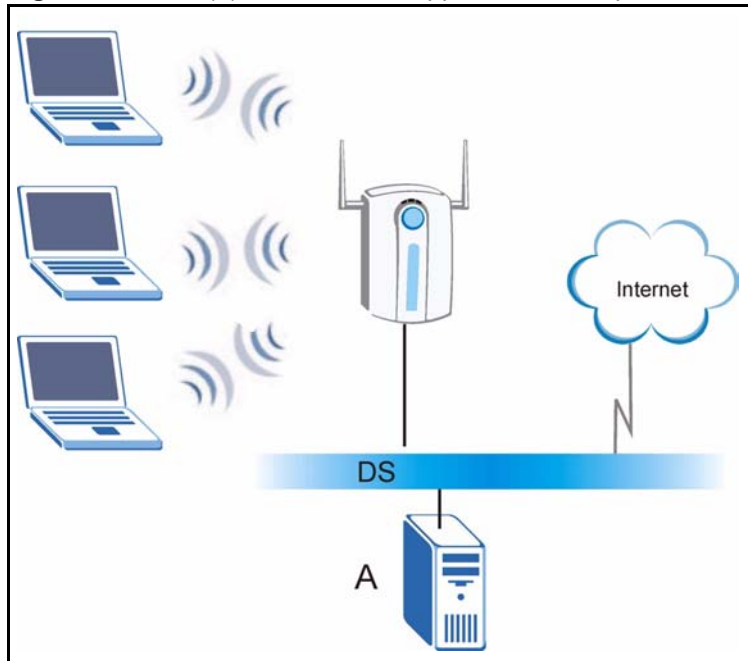
Figure 28 WPA(2)-PSK Authentication



6.7 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 29 WPA(2) with RADIUS Application Example

6.8 Security Modes

The following table describes the security modes you can configure.

Table 16 Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP	Select this to use WEP encryption.
802.1x-Only	Select this to use 802.1x authentication with no data encryption.
802.1x-Dynamic64	Select this to use 802.1x authentication with a dynamic 64bit WEP key.
802.1x-Dynamic128	Select this to use 802.1x authentication with a dynamic 128bit WEP key.
802.1x-Static64	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
802.1x-Static128	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA2-PSK	Select this to use WPA2 with a pre-shared key.
WPA2-PSK-MIX	Select this to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
WPA	Select this to use WPA.
WPA-MIX	Select this to use either WPA or 802.1x Only depending on which security mode the wireless client uses.
WPA2	Select this to use WPA2.

Table 16 Security Modes

SECURITY MODE	DESCRIPTION
WPA2-MIX	Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.
No-Access	Select this to prevent wireless client access to the ZyAIR.

6.9 Security Modes and Wireless Client Compatibility

Different security modes can be configured for each SSID. However, not all security modes are compatible with the security mode of the wireless client. The following table shows combinations of security modes between a Windows XP wireless client and the ZyAIR. Combinations of security modes not marked with a “O” or not listed may not be able to make a connection using the SSID. Other wireless clients such as Funk Odyssey may connect using a security combination not listed on the table.

Table 17 Security Modes for ZyAIR and Windows XP Wireless Client

	WEP	8021X-ONLY	8021X-DYNAMIC	8021X-STATIC	WPA	WPA-PSK	WPA-MIX	WPA2	WPA2-PSK	WPA2-MIX	WPA2-PSK-MIX	NONE	NO ACCESS
WEP	O	O	O	O									O
8021X-ONLY	O	O	O	O									O
8021X-DYNAMIC	O	O	O	O									O
8021X-STATIC	O	O	O	O									O
WPA					O			O	O				
WPA-PSK						O		O	O				
WPA-MIX							O	O	O				
WPA2					O	O	O	O					
WPA2-PSK					O	O	O		O				
WPA2-MIX										O			
WPA2-PSK-MIX											O		
NONE												O	
NO ACCESS	O	O	O	O									O

6.10 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.


The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

The Funk Software's Odyssey client is bundled free (at the time of writing) with the client wireless adaptor(s).

6.11 Wireless Security Effectiveness

The following figure shows the relative effectiveness of these wireless security methods available on your ZyAIR. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Table 18 ZyAIR 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
	Wi-Fi Protected Access (WPA)
	Most Secure WPA2

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

6.12 Configuring Security

Use the Security screen to create secure profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **SSID** configuration screen.

You can configure up to 16 security profiles.

To change your ZyAIR's wireless security settings, click the **WIRELESS** link under **ADVANCED** and then the **Security** tab.

Figure 31 Security: No Access or None

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Name : <input type="text" value="security02"/> Security Mode : <input type="text" value="No-Access"/>							
<input type="button" value="Apply"/> <input type="button" value="Reset"/>							

The following table describes the labels in this screen.

Table 20 Security: No Access or None

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Choose No Access or None in this field.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.12.2 Security: WEP

Select **WEP** in the **Security Mode** field to display the following screen.

Figure 32 Security: WEP

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Name : <input type="text" value="security01"/> Security Mode : <input type="text" value="WEP"/> WEP Encryption : <input type="text" value="64-bit WEP"/> Authentication Method : <input type="text" value="Auto"/>							
<input checked="" type="radio"/> ASCII <input type="radio"/> Hex							
<input checked="" type="radio"/> Key 1 <input type="text"/> <input type="radio"/> Key 2 <input type="text"/> <input type="radio"/> Key 3 <input type="text"/> <input type="radio"/> Key 4 <input type="text"/>							
<input type="button" value="Apply"/> <input type="button" value="Reset"/>							

The following table describes the labels in this screen.

Table 21 Security: WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Choose WEP in this field.

Table 21 Security: WEP

LABEL	DESCRIPTION
WEP Encryption	Select Disable to allow wireless stations to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	Select Auto , Open System or Shared Key from the drop-down list box. The default setting is Auto .
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyAIR and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.12.3 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP

Select **802.1x Only**, **802.1x Static 64** or **802.1x Static 128** in the **Security Mode** field to display the following screen.

Figure 33 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Name :		<input type="text" value="security02"/>					
Security Mode :		<input type="text" value="8021x-Static128"/>					
		<input checked="" type="radio"/> ASCII <input type="radio"/> Hex					
<input type="radio"/> Key 1		<input type="text"/>					
<input type="radio"/> Key 2		<input type="text"/>					
<input type="radio"/> Key 3		<input type="text"/>					
<input type="radio"/> Key 4		<input type="text"/>					
ReAuthentication Timer :		<input type="text" value="1800"/> (in seconds)					
Idle Timeout :		<input type="text" value="3600"/> (in seconds)					
Authentication Databases :		<input type="text" value="RADIUS Only"/>					
		<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels in this screen.

Table 22 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Choose 802.1x Only , 802.1x Static 64 or 802.1x Static 128 in this field.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	<p>If you chose 64-bit WEP in the WEP Encryption field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>If you chose 128-bit WEP in the WEP Encryption field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.</p> <p>The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>
ReAuthentication Timer	<p>Specify how often wireless stations have to resend user names and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	<p>The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.</p> <p>The default time interval is 3600 seconds (or 1 hour).</p>

Table 22 Security: 802.1x Only, 802.1x Static 64-bit WEP, 128-bit WEP

LABEL	DESCRIPTION
Authentication Databases	<p>The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.12.4 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP

Select **802.1x Dynamic 64** or **802.1x Dynamic 128** in the **Security Mode** field to display the following screen.

Figure 34 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP

The screenshot shows a configuration interface with the following fields and values:

- Name :** security02
- Security Mode :** 8021x-Dynamic128
- ReAuthentication Timer :** 1800 (in seconds)
- Idle Timeout :** 3600 (in seconds)

Buttons for **Apply** and **Reset** are located at the bottom of the form.

The following table describes the labels in this screen.

Table 23 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Choose 802.1x Dynamic 64 or 802.1x Dynamic 128 in this field.

Table 23 Security: 802.1x Dynamic 64-bit WEP, 128-bit WEP

LABEL	DESCRIPTION
ReAuthentication Timer	<p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	<p>The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>The default time interval is 3600 seconds (or 1 hour).</p>
Authentication Databases	<p>The authentication database contains wireless station login information. The local user database is the built-in database on the ZyAIR. The RADIUS is an external server. Use this drop-down list box to select which database the ZyAIR should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local User Database Only to have the ZyAIR just check the built-in user database on the ZyAIR for a wireless station's username and password.</p> <p>Select RADIUS Only to have the ZyAIR just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select Local first, then RADIUS to have the ZyAIR first check the user database on the ZyAIR for a wireless station's username and password. If the user name is not found, the ZyAIR then checks the user database on the specified RADIUS server.</p> <p>Select RADIUS first, then Local to have the ZyAIR first check the user database on the specified RADIUS server for a wireless station's username and password. If the ZyAIR cannot reach the RADIUS server, the ZyAIR then checks the local user database on the ZyAIR. When the user name is not found or password does not match in the RADIUS server, the ZyAIR will not check the local user database and the authentication fails.</p>
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.12.5 Security: WPA, WPA-MIX, WPA2, WPA2-MIX

Select **WPA**, **WPA-MIX**, **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 35 Security: WPA, WPA-MIX, WPA2 or WPA2-MIX

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
<p>Name : <input type="text" value="security02"/></p> <p>Security Mode : <input type="text" value="WPA"/></p> <p>ReAuthentication Timer : <input type="text" value="1800"/> (in seconds)</p> <p>Idle Timeout : <input type="text" value="3600"/> (in seconds)</p> <p>Group Key Update Timer : <input type="text" value="1800"/> (in seconds)</p> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </p>							

The following table describes the labels not previously discussed

Table 24 Security: WPA, WPA-MIX, WPA2 or WPA2-MIX

LABEL	DESCRIPTIONS
Name	Type a name to identify this security profile.
Security Mode	Choose WPA , WPA-MIX , WPA2 or WPA2-MIX in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) 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. Setting of the Group Key Update Timer is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.12.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

Figure 36 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
<p>Name : <input type="text" value="security02"/></p> <p>Security Mode : <input type="text" value="WPA-PSK"/></p> <p>Pre-Shared Key : <input type="text" value="12345678"/></p> <p>ReAuthentication Timer : <input type="text" value="1800"/> (in seconds)</p> <p>Idle Timeout : <input type="text" value="3600"/> (in seconds)</p> <p>Group Key Update Timer : <input type="text" value="1800"/> (in seconds)</p> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </p>							

The following table describes the labels not previously discussed

Table 25 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Choose WPA-PSK , WPA2-PSK or WPA2-PSK-MIX in this field.
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 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyAIR automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK key management) or RADIUS server (if using WPA key management) 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. Setting of the Group Key Update Timer is also supported in WPA-PSK mode. The ZyAIR default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.13 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 ZyAIR acts as a message relay between the wireless station and the network RADIUS server.

6.14 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using an external server.

You can configure up to four RADIUS server profiles. Each profile also has one backup authentication server and a backup accounting server. These profiles can be assigned to an SSID profile in the **SSID** configuration screen

To set up your ZyAIR's RADIUS server settings, click the **WIRELESS** link under **ADVANCED** and then the **RADIUS** tab. The screen appears as shown.

Figure 37 RADIUS

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Index :		2					
Profile Name :		radius02					
		<input checked="" type="checkbox"/> Active		<input type="checkbox"/> Active			
RADIUS Server IP Address		10.20.20.10		0.0.0.0			
RADIUS Server Port		1812		1812			
Share Secret		12345678					
		<input checked="" type="checkbox"/> Active		<input type="checkbox"/> Active			
Accounting Server IP Address		10.20.20.30		0.0.0.0			
Accounting Server Port		1813		1813			
Share Secret		12345678					
		Apply		Reset			

The following table describes the labels in this screen.

Table 26 RADIUS

LABEL	DESCRIPTION
Index	Select the RADIUS profile you want to configure from the drop-down list box.
Profile Name	Type a name for the RADIUS profile associated with the Index number above.
Primary	Configure the fields below to have user authenticate and accounting through external servers.
Backup	If the ZyAIR cannot authenticate a wireless station(s) using the Primary RADIUS server or communicate with the Primary accounting server, you can have the ZyAIR use a Backup RADIUS server. Make sure the Active check boxes are selected if you want to use backup servers. The ZyAIR will attempt to communicate three times before using the Backup servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the ReAuthentication Timer field in the Security screen.
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the ZyAIR.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
RADIUS Server Port	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.
Share Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyAIR. The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network.
Active	Select the check box to enable user accounting through an external authentication server.

Table 26 RADIUS

LABEL	DESCRIPTION
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyAIR. The key must be the same on the external authentication server and your ZyAIR. The key is not sent over the network.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

6.15 Configuring Local User Database

To change your ZyAIR's local user database, click the **WIRELESS** link under **ADVANCED** and then the **Local User Database** tab. The screen appears as shown.

Figure 38 Local User Database

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
...
30	<input type="checkbox"/>		
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

The following table describes the labels in this screen.

Table 27 Local User Database

LABEL	DESCRIPTION
Active	Select this check box to activate the user profile.
User Name	Enter the username (up to 31 characters) for this user profile.
Password	Type a password (up to 31 characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 7

Multiple ESS, SSID and VLAN

This chapter describes how to use configure multiple ESS, SSID and VLAN on your ZyAIR.

7.1 Wireless LAN Infrastructures

See the Wizard Setup and Wireless LAN chapters for some basic WLAN scenarios and terminology.

7.1.1 Multiple ESS

Traditionally, you needed different APs to configure different ESSs. As well as the cost of buying extra APs, there was also the possibility of channel interference. The ZyAIR's Multiple ESS (Multi-ESS) function allows multiple ESSs to be configured on just one access point (the ZyAIR).

Wireless stations can use different ESS IDs to associate with the same AP. Only wireless stations with the same ESS ID can communicate with each other. This allows the AP to logically group wireless stations in a manner similar to VLAN (Virtual LAN).

With Multi-ESS, the ZyAIR ignores the ToS in the header of data packets and uses a single QoS priority level for all of an ESS's traffic.

7.1.2 Notes on Multiple-ESS

- A maximum of eight ESSs are allowed on one AP.
- Each ESS has its own MAC filter set; see the MAC filter set section for more information.
- When you enable Multi-ESS on the ZyAIR, you need to configure separate Unicast and Multicast/Broadcast keys for each ESS. A Unicast transmission is from one sender to one recipient. A broadcast transmission is from one sender to everybody on the network. A Multicast transmission is from one sender to a group of hosts on the network.
- You must use different WEP keys for different ESSs. If two stations have different ESS IDs (they are in different ESSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).
- When you enable Multi-ESS, ESS IDs are automatically hidden (so site survey tools cannot find other station ESS IDs).
- Multi-ESS should not replace but rather be used in conjunction with 802.1x security.

7.1.3 Multiple ESS Example

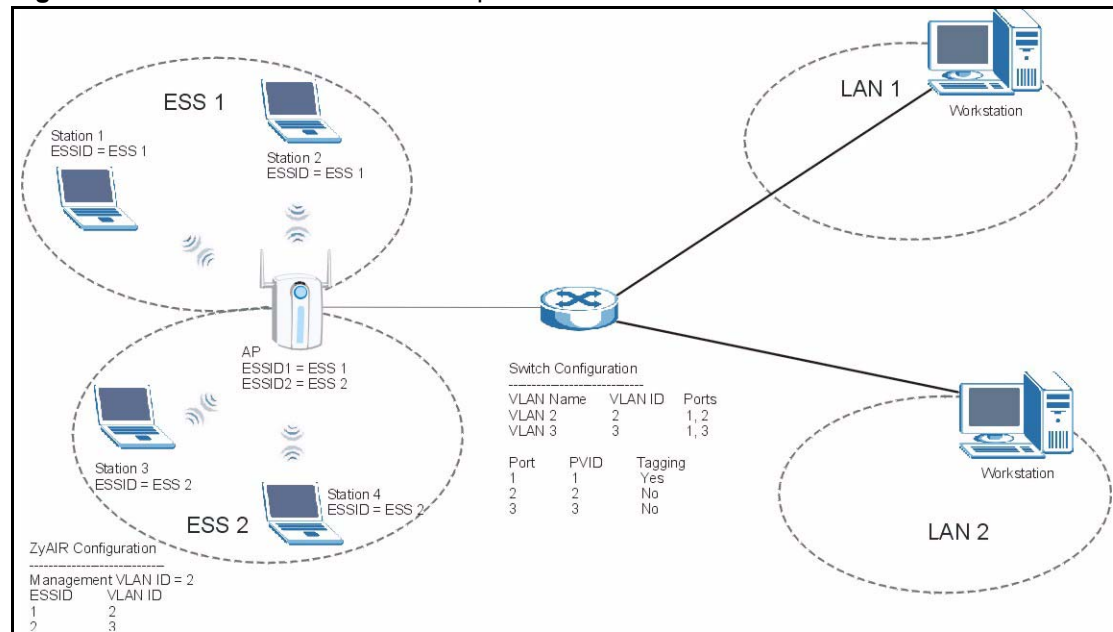
Refer to the section on ZyAIR applications for more information.

7.1.4 Multi-ESS with VLAN Example

In this example, VLAN 2 is the management VLAN and includes the computers in ESS1 and LAN 1. Computers in ESS2 and LAN 2 belong to VLAN 2. “Wireless group” ESS1 is limited to accessing the resources on LAN 1 and similarly “wireless group” ESS2 may only access resources on LAN 2.

The switch adds the PVID tag to incoming frames that don't already have tags on switch ports where PVID is enabled.

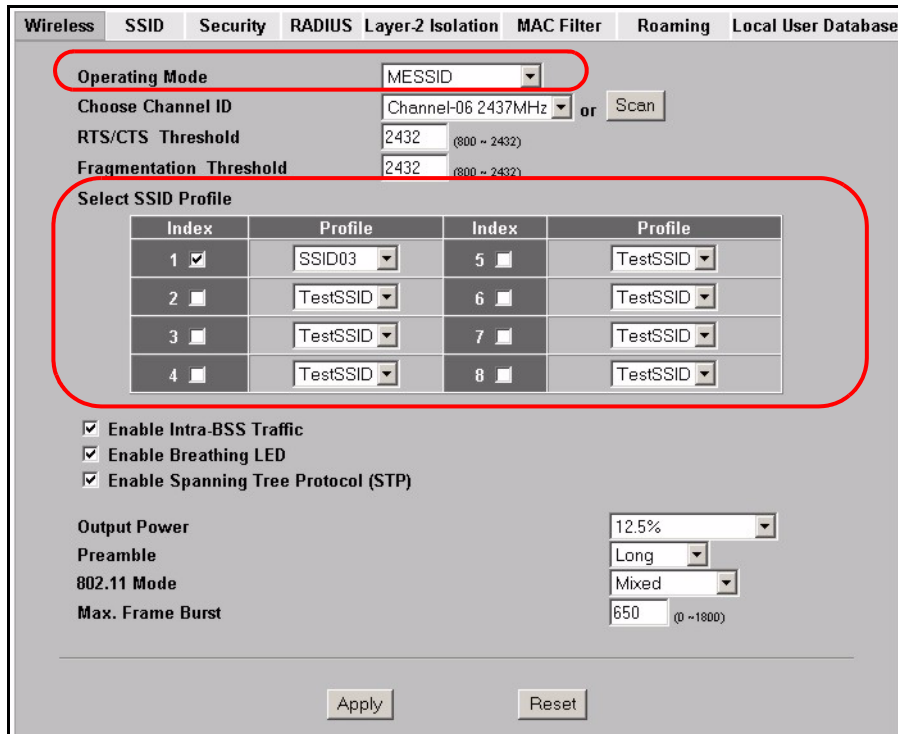
Figure 39 Multi-ESS with VLAN Example



7.1.5 Configuring Multiple ESS

Click the **WIRELESS** link under **ADVANCED** and the **Wireless tab**. Select **MESSID** in the **Operating Mode** drop-down list box to display the screen as shown.

Figure 40 Wireless: Multiple ESS



The following table describes the labels in this screen.

Table 28 Wireless: Multiple ESS

LABEL	DESCRIPTION
Operating Mode	Select MESSID in this field to display the screen as shown
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the ZyAIR to use a channel, select a channel from the drop-down list box. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyAIR automatically select a channel, click Scan instead. Refer to the Wizard Setup chapter for a little more information on channels.
Scan	To have the ZyAIR automatically select a channel, click Scan instead.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 800 and 2432 .
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 800 and 2432 .

Table 28 Wireless: Multiple ESS

LABEL	DESCRIPTION
Select SSID Profile	<p>The SSID (Service Set Identity) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.</p> <p>Note: If you are configuring the ZyAIR from a computer connected to the wireless LAN and you change the ZyAIR's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyAIR's new settings.</p>
Index	Select the check box to activate an ESS on the ZyAIR.
Profile	Select an SSID Profile from the drop-down list box. Configure SSID profiles in the SSID screen.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Select this check box to enable Intra-BSS traffic.
Enable Breathing LED	<p>Select this check box to enable the Breathing LED, also known as the ZyAIR LED.</p> <p>The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations.</p> <p>Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.</p>
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyAIR.
Output Power	<p>Set the output power of the ZyAIR in this field. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference with other APs. Select one of the following 100%(Full Power), 50%, 25% or 12.5%. These percentages represent the following power ranges;</p> <ul style="list-style-type: none"> • 100%(Full Power) <11b>17dBm/<11g>13dBm (<11b>50mW/<11g>20mW), • 50% <11b>15dBm/<11g>11dBm (<11b>32mW/<11g>12.6mW), • 25% <11b>13dBm/<11g>9dBm (<11b>20mW/<11g>7.9mW), • 12.5% <11b>11dBm/<11g>7dBm (<11b>12.6mW/<11g>5mW).
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are Long, Short and Dynamic.</p> <p>See the section on preamble for more information.</p>
802.11 Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR.</p> <p>Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.</p>

Table 28 Wireless: Multiple ESS

LABEL	DESCRIPTION
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

7.2 SSID

Click the **WIRELESS** link under **ADVANCED** and the **SSID** tab to display the screen as shown.

Figure 41 SSID

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Index	Name	SSID	VLAN	Second Rx VLAN	Security	RADIUS	QoS
1	SSID01	ZyXEL	1	1	security01	radius01	besteffort
2	SSID02	ZyXEL02	2	2	security01	radius01	besteffort
3	SSID03	ZyXEL03	3	3	security01	radius01	besteffort
4	SSID04	ZyXEL04	4	4	security01	radius01	besteffort
5	SSID05	ZyXEL05	5	5	security01	radius01	besteffort
6	SSID06	ZyXEL06	6	6	security01	radius01	besteffort
7	SSID07	ZyXEL07	7	7	security01	radius01	besteffort
8	SSID08	ZyXEL08	8	8	security01	radius01	besteffort
9	SSID09	ZyXEL09	9	9	security01	radius01	besteffort
10	SSID10	ZyXEL10	10	10	security01	radius01	besteffort
11	SSID11	ZyXEL11	11	11	security01	radius01	besteffort
12	SSID12	ZyXEL12	12	12	security01	radius01	besteffort
13	SSID13	ZyXEL13	13	13	security01	radius01	besteffort
14	SSID14	ZyXEL14	14	14	security01	radius01	besteffort
15	SSID15	ZyXEL15	15	15	security01	radius01	besteffort
16	SSID16	ZyXEL16	16	16	security01	radius01	besteffort

Edit

The following table describes the labels in this screen.

Table 29 SSID

LABEL	DESCRIPTION
Index	This field displays the index number of each SSID profile.
Name	This field displays the identification name of each SSID profile on the ZyAIR.

Table 29 SSID

LABEL	DESCRIPTION
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate, this is the identity that is broadcast and viewed in the wireless client utility.
VLAN	This field displays the VLAN ID. Incoming traffic from the WAN is tagged with this ID before it is sent to the LAN interface. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Second Rx VLAN	This field displays the identification number of incoming Ethernet frames that are forwarded to this ESS. This number can be the same for many ESS groups, depending on how many you want to be members of a particular VLAN.
Security	This field displays a security profile. See Configuring Security on page 80 for more information.
RADIUS	This field displays a RADIUS profile, if you have a RADIUS server configured.
QoS	This field displays the Quality of Service setting for this profile.
Edit	Click the radio button next to the profile you want to configure and click Edit to go to the SSID configuration screen.

7.2.1 Configuring SSID

Configure appropriate fields in the **Wireless**, **Security**, **RADIUS**, **MAC Filter**, **Layer-2 Isolation** and **VLAN** screens to use those settings in the following screen. These settings can be used instead of the default settings to create SSID profiles.

Figure 42 Configuring SSID

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Name :	<input type="text" value="SSID01"/>						
SSID :	<input type="text" value="ZyXEL"/>						
VLAN ID :	<input type="text" value="1"/>						
Second Rx VLAN ID :	<input type="text" value="3"/>						
Security :	security02 ▾						
RADIUS :	radius02 ▾						
QoS :	video ▾						
L2 Isolation :	Enable ▾						
Enable MAC Filtering :	Disable ▾						
<input type="button" value="Apply"/> <input type="button" value="Reset"/>							

The following table describes the labels in this screen.

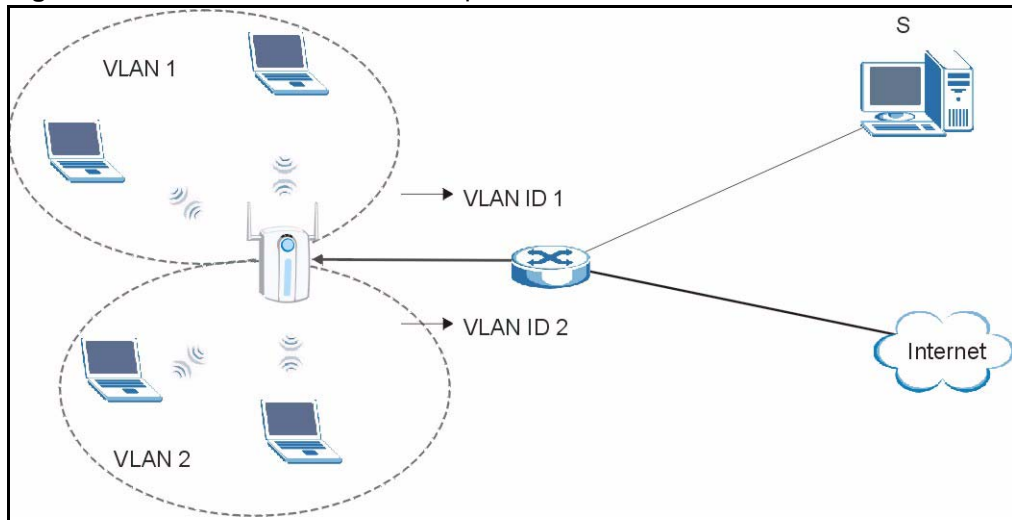
Table 30 Configuring SSID

LABEL	DESCRIPTION
Name	Type a name to identify this SSID profile on the ZyAIR.
SSID	Type a name to identify this wireless profile on the network. When a wireless client scans for an AP to associate, this is the identity that is broadcast and viewed in the wireless client utility.
VLAN	Enter a number from 1 to 4094. Incoming traffic from the WAN is tagged with this ID before it is sent to the LAN interface. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Second Rx VLAN	Enter a number from 1 to 4094, but different to the VLAN ID entered. Traffic received from the LAN interface is tagged with a Second Rx VLAN and forwarded to this SSID profile on the wireless LAN interface.
Security	Select a security profile. See Configuring Security on page 80 for more information.
RADIUS	Select a RADIUS profile from the drop-down list box, if you have a RADIUS server configured. If you do not need to use RADIUS authentication, ignore this field.
QoS	With Multi-ESS, the ZyAIR ignores the ToS in the packet headers and uses a single QoS priority level for all of an ESS's traffic. Select the Quality of Service priority for this ESS's traffic. See Table 10 on page 60 for more information on the priority levels.
L2 Isolation	Select Enable from the drop down list box to activate layer-2 isolation.
Enable MAC Filtering	Select Enable from the drop down list box to activate MAC address filtering.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

7.2.2 Second Rx VLAN ID

The ZyAIR tags Ethernet frames in VLAN 1 with VLAN ID 1 and tags Ethernet frames in VLAN 2 with VLAN ID 2. Both VLAN 1 and VLAN 2 have Internet access. VLAN 1 and VLAN 2 have access to a server. Ethernet frames forwarded from the server back to the switch are tagged. Ethernet frames are tagged with a second Rx VLAN ID (incoming VLAN ID). These incoming VLAN packets are forwarded to the ZyAIR. The ZyAIR matches the Second Rx VLAN ID with VLAN ID.

Figure 43 Second Rx VLAN ID Example



The following steps show you where to setup a Second Rx VLAN ID on the ZyAIR.

- 1 Click **WIRELESS** under **ADVANCED** in your web configurator and the SSID tab.
- 2 Click **Edit** in the **SSID** screen.
- 3 You can enter a **Second Rx VLAN ID** in the following screen. The following screen shows VLAN 1 tagged with VLAN ID 1. Incoming packets (Second Rx VLAN ID) with a VLAN ID 3 are matched to VLAN 1.

Figure 44 Configuring SSID: Second Rx VLAN ID Example

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Name :	SSID01						
SSID :	ZyXEL						
VLAN ID :	1						
Second Rx VLAN ID :	3						
Security :	security02						
RADIUS :	radius02						
QoS :	video						
L2 Isolation :	Enable						
Enable MAC Filtering :	Disable						
<input type="button" value="Apply"/> <input type="button" value="Reset"/>							

- 4 Click **Apply** to save these settings to the ZyAIR.

CHAPTER 8

Other Wireless Configurations

This chapter describes how to configure the **Layer-2 Isolation**, **MAC Filter** and **Roaming** screens on your ZyAIR.

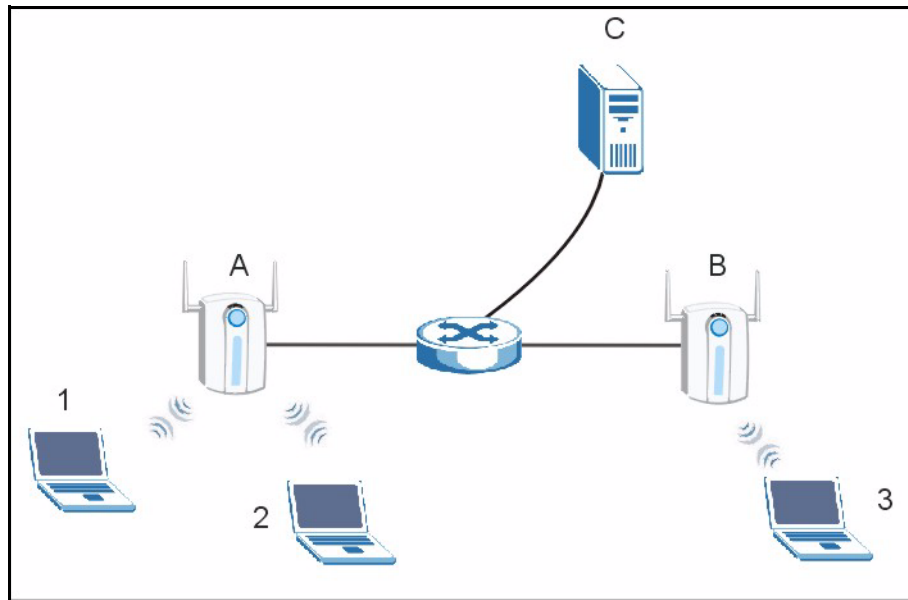
8.1 Layer-2 Isolation Introduction

Layer-2 isolation is used to prevent wireless clients associated with your ZyAIR from communicating with other wireless clients, AP's, computers or routers in a network.

In the following figure, A represents your ZyAIR, B represents an AP, C represents a server and 1, 2 and 3 represent wireless clients. If layer-2 isolation is enabled on the ZyAIR (A), then wireless clients 1 and 2 cannot communicate with B, C or 3. Wireless clients 1 and 2 cannot communicate with each other unless you enable Intra-BSS in the Wireless configuration screen.

Note: In the Wireless configuration screen, the Enable Intra-BSS Traffic check box is cleared when you enable layer-2 isolation.

If you want 1 and 2 to be able to communicate with C, B and/ or 3 then enter the MAC addresses of C, B and/or 3 in the Allow devices with these MAC addresses table.

Figure 45 Layer-2 Isolation Application

MAC addresses that are not listed in the Allow devices with these MAC addresses table are blocked from communicating with the ZyAIR's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS Traffic allows wireless clients associated with the same AP to communicate with each other.

8.2 Configuring Layer-2 Isolation

If layer-2 isolation is enabled, you need to know the MAC address of the wireless client, AP, computer or router that you want to allow to communicate with the ZyAIR's wireless clients.

To configure layer-2 isolation, click the **WIRELESS** link under **ADVANCED** and then the **Layer-2 Isolation** tab. The screen appears as shown next.

Figure 46 Layer-2 Isolation Configuration Screen

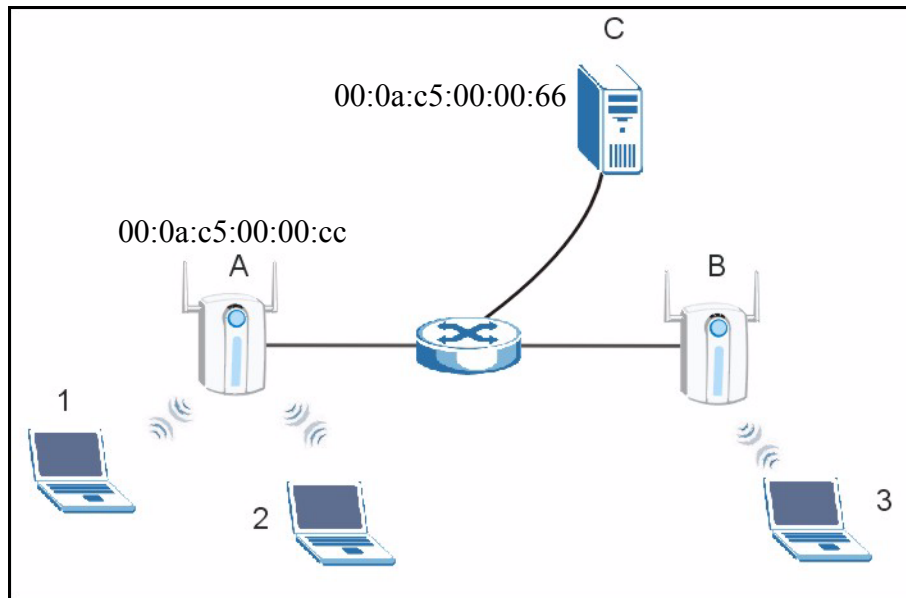
The following table describes the labels in this screen.

Table 31 Layer-2 Isolation Configuration

LABEL	DESCRIPTION
Enable Layer-2 Isolation	Select the Enable Layer-2 Isolation check box to enable layer-2 isolation on the ZyAIR. When you select the Enable Layer-2 Isolation check box and save this configuration screen, the Enable Intra-BSS Traffic check box in the Wireless configuration screen is cleared. This means that wireless clients connected to the ZyAIR cannot communicate with one another. This would be appropriate in a hotspot application, for example, in a hotel where wireless clients can access the Internet, but cannot communicate with other wireless clients or AP's. If you want wireless clients associated with the ZyAIR to be able to communicate with each other, you must select the Enable Intra-BSS Traffic check box in the Wireless configuration screen.
Allow devices with these MAC addresses	These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the ZyAIR can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table.
Set	This is the index number of the MAC address.
MAC Address	Type the MAC addresses of the wireless client, AP, computer or router that you want to allow the ZyAIR associated wireless clients to have access to in these address fields. Type the MAC address in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

8.2.1 Layer-2 Isolation Examples

The following section shows you example layer-2 isolation configurations on the ZyAIR (A).

Figure 47 Layer-2 Isolation Example

8.2.2 Layer-2 Isolation Example 1

In the following example wireless clients 1 and 2 cannot communicate with C, B or 3.

- Select the **Enable Layer-2 Isolation** check box, but do not configure any MAC addresses in the **Allow devices with these MAC addresses** table (1 and 2 cannot communicate with each other unless you enable Intra-BSS).

Figure 48 Layer-2 Isolation Example 1

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Layer-2 Isolation Configuration							
<input checked="" type="checkbox"/> Enable Layer-2 Isolation							
Allow devices with these MAC addresses							
Set	MAC Address		Set	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			
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			
				Apply		Reset	

8.2.3 Layer-2 Isolation Example 2

In the following example wireless clients 1 and 2 can communicate with C, but not B or 3.

- Select the **Enable Layer-2 Isolation** check box.
- Enter C's MAC address in the Allow devices with these MAC addresses field.

Figure 49 Layer-2 Isolation Example 2

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Layer-2 Isolation Configuration							
<input checked="" type="checkbox"/> Enable Layer-2 Isolation							
Allow devices with these MAC addresses							
Set	MAC Address			Set	MAC Address		
1	00:0a:c5:00:00:66			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		
<input type="button" value="Apply"/> <input type="button" value="Reset"/>							

8.2.4 Layer-2 Isolation Example 3

In the following example wireless clients 1 and 2 can communicate with B and C but not 3.

- Select the Enable Layer-2 Isolation check box.
- Configure more than one MAC address. Enter the server and your ZyAIR MAC addresses in the Allow devices with these MAC addresses fields.

Figure 50 Layer-2 Isolation Example 3

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter	Roaming	Local User Database
Layer-2 Isolation Configuration							
<input checked="" type="checkbox"/> Enable Layer-2 Isolation							
Allow devices with these MAC addresses							
Set	MAC Address		Set	MAC Address			
1	00:0a:c5:00:00:66		17	00:00:00:00:00:00			
2	00:0a:c5:00:00:cc		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			
<input type="button" value="Apply"/>				<input type="button" value="Reset"/>			

8.3 Configuring MAC Filter

The MAC filter screen allows you to configure the ZyAIR to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the ZyAIR (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 address of the devices to configure this screen.

To change your ZyAIR's MAC filter settings, click the **WIRELESS** link under **ADVANCED** and the **MAC Filter** tab. The screen appears as shown.

Figure 51 MAC Address Filter

The following table describes the labels in this screen.

Table 32 MAC Address Filter

LABEL	DESCRIPTION
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select Deny Association to block access to the router, MAC addresses not listed will be allowed to access the router. Select Allow Association to permit access to the router, MAC addresses not listed will be denied access to the router.
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 ZyAIR in these address fields.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

Note: To activate MAC filtering on a profile, select **Enable** from the **Enable MAC Filtering** drop-down list box in the SSID configuration screen and click **Apply**.

8.4 Configuring Roaming

A wireless station is a device with an IEEE 802.11b or an IEEE 802.11g compliant wireless interface. 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.

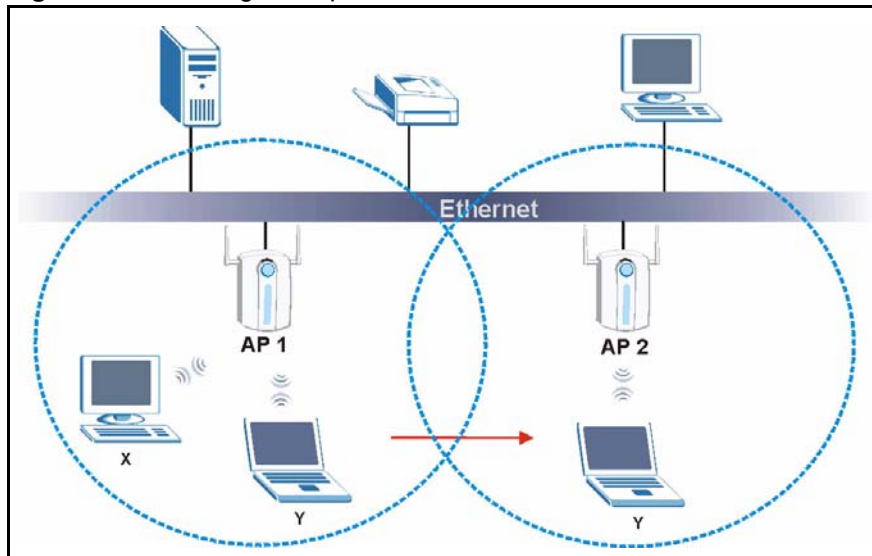
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending 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 52](#).

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). 802.1x authentication information is not exchanged (at the time of writing).

Figure 52 Roaming Example



The steps below describe the roaming process.

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

8.4.1 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.

To enable roaming on your ZyAIR, click the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

Figure 53 Roaming

The following table describes the labels in this screen.

Table 33 Roaming

LABEL	DESCRIPTION
Active	Select Yes from the drop-down list box to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 3517. Make sure this port is not used by other services.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 9

VLAN

This chapter discusses how to configure VLAN on the ZyAIR.

9.1 VLAN

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network can belong to one or more groups. Only stations within the same group can talk to each other.

The ZyAIR supports 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyAIR can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

9.1.1 Management VLAN ID

The Management VLAN ID identifies the “management VLAN”. A device must be a member of this “management VLAN” in order to access and manage the ZyAIR. If a device is not a member of this VLAN, then that device cannot manage the ZyAIR.

If no devices are in the management VLAN, then no one will be able to access the ZyAIR and you will have to restore the default configuration file.

9.1.2 VLAN Tagging

The ZyAIR supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyAIR can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

Note: You must connect the ZyAIR to a VLAN-aware device that is a member in the management VLAN in order to perform management. See the **Configuring Management VLAN Example** BEFORE you configure the **VLAN** screen.

9.2 Configuring VLAN

Click **ADVANCED** and then **VLAN**. The screen appears as shown next.

Figure 54 VLAN

VLAN

VIRTUAL LAN Setup

Enable VLAN Tagging

Management VLAN ID (1 ~ 4094)

VLAN Mapping Table

	Index	ID	Name
<input type="checkbox"/>	1	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	2	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	3	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	4	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	5	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	6	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	7	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	8	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	9	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	10	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	11	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	12	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	13	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	14	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	15	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>
<input type="checkbox"/>	16	<input type="text" value="1"/> (1 ~ 4094)	<input type="text" value="zyxel"/>

The following table describes the labels in this screen.

Table 34 VLAN

LABEL	DESCRIPTION
Enable VLAN Tagging	Select this check box to turn on VLAN tagging.
Management VLAN ID	Enter a number from 1 to 4094 to define this VLAN group. At least one device in your network must belong to this VLAN in order to manage the ZyAIR. Note: Mail and FTP servers must have the same management VLAN ID to communicate with the ZyAIR. See Configuring Management VLAN Example on page 115 for more information.
VLAN Mapping Table	Use this table to map names to VLAN IDs so that the RADIUS server can assign each user or user group a mapped VLAN ID. See the your RADIUS server documentation for more information on configuring VLAN ID attributes. See Configuring Microsoft's IAS Server Example on page 117 for more information.
Index	Select a check box to enable the VLAN mapping profile.
ID	Type a VLAN ID. Incoming traffic from the WLAN is authorized and assigned a VLAN ID by the RADIUS server before it is sent to the LAN. Note: This ID is NOT the same as the VLAN ID displayed in the SSID screen.

Table 34 VLAN

LABEL	DESCRIPTION
Name	Type a name to have the ZyAIR check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured Name field is checked against these attributes. If the configured Name field matches these attributes, the corresponding VLAN ID entry is used to access the specific VLAN group. If the configured Name field does not match the VLAN related attributes sent from the RADIUS server, a wireless station is assigned the associated SSID VLAN ID. See VLAN ID in the SSID screen.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

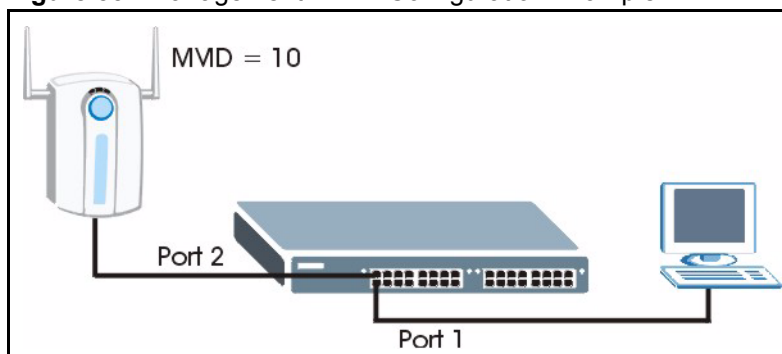
9.2.1 Configuring Management VLAN Example

This section shows you how to create a VLAN on an Ethernet switch.

By default, the port on the ZyAIR is a member of the management VLAN (VID 1). The following procedure shows you how to configure a tagged VLAN.

Note: Use the out-of-band management port or console port to configure the switch if you misconfigure the management VLAN and lock yourself out from performing in-band management.

On an Ethernet switch, create a VLAN that has the same management VLAN ID as the ZyAIR. The following figure has the ZyAIR connected to port 2 of the switch and your computer connected to port 1. The management VLAN ID is ten.

Figure 55 Management VLAN Configuration Example

Perform the following steps in the switch web configurator:

- 1** Click **VLAN** under **Advanced Application**.
- 2** Click **Static VLAN**.
- 3** Select the **ACTIVE** check box.
- 4** Type a **Name** for the VLAN ID.

- 5 Type a **VLAN Group ID**. This should be the same as the management VLAN ID on the ZyAIR.
- 6 Enable **Tx Tagging** on the port which you want to connect to the ZyAIR. Disable **Tx Tagging** on the port you are using to connect to your computer.
- 7 Under **Control**, select **Fixed** to set the port as a member of the VLAN.

Figure 56 VLAN-Aware Switch - Static VLAN

Port	Control	Tagging
1	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

- 8 Click **Apply**. The following screen displays.

Figure 57 VLAN-Aware Switch

VID	Active	Name	Delete
10	Yes	VID1	<input type="checkbox"/>
2	Yes	2	<input type="checkbox"/>
3	Yes	3	<input type="checkbox"/>
4	Yes	VLAN4	<input type="checkbox"/>
5	Yes	ctn-test	<input type="checkbox"/>

- 9 Click **VLAN Status** to display the following screen.

Figure 58 VLAN-Aware Switch - VLAN Status

Index	VID	Port Number																									Elapsed Time	Status	
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	S2			S1
1	10	T	-	-	-	-	-	-	T	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static
2	2	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static	
3	3	T	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static	
4	4	-	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:27	Static	
5	5	-	-	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:27	Static	

Follow the instructions in the Quick Start Guide to set up your ZyAIR for configuration. The ZyAIR should be connected to the VLAN-aware switch. In the above example, the switch is using port 1 to connect to your computer and port 2 to connect to the ZyAIR: [see Figure 55](#).

- 1 In the ZyAIR web configurator click **VLAN** under **ADVANCED** to open the VLAN setup screen.
- 2 Select the **Enable VLAN Tagging** check box and type a **Management VLAN ID** (10 in this example) in the field provided.

3 Click Apply.

Figure 59 VLAN Setup

VLAN

VIRTUAL LAN Setup

Enable VLAN Tagging

Management VLAN ID: 10 (1 ~ 4094)

VLAN Mapping Table

Index	ID	Name
1	1 (1 ~ 4094)	zyxel
2	1 (1 ~ 4094)	zyxel
3	1 (1 ~ 4094)	zyxel
4	1 (1 ~ 4094)	zyxel
5	1 (1 ~ 4094)	zyxel
6	1 (1 ~ 4094)	zyxel
7	1 (1 ~ 4094)	zyxel
8	1 (1 ~ 4094)	zyxel
9	1 (1 ~ 4094)	zyxel
10	1 (1 ~ 4094)	zyxel
11	1 (1 ~ 4094)	zyxel
12	1 (1 ~ 4094)	zyxel
13	1 (1 ~ 4094)	zyxel
14	1 (1 ~ 4094)	zyxel
15	1 (1 ~ 4094)	zyxel
16	1 (1 ~ 4094)	zyxel

Apply Reset

4 The ZyAIR attempts to connect with a VLAN-aware device. You can now access and manage the ZyAIR through the Ethernet switch.

Note: If you do not connect the ZyAIR to a correctly configured VLAN-aware device, you will lock yourself out of the ZyAIR. If this happens, you must reset the ZyAIR to access it again.

9.2.2 Configuring Microsoft's IAS Server Example

Dynamic VLAN assignment can be used with the ZyAIR. Dynamic VLAN assignment allows network administrators to assign a specific VLAN (configured on the ZyAIR) to an individual's Windows User Account. When a wireless station is successfully authenticated to the network, it is automatically placed into its respective VLAN.

ZyXEL uses the following standard RADIUS attributes returned from Microsoft's IAS RADIUS service to place the wireless station into the correct VLAN:

Table 35 Standard RADIUS Attributes

ATTRIBUTE NAME	TYPE	VALUE
Tunnel-Type	064	13 (decimal) – VLAN
Tunnel-Medium-Type	065	6 (decimal) – 802
Tunnel-Private-Group-ID	081	<vlan-name> (string) – either the Name you enter in the ZyAIR VLAN screen or the number. See Figure 71 on page 125 .

The following occurs under Dynamic VLAN Assignment:

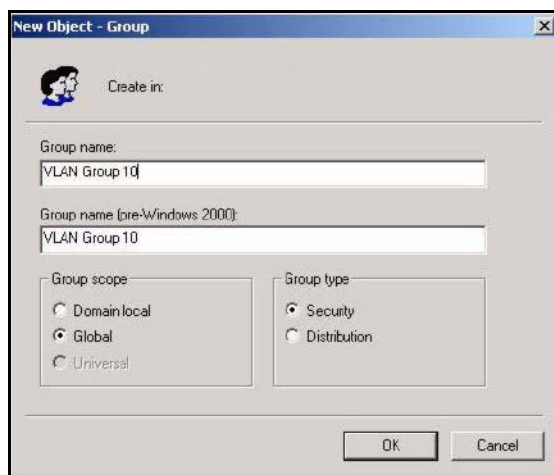
- 1 When you configure your wireless credentials, the ZyAIR sends the information to the IAS server using RADIUS protocol.
- 2 Authentication by the RADIUS server is successful.
- 3 The RADIUS server sends three attributes related to this feature.
- 4 The ZyAIR compares these attributes with the VLAN screen mapping table.
 - a If the **Name**, if for example VLAN 20 is found, the mapped VLAN ID is used. If it is not found in the mapping table
 - b the string in the **Tunnel-Private-Group-ID** attribute is considered as a number ID format, for example 2493. The range of the number ID (Name:string) is between 1 and 4094.
 - c If a or b are not matched, the ZyAIR uses the VLAN ID configured in the **SSID** screen and the wireless station. This **VLAN ID** is independent and hence different to the **ID** in the VLAN screen.

9.2.2.1 Configuring VLAN Groups

To configure a VLAN group you must first define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group.

- 1 Using the Active Directory Users and Computers administrative tool, create the VLAN Groups that will be used for each VLAN ID. One VLAN Group must be created for each VLAN defined on the ZyAIR. The VLAN Groups must be created as Global/Security groups.
 - Type a name for the **VLAN Group** that describes the VLAN Group's function.
 - Select the **Global** Group scope parameter check box.
 - Select the **Security** Group type parameter check box.
 - Click **OK**.

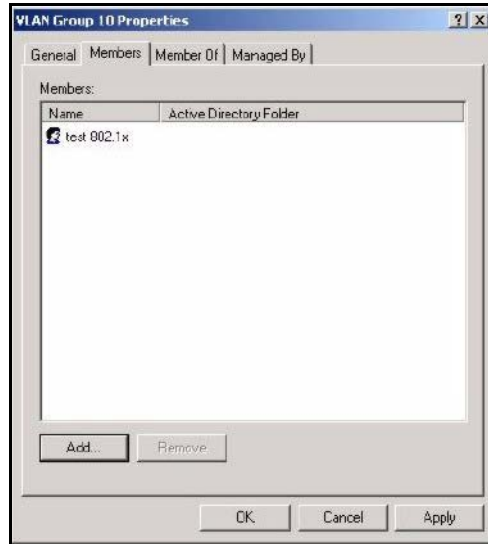
Figure 60 New Global Security Group



- 2 In **VLAN Group ID Properties**, click the **Members** tab.

- The IAS uses group memberships to determine which user accounts belong to which VLAN groups. Click the **Add** button and configure the VLAN group details.
- 3** Repeat the previous step to add each VLAN group required.

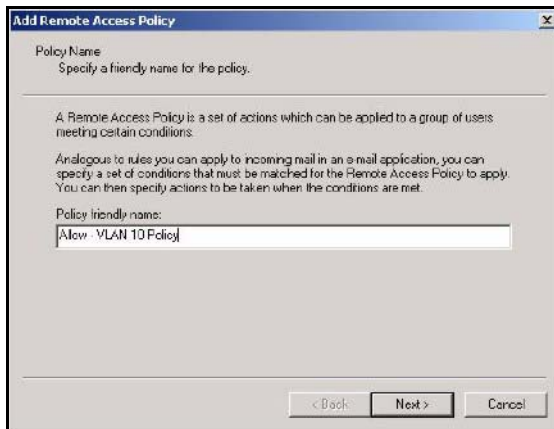
Figure 61 Add Group Members



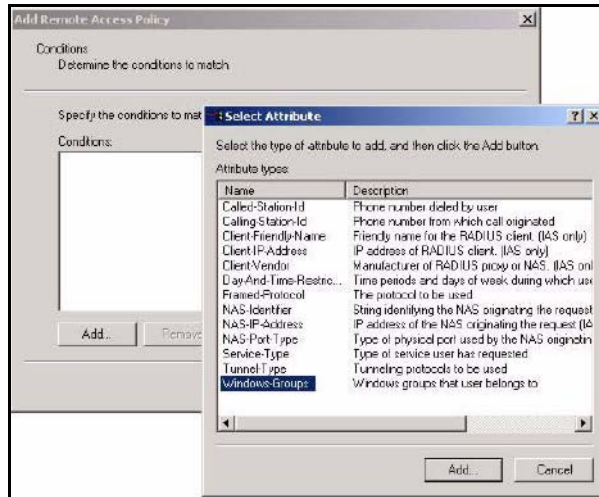
9.2.2.2 Configuring Remote Access Policies

Once the VLAN Groups have been created, the IAS Remote Access Policy needs to be defined. This allows the IAS to compare the user account being authenticated against the group memberships of each VLAN Group.

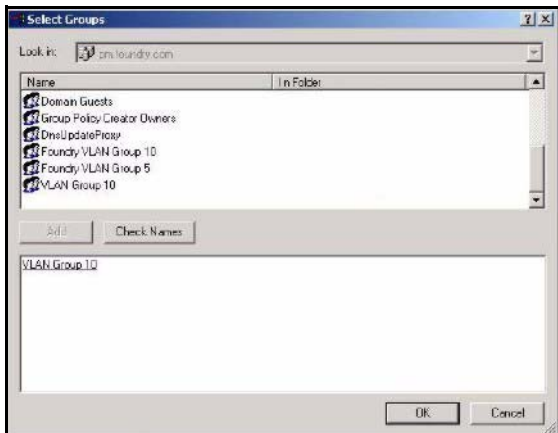
- 1** Using the **Remote Access Policy** option on the Internet Authentication Service management interface, create a new VLAN Policy for each VLAN Group defined in the previous section. The order of the remote access policies is important. The most specific policies should be placed at the top of the policy list and the most general at the bottom. For example, if the Day-And-Time Restriction policy is still present, it should be moved to the bottom or deleted to allow the VLAN Group policies to take precedence.
- Right click **Remote Access Policy** and select **New Remote Access Policy**.
 - Enter a **Policy friendly name** that describes the policy. Each Remote Access Policy will be matched to one VLAN Group. An example may be, **Allow - VLAN 10 Policy**.
 - Click **Next**.

Figure 62 New Remote Access Policy for VLAN Group

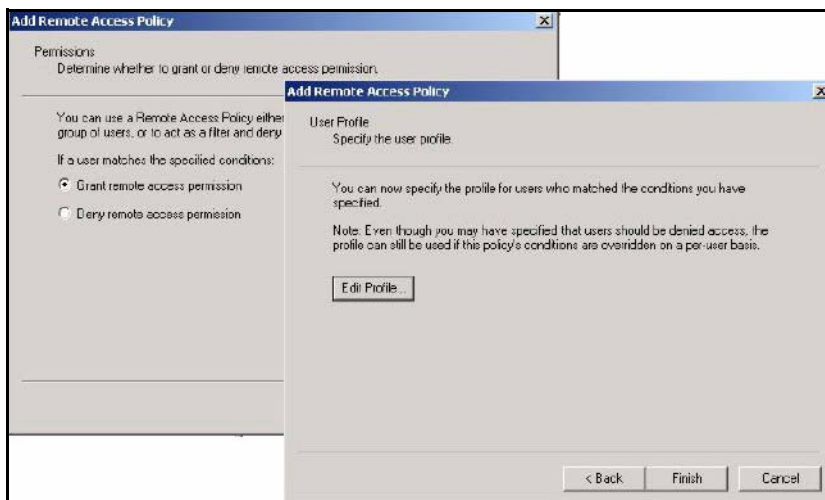
- 2** The **Conditions** window displays. Select **Add** to add a condition for this policy to act on.
- 3** In the **Select Attribute** screen, click **Windows-Groups** and the **Add** button.

Figure 63 Specifying Windows-Group Condition

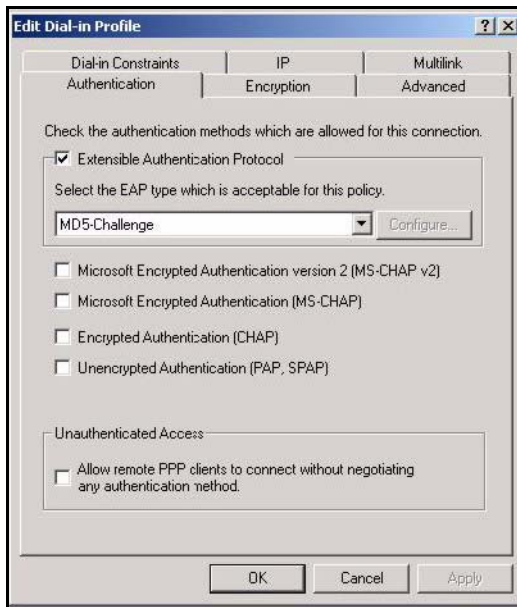
- 4** The **Select Groups** window displays. Select a remote access policy and click the **Add** button. The policy is added to the field below. Only one VLAN Group should be associated with each policy.
- 5** Click **OK** and **Next** in the next few screens to accept the group value.

Figure 64 Adding VLAN Group

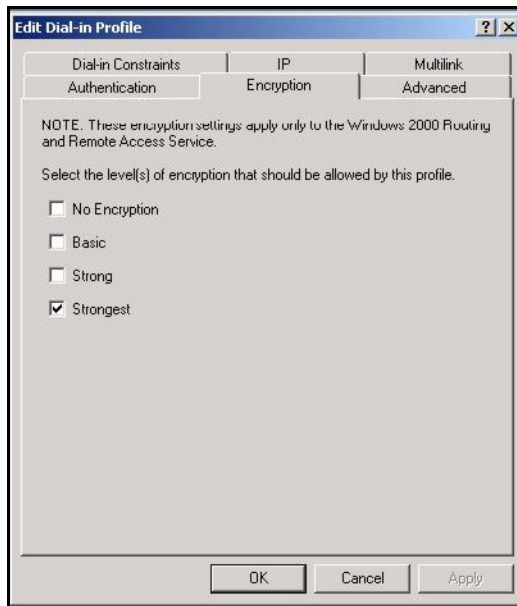
- 6** When the **Permissions** options screen displays, select **Grant remote access permission**.
- Click **Next** to grant access based on group membership.
 - Click the **Edit Profile** button.

Figure 65 Granting Permissions and User Profile Screens

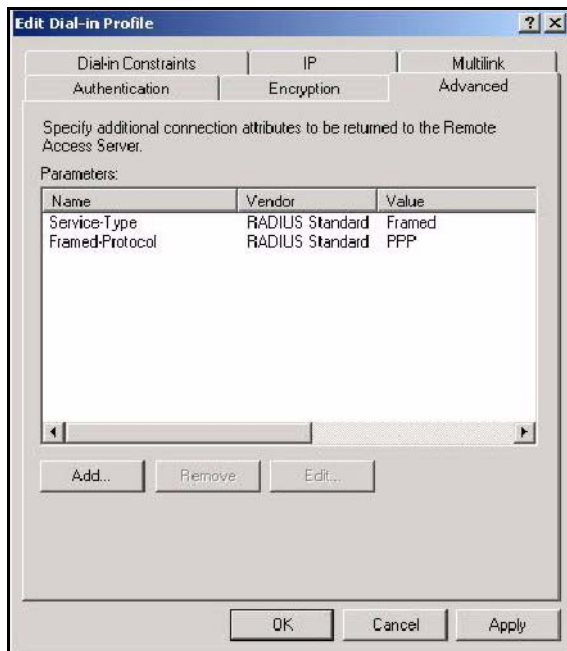
- 7** The **Edit Dial-in Profile** screen displays. Click the **Authentication** tab and select the **Extensible Authentication Protocol** check box.
- Select an EAP type depending on your authentication needs from the drop-down list box.
 - Clear the check boxes for all other authentication types listed below the drop-down list box.

Figure 66 Authentication Tab Settings

- 8** Click the **Encryption** tab. Select the **Strongest** encryption option. This step is not required for EAP-MD5, but is performed as a safeguard.

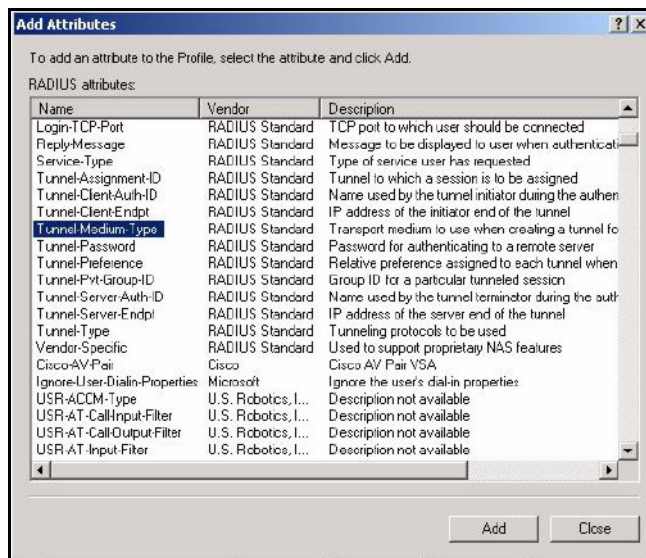
Figure 67 Encryption Tab Settings

- 9** Click the **IP** tab and select the **Client may request an IP address** check box for DHCP support.
- 10** Click the **Advanced** tab. The current default parameters returned to the ZyAIR should be **Service-Type** and **Framed-Protocol**.
- Click the **Add** button to add an additional three RADIUS VLAN attributes required for 802.1X Dynamic VLAN Assignment.

Figure 68 Connection Attributes Screen

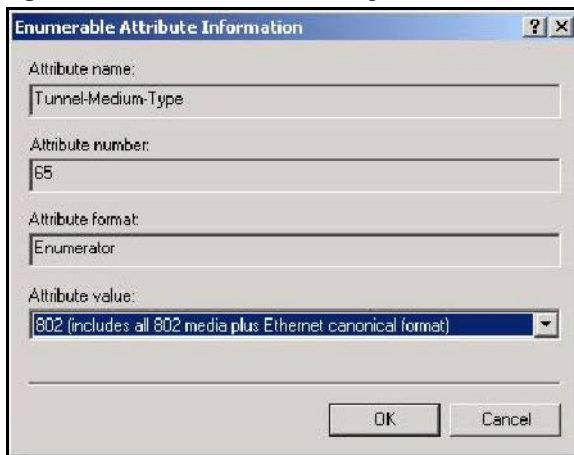
11The RADIUS Attribute screen displays. From the list, three RADIUS attributes will be added:

- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID
- Tunnel-Type
- Click the **Add** button
- Select **Tunnel-Medium-Type**
- Click the **Add** button.

Figure 69 RADIUS Attribute Screen

12 The **Enumerable Attribute Information** screen displays. Select the **802** value from the **Attribute value** drop-down list box.

- Click **OK**.

Figure 70 802 Attribute Setting for Tunnel-Medium-Type

13 Return to the **RADIUS Attribute Screen** shown as [Figure 69](#) on page 124.

- Select **Tunnel-Pvt-Group-ID**.
- Click **Add**.

14 The **Attribute Information** screen displays.

- In the **Enter the attribute value in:** field select **String** and type a number in the range 1 to 4094 or a **Name** for this policy. This **Name** should match a name in the VLAN mapping table on the ZyAIR. Wireless stations belonging to the VLAN Group specified in this policy will be given a VLAN **ID** specified in the ZyAIR VLAN table.
- Click **OK**.

Figure 71 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID

The screenshot shows a dialog box titled "Attribute Information". It contains the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in: String Hexadecimal
- Value field: 10
- Buttons: OK, Cancel

15Return to the **RADIUS Attribute Screen** shown as [Figure 69 on page 124](#).

- Select **Tunnel-Type**.
- Click **Add**.

16The **Enumerable Attribute Information** screen displays.

- Select **Virtual LANs (VLAN)** from the attribute value drop-down list box.
- Click **OK**.

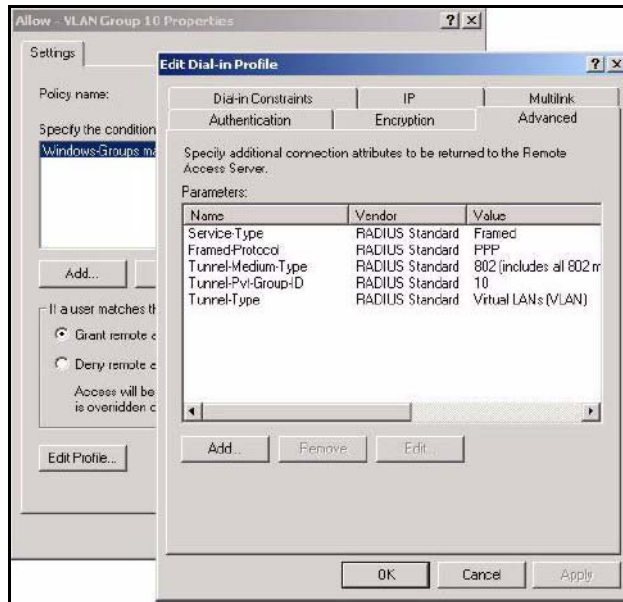
Figure 72 VLAN Attribute Setting for Tunnel-Type

The screenshot shows a dialog box titled "Enumerable Attribute Information". It contains the following fields and controls:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute value: Virtual LANs (VLAN) (selected in a drop-down menu)
- Buttons: OK, Cancel

17Return to the **RADIUS Attribute Screen** shown as [Figure 69 on page 124](#).

- Click the **Close** button.
- The completed **Advanced** tab configuration should resemble the following screen.

Figure 73 Completed Advanced Tab

Note: Repeat the **Configuring Remote Access Policies** procedure for each VLAN Group defined in the Active Directory. Remember to place the most general Remote Access Policies at the bottom of the list and the most specific at the top of the list.

CHAPTER 10

IP Screen

This chapter discusses how to configure IP on the ZyAIR

10.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyAIR are preset in the factory with the following values:

- 1 IP address of 192.168.1.2
- 2 Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

10.2 TCP/IP Parameters

10.2.1 IP Address and Subnet Mask

Refer to the [IP Address and Subnet Mask](#) section in the [Wizard Setup](#) chapter for this information.

10.2.2 WAN 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 36 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.

10.3 Configuring IP

Click **ADVANCED** and then **IP** to display the screen shown next.

Figure 74 IP Setup

The following table describes the labels in this screen.

Table 37 IP Setup

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyAIR is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again.
Use fixed IP address	Select this option if your ZyAIR is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation. Note: If you change the ZyAIR's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over the WAN, the gateway must be the IP address of one of the remote node.
Apply	Click Apply to save your changes back to the ZyAIR.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 11

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

11.1 Certificates Overview

The ZyAIR can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyAIR to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyAIR uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyAIR does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyAIR can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

11.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyAIR only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

11.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the ZyAIR act as a certification authority and sign its own certificates.

11.3 Configuration Summary

This section summarizes how to manage certificates on the ZyAIR.

Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyAIRs' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the ZyAIR.

11.4 My Certificates

Click **CERTIFICATES**, **My Certificates** to open the ZyAIR's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 75 My Certificates

My Certificates Trusted CAs

PKI Storage Space in Use

0% 1% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyAIR models. Click Replace to create a certificate using your ZyAIR's MAC address that will be specific to this device.

Replace

My Certificates Setting

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-3000 Factory Default Certificate	CN=ZyAIR G-3000 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

Details Create Import Delete Refresh

The following table describes the labels in this screen.

Table 38 My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyAIR's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyAIR has the factory default certificate. The factory default certificate is common to all ZyAIRs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyAIR's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. *SELF represents the default self-signed certificate, which the ZyAIR uses to sign imported trusted remote host certificates. CERT represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

Table 38 My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Details	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows *SELF in the Type field.</p> <ol style="list-style-type: none"> 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the *SELF certificate. 2. Click the details icon next to another self-signed certificate (see the description on the Create button if you need to create a self-signed certificate). 3. Select the Default self-signed certificate which signs the imported remote host certificates check box. 4. Click Apply to save the changes and return to the My Certificates screen. 5. The certificate that originally showed *SELF displays SELF and you can delete it now. <p>Note that subsequent certificates move up by one when you take this action</p>
Create	Click Create to go to the screen where you can have the ZyAIR generate a certificate or a certification request.
Import	Click Import to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyAIR.
Delete	Click Delete to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click Refresh to display the current validity status of the certificates.

11.5 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyAIR currently allows the importation of a PKCS#7 file that contains a single certificate.

- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

11.6 Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyAIR, see the following figure.

Note: You can only import a certificate that matches a corresponding certification request that was generated by the ZyAIR.

Note: The certificate you import replaces the corresponding request in the My Certificates screen.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 76 My Certificate Import

The following table describes the labels in this screen.

Table 39 My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyAIR.
Cancel	Click Cancel to quit and return to the My Certificates screen.

11.7 Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyAIR create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

Figure 77 My Certificate Create

The following table describes the labels in this screen.

Table 40 My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.

Table 40 My Certificate Create (continued)

LABEL	DESCRIPTION
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyAIR drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyAIR drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyAIR drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select Create a self-signed certificate to have the ZyAIR generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select Create a certification request and save it locally for later manual enrollment to have the ZyAIR generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see the My Certificate Details section) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select Create a certification request and enroll for a certificate immediately online to have the ZyAIR generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the Trusted CAs screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the CA Certificate drop-down list box. You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the ZyAIR's list of certificates of trusted certification authorities.
Request Authentication	When you select Create a certification request and enroll for a certificate immediately online , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just fill in the Key field if your certification authority uses the SCEP enrollment protocol.

Table 40 My Certificate Create (continued)

LABEL	DESCRIPTION
Key	Type the key that the certification authority gave you.
Apply	Click Apply to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyAIR is generating the self-signed certificate or certification request.

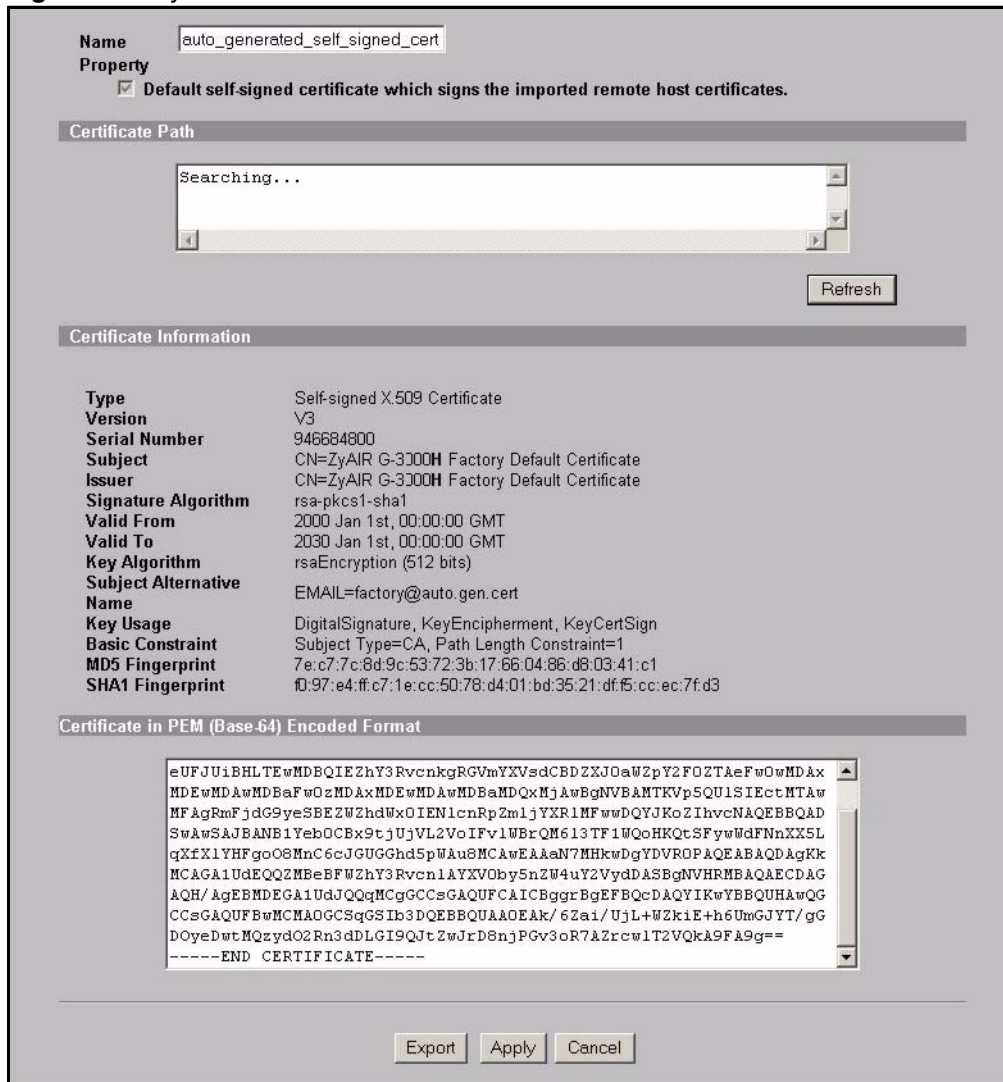
After the ZyAIR successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyAIR enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyAIR to enroll a certificate online.

11.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see [Figure 75](#)). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyAIR uses to sign the trusted remote host certificates that you import to the ZyAIR.

Figure 78 My Certificate Details



The following table describes the labels in this screen.

Table 41 My Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyAIR use this certificate to sign the trusted remote host certificates that you import to the ZyAIR. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.

Table 41 My Certificate Details (continued)

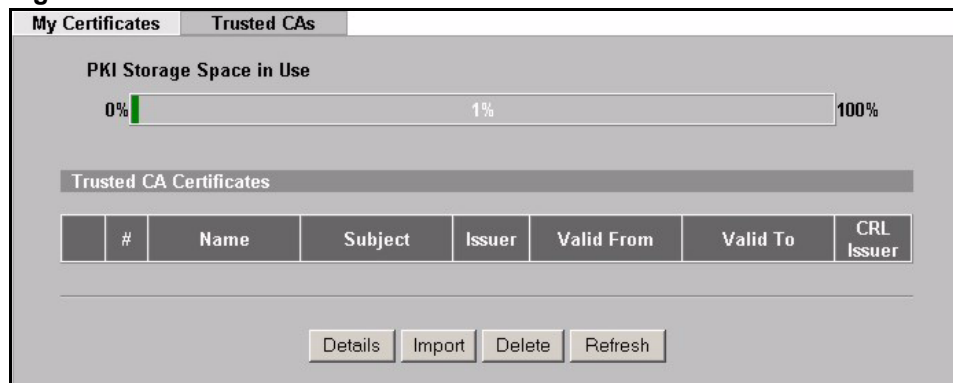
LABEL	DESCRIPTION
Certificate Path	Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyAIR does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyAIR.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyAIR uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyAIR uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the MD5 algorithm.

Table 41 My Certificate Details (continued)

LABEL	DESCRIPTION
SHA1 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes back to the ZyAIR. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click Cancel to quit and return to the My Certificates screen.

11.9 Trusted CAs

Click **CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyAIR to accept as trusted. The ZyAIR accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

Figure 79 Trusted CAs

The following table describes the labels in this screen.

Table 42 Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyAIR's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the Issues certificate revocation lists (CRL) check box in the certificate's details screen to have the ZyAIR check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Details	Click Details to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyAIR to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyAIR.

Table 42 Trusted CAs (continued)

LABEL	DESCRIPTION
Delete	Click Delete to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click this button to display the current validity status of the certificates.

11.10 Importing a Trusted CA's Certificate

Click **CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyAIR, see the following figure.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 80 Trusted CA Import

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

The following table describes the labels in this screen.

Table 43 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the ZyAIR.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

11.11 Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyAIR to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 81 Trusted CA Details

Name: auto_generated_self_signed_cert

Property: Default self-signed certificate which signs the imported remote host certificates.

Certificate Path: Searching... Refresh

Certificate Information

Type: Self-signed X.509 Certificate
Version: V3
Serial Number: 946684800
Subject: CN=ZyAIR G-3000H Factory Default Certificate
Issuer: CN=ZyAIR G-3000H Factory Default Certificate
Signature Algorithm: rsa-pkcs1-sha1
Valid From: 2000 Jan 1st, 00:00:00 GMT
Valid To: 2030 Jan 1st, 00:00:00 GMT
Key Algorithm: rsaEncryption (512 bits)
Subject Alternative Name: EMAIL=factory@auto.gen.cert
Key Usage: DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint: Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint: 7e:c7:7c:8d:9c:53:72:3b:17:66:04:66:d8:03:41:c1
SHA1 Fingerprint: f0:97:e4:ff:c7:1e:cc:50:78:d4:01:bd:35:21:df:f5:cc:ec:7f:d3

Certificate in PEM (Base-64) Encoded Format

```
eUFJU1BHLTEwMDBQIEZhy3RvcnkgRGVmYXVsdCBDZXJoaWZpY2FOZTAeFw0wMDAx
MDEwMDAwMDEBaFw0zMDAxMDEwMDAwMDEBaMDQxMjAwBgNVBAHTKp5QU1SIEctHTAw
MFAgRmFjdG9yeSBEZWZhdWx0IENlcnRpZmljYXR1MFwwDQYJKoZIhvcNAQEBBQAD
SwAwSAJBANB1YebOCBx9tjUjVL2VoIFv1WBrQM613TF1WQoHKQtSFywUdFNnXX5L
qXfX1YHFgoOSMnCcJGUGhd5pWAu8MCAwEAAN7MHkwDgYDVROPAQEABADAgKk
MCAGA1UdEQQZMBEwBFwZhy3Rvcn1AYXV0by5nZW4uY2VydASBgNVHRMBAQAECDAG
AQH/AgEBMDEGA1UdJQQgMCgGCCsGAQUFCAICBggrBgEFBQcDAQYIKwYBBQUHAWQG
CCsGAQUFBwMCAAGCSqGSIb3DQEBBQUAA0EAK/6Za1/UjL+WZkiE+h6UmGJYT/gG
DOyDwtMQzydO2Rn3dDLGI9QJtZwJrD8njPGv3oR7AZrcw1T2VQkA9FA9g==
-----END CERTIFICATE-----
```

Export Apply Cancel

The following table describes the labels in this screen.

Table 44 Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyAIR use this certificate to sign the trusted remote host certificates that you import to the ZyAIR. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.

Table 44 Trusted CA Details (continued)

LABEL	DESCRIPTION
Certificate Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyAIR does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyAIR uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

Table 44 Trusted CA Details (continued)

LABEL	DESCRIPTION
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyAIR calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes back to the ZyAIR. You can only change the name and/or set whether or not you want the ZyAIR to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

CHAPTER 12

Remote Management Screens

This chapter provides information on the Remote Management screens.

12.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyAIR interface (if any) from which computers.

You may manage your ZyAIR from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyAIR automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Telnet
- 2 HTTP

12.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

12.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

12.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyAIR automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

12.2 Configuring WWW

To change your ZyAIR's World Wide Web settings, click **REMOTE MGNT** to display the **WWW** screen.

Figure 82 Remote Management: WWW

TELNET	FTP	WWW	SNMP
HTTPS			
Server Certificate	auto_generated_self_signed_cert (See My Certificates)		
<input type="checkbox"/> Authenticate Client Certificates (See Trusted CAs)			
Server Port	443		
Server Access	WLAN & LAN		
Secured Client IP Address	<input checked="" type="radio"/> All <input type="radio"/> Selected	0.0.0.0	
WWW			
Server Port	80		
Server Access	WLAN & LAN		
Secured Client IP Address	<input checked="" type="radio"/> All <input type="radio"/> Selected	0.0.0.0	
Apply		Reset	

The following table describes the labels in this screen.

Table 45 Remote Management: WWW

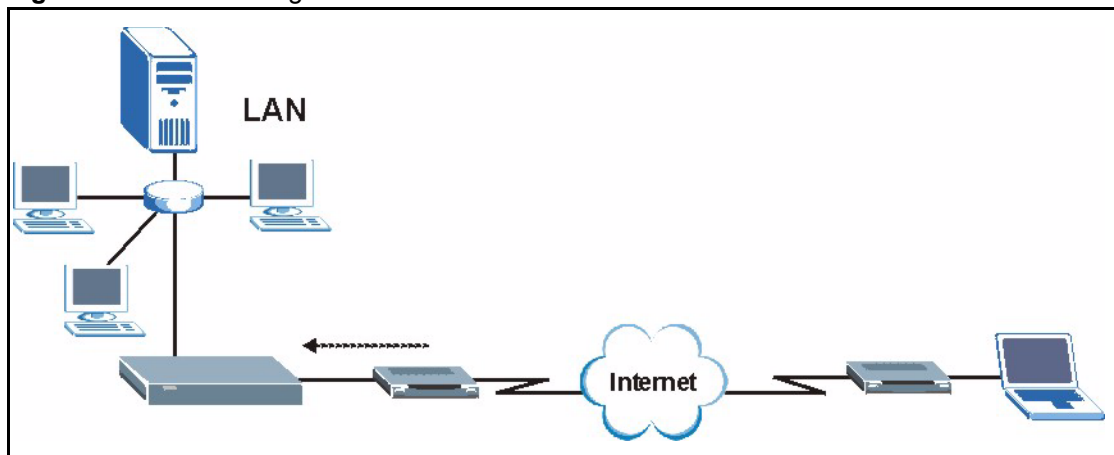
LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the Server Certificate that the ZyAIR will use to identify itself. The ZyAIR is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyAIR).
Authenticate Client Certificates	Select Authenticate Client Certificates (optional) to require the SSL client to authenticate itself to the ZyAIR by sending the ZyAIR a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyAIR (see the appendix on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyAIR, for example 8443, then you must notify people who need to access the ZyAIR web configurator to use "https://ZyAIR IP Address: 8443 " as the URL.
Server Access	Select a ZyAIR interface from Server Access on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the HTTP Server Access field to Disable and setting the HTTPS Server Access field to an interface(s).
Secured Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
WWW	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 45 Remote Management: WWW

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.3 Configuring Telnet

You can configure your ZyAIR for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the ZyAIR.

Figure 83 Telnet Configuration on a TCP/IP Network

12.4 Configuring TELNET

Click **REMOTE MGNT** and the **TELNET** tab to display the screen as shown.

Figure 84 Remote Management: Telnet

The screenshot shows a configuration interface for Telnet. At the top, there are four tabs: TELNET, FTP, WWW, and SNMP. The TELNET tab is selected. Below the tabs, there is a header bar with the word 'TELNET'. The main area contains three configuration items: 'Server Port' with a text box containing '23'; 'Server Access' with a dropdown menu showing 'WLAN & LAN'; and 'Secured Client IP Address' with two radio buttons, 'All' (which is selected) and 'Selected', followed by a text box containing '0.0.0.0'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 46 Remote Management: Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.5 Configuring FTP

You can upload and download the ZyAIR’s firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyAIR’s FTP settings, click **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

Figure 85 Remote Management: FTP

The following table describes the labels in this screen.

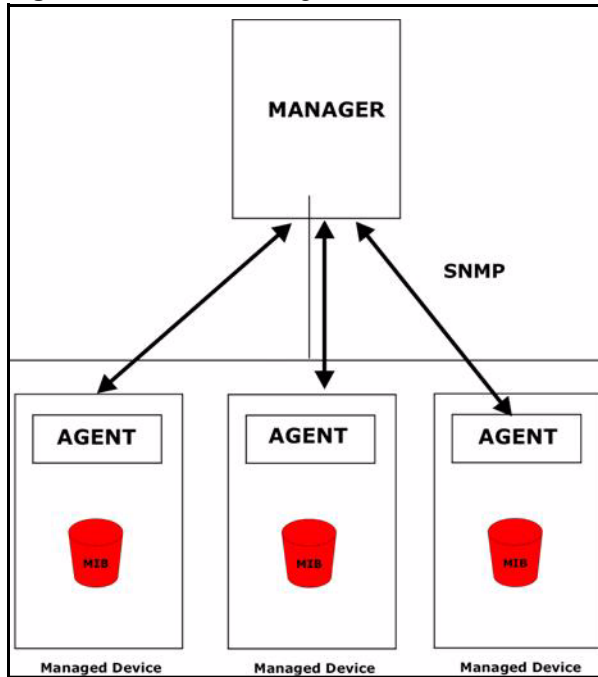
Table 47 Remote Management: FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

12.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Note: SNMP is only available if TCP/IP is configured.

Figure 86 SNMP Management Model

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyAIR). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

12.6.1 Supported MIBs

The ZyAIR supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

12.6.2 SNMP Traps

The ZyAIR can send the following traps to the SNMP manager.

Table 48 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure (defined in <i>RFC-1215</i>)	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.
pwStaAssociation	1.3.6.1.4.1.890.1.9.2.3.1.1	This trap is sent when a wireless client has successfully connected to the AP. The MAC address of the wireless client and the ESSID are listed.
pwWlanStaDisassociation	1.3.6.1.4.1.890.1.9.2.3.1.2	This trap is sent when a wireless client has disconnected from the AP. The MAC address of the wireless client and the ESSID are listed.

Table 48 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
pwWlanStaAuthFail	1.3.6.1.4.1.890.1.9.2.3.2.1	This trap is sent when a wireless client has failed to connect to the AP. The MAC address of the wireless client, the ESSID and the reason are listed.
pwTFTPStatus	1.3.6.1.4.1.890.1.9.2.3.3.1	This trap is sent to indicate the status and result of a TFTP client session that has ended.

12.7 SNMP Traps

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyAIR's physical ports.

Table 49 SNMP Interface Index to Physical Port Mapping

INTERFACE TYPE	PHYSICAL PORT
enet0	WLAN
enet1	Ethernet port

12.7.1 Configuring SNMP

To change your ZyAIR's SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

Figure 87 Remote Management: SNMP

The screenshot shows a web-based configuration interface for SNMP. At the top, there are navigation tabs: TELNET, FTP, WWW, and SNMP. The main content area is titled "SNMP Configuration" and contains several input fields: "Get Community" (public), "Set Community" (public), "Community" (public), and "Destination" (0.0.0.0). Below this is a section titled "SNMP" with "Service Port" (161), "Service Access" (WLAN & LAN), and "Secured Client IP Address" (All selected, 0.0.0.0). At the bottom, there are "Apply" and "Reset" buttons.

The following table describes the labels in this screen.

Table 50 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyAIR using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyAIR using this service. Select All to allow any computer to access the ZyAIR using this service. Choose Selected to just allow the computer with the IP address that you specify to access the ZyAIR using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

CHAPTER 13

Log Screens

This chapter contains information about configuring general log settings and viewing the ZyAIR's logs. Refer to the appendix for example log message explanations.

13.1 Configuring View Log

The web configurator allows you to look at all of the ZyAIR's logs in one location.

Click the **LOGS** links under **ADVANCED** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Figure 89](#)). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.

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

Figure 88 View Log

#	Time ▲	Message	Source	Destination	Notes
1	01/01/2000 00:03:20	Successful HTTP login	192.168.1.29		User:admin

The following table describes the labels in this screen.

Table 51 View Log

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select All Logs . The number of categories shown in the drop down list box depends on the selection in the Log Settings page.
Time	This field displays the time the log was recorded.
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.
Destination	This field lists the destination IP address and the port number of the incoming packet.

Table 51 View Log

LABEL	DESCRIPTION
Notes	This field displays additional information about the log entry.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page.
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to clear all the logs.

13.2 Configuring Log Settings

To change your ZyAIR's log settings, click the **LOGS** links under **ADVANCED** and then the **Log Settings** tab. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyAIR is to send the logs; the schedule for when the ZyAIR is to send the logs and which logs and/or immediate alerts the ZyAIR is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Figure 89 Log Settings

The following table describes the labels in this screen.

Table 52 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyAIR sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	

Table 52 Log Settings

LABEL	DESCRIPTION
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	<p>This field is only available when you select Weekly in the Log Schedule field. Use the drop down list box to select which day of the week to send the logs.</p>
Time for Sending Log	<p>Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.</p>
Clear log after sending mail	<p>Select the check box to clear all logs after logs and alert messages are sent via e-mail.</p>
Log	<p>Select the categories of logs that you want to record.</p>
Send Immediate Alert	<p>Select the categories of alerts for which you want the ZyAIR to immediately send e-mail alerts.</p>
Apply	<p>Click Apply to save your customized settings and exit this screen.</p>
Reset	<p>Click Reset to reconfigure all the fields in this screen.</p>

CHAPTER 14

Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

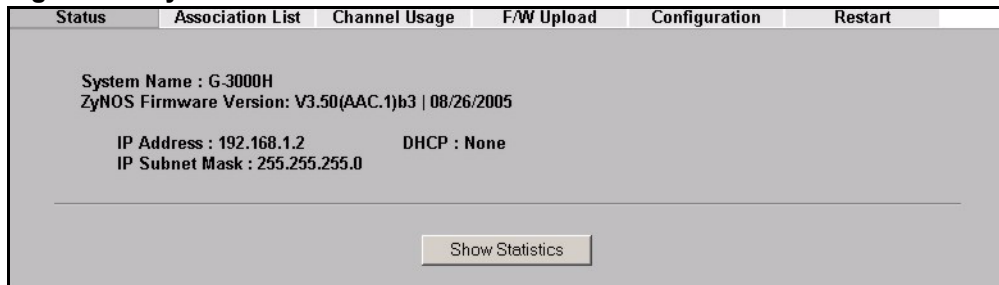
14.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyAIR.

14.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can use to monitor your ZyAIR. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 90 System Status



The following table describes the labels in this screen.

Table 53 System Status

LABEL	DESCRIPTION
System Name	This is the System Name you enter in the first Internet Access Wizard screen. It is for identification purposes
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
IP Address	This is the Ethernet port IP address.
IP Subnet Mask	This is the Ethernet port subnet mask.
DHCP	This is the Ethernet port DHCP role - Client or None .
Show Statistics	Click Show Statistics to see router performance statistics such as number of packets sent and number of packets received for each port.

14.2.1 System Statistics

Read-only information here includes port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable.

Figure 91 System Status: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	1963	1251	0	1226	838	0:33:35
WLAN	54M	1303	0	0	0	0	0:35:07

Bridge Link #	Active	Remote Bridge MAC Address	Status	TxPkts	RxPkts
1	No	00:00:00:00:00:00	Down	0	0
2	No	00:00:00:00:00:00	Down	0	0
3	No	00:00:00:00:00:00	Down	0	0
4	No	00:00:00:00:00:00	Down	0	0
5	No	00:00:00:00:00:00	Down	0	0

System Up Time : 0:35:12

Poll Interval(s) : sec

The following table describes the labels in this screen.

Table 54 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet or wireless port.
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. This shows the transmission speed only for wireless port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.
Bridge Link #	This is the index number of the bridge connection.
Active	This shows whether the bridge connection is activated or not.
Remote Bridge MAC Address	This is the MAC address of the peer device in bridge mode.
Status	This shows the current status of the bridge connection, which can be Up or Down .

Table 54 System Status: Show Statistics

LABEL	DESCRIPTION
TxPkts	This is the number of transmitted packets on the wireless bridge.
RxPkts	This is the number of received packets on the wireless bridge.
System Up Time	This is the total time the ZyAIR 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.

14.3 Association List

View the wireless stations that are currently associated to the ZyAIR in the **Association List** screen.

Click **MAINTENANCE** and then the **Association List** tab to display the screen as shown next.

Figure 92 Association List

The following table describes the labels in this screen.

Table 55 Association List

LABEL	DESCRIPTION
Stations	
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyAIR.
Name (SSID)	This field displays the SSID to which the wireless station is associated.
WDS Link This screen displays when bridge mode is activated on the ZyAIR.	
Link No	This field displays the index number of a bridge connection on the WDS.
MAC Address	This field displays a remote bridge MAC address.
Link Time	This field displays the WDS link up-time.

Table 55 Association List

LABEL	DESCRIPTION
Privacy	This field displays whether traffic on the WDS is encrypted or not.
Refresh	Click Refresh to reload the screen.

14.4 Channel Usage

The **Channel Usage** screen shows whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **MAINTENANCE** and then the **Channel Usage** tab to display the screen shown next.

Wait a moment while the ZyAIR compiles the information.

Figure 93 Channel Usage

Status	Association List	Channel Usage	F/W Upload	Configuration	Restart
	SSID	MAC Address	Channel	Signal	Network Mode
	ZyXEL_12378	00:13:49:00:00:01	6	23 %	Infra
	ZyXEL	00:13:49:00:00:05	6	82 %	Infra
	Wireless	00:A0:C5:00:07:77	6	42 %	Infra
		00:20:A6:4F:27:BE	6	40 %	Infra
	ZyXEL_MIS	00:A0:C5:62:B0:CE	3	28 %	Infra, WEP
	test3237	00:13:49:F5:18:01	6	23 %	Infra
	6818_3_wpamix	00:13:49:2A:2A:FA	6	32 %	Infra, WEP
	ZyXEL	00:13:49:11:99:81	6	25 %	Infra
	ct520d	00:13:49:07:30:03	6	36 %	Infra, WEP
	ZyXEL	00:13:49:F5:18:74	6	21 %	Infra
	abc	00:13:49:12:34:56	6	37 %	Infra
	6812-G3KTest	00:13:49:07:30:02	3	25 %	Infra, WEP
	ZyXEL	00:13:49:18:90:11	6	33 %	Infra
	PQA_3272_ZW10W	00:A0:C5:44:E2:B6	6	26 %	Infra
	CPE_5257_02	00:0B:6B:30:25:4D	11	37 %	Infra, WEP
	PKW8C	00:A0:C5:00:08:87	11	26 %	Infra
	ZyXEL16	00:13:49:16:45:30	10	37 %	Infra, WEP
	Cisco AP	00:0E:D7:8D:15:30	9	22 %	Infra, WEP
		00:13:49:2A:2A:F7	10	37 %	Infra, WEP
	Wireless	00:A0:C5:5C:AF:7A	11	25 %	Infra
	PQA-3214-G3000H_1	00:A0:C5:F5:02:06	11	22 %	Infra, WEP

Refresh

The following table describes the labels in this screen.

Table 56 Channel Usage

LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the Wireless Configuration and Roaming chapter for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.

Table 56 Channel Usage

LABEL	DESCRIPTION
Network Mode	"Network mode" in this screen refers to your wireless LAN infrastructure (refer to the Wireless LAN chapter) and WEP setup. Network modes are: Infrastructure (same as an extended service set ESS), Infrastructure with WEP (WEP encryption is enabled), Ad-Hoc (same as an independent basic service set IBSS), or Ad-Hoc with WEP .
Refresh	Click Refresh to reload the screen.

14.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "zyair.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** and then **F/W Upload**. Follow the instructions in this screen to upload firmware to your ZyAIR.

Figure 94 Firmware Upload

The following table describes the labels in this screen.

Table 57 Firmware Upload

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

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

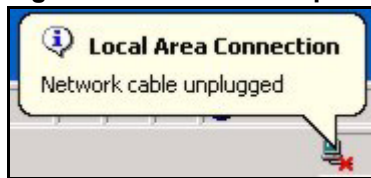
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyAIR again.

Figure 95 Firmware Upload In Process



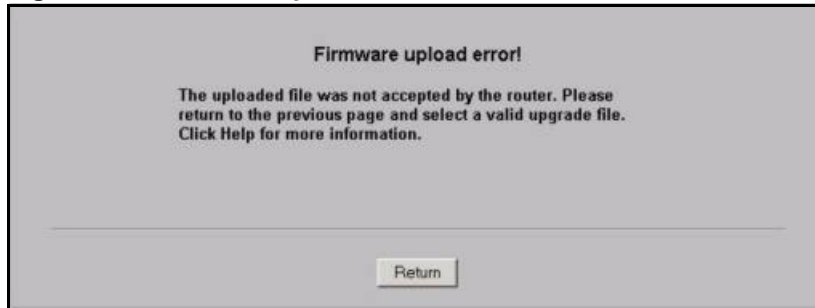
The ZyAIR automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 96 Network Temporarily Disconnected



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

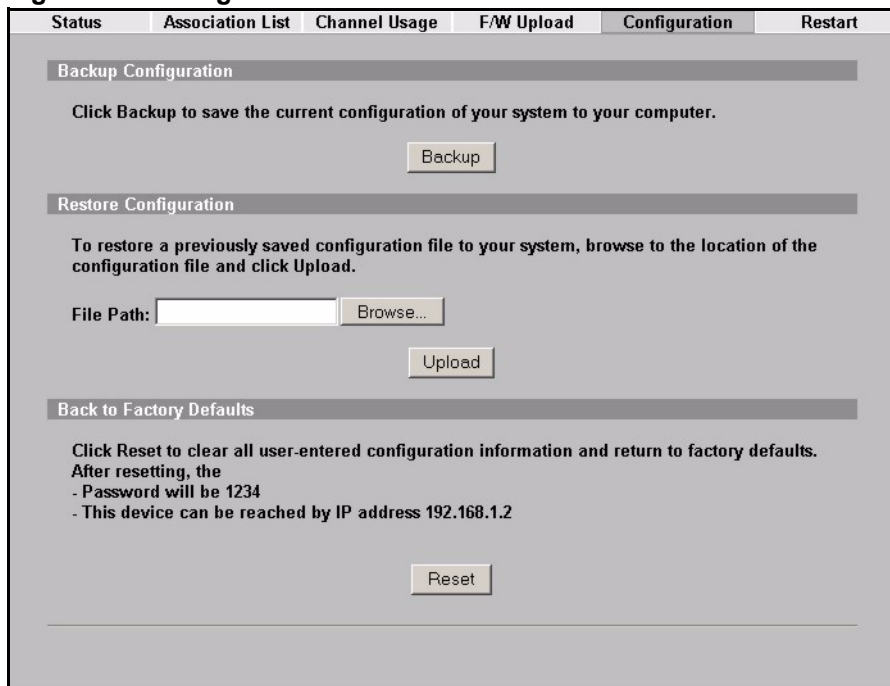
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 97 Firmware Upload Error

14.6 Configuration Screen

See the [Firmware and Configuration File Maintenance](#) chapter for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 98 Configuration

14.6.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyAIR's current configuration to a file on your computer. Once your ZyAIR 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 ZyAIR's current configuration to your computer.

14.6.2 Restore Configuration

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

Table 58 Restore Configuration

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

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

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyAIR again.

Figure 99 Configuration Upload Successful



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

Figure 100 Network Temporarily Disconnected



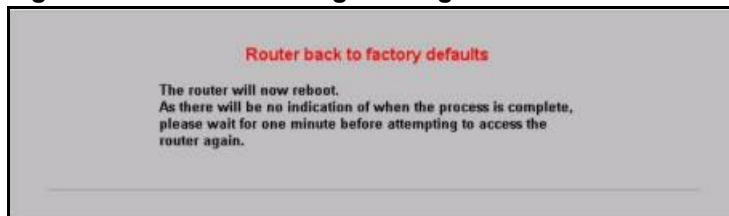
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyAIR IP address (192.168.1.2). See your *Quick Installation Guide* for details on how to set up your computer's IP address.

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

Figure 101 Configuration Upload Error

14.6.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyAIR to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 102 Reset Warning Message

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

14.7 Restart Screen

System restart allows you to reboot the ZyAIR without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the ZyAIR reboot. This does not affect the ZyAIR's configuration.

Figure 103 Restart Screen

CHAPTER 15

Introducing the SMT

This chapter describes how to access the SMT and provides an overview of its menus.

15.1 Connect to your ZyAIR Using Telnet

The following procedure details how to telnet into your ZyAIR.

- 1 In Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.1.2” (the default IP address) and click **OK**.
- 2 For your first login, enter the default password “1234”. As you type the password, the screen displays an asterisk “*” for each character you type.

Figure 104 Login Screen

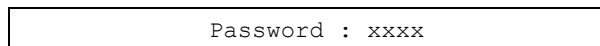


Figure 104 shows a login screen with a text input field containing the text "Password : xxxx".

- 3 After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyAIR will automatically log you out. You will then have to telnet into the ZyAIR again. You can use the web configurator or the CI commands to change the inactivity time out period.

15.2 Changing the System Password

Change the ZyAIR default password by following the steps shown next.

- 1 From the main menu, enter 23 to display **Menu 23 – System Security**.
- 2 Enter 1 to display **Menu 23.1 – System Security – Change Password** as shown next.
- 3 Type your existing system password in the **Old Password** field, and press [ENTER].

Figure 105 Menu 23.1 System Security: Change Password

```

Menu 23.1 - System Security - Change Password
Old Password= ****
New Password= ?
Retype to confirm= ?
Enter here to CONFIRM or ESC to CANCEL:

```

- 4** Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- 5** Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk “*” for each character you type.

15.3 ZyAIR SMT Menu Overview Example

The following table gives you an overview of your ZyAIR’s various SMT menus.

Table 59 SMT Menu Overview

MENUS	SUB MENUS	
1 General Setup	1.1 Configure Dynamic DNS	
3 LAN Setup	3.2 TCP/IP Setup	
	3.5 Wireless LAN Setup	3.5.1 WLAN MAC Address Filter
		3.5.2 Roaming Configuration
		3.5.4 Bridge Link Configuration
3.5.6 SSID Profile Edit		
14 Dial-in User Setup		
16 VLAN Setup		
23 System Security	23.1 System Security	
	23.5 Security Profile Edit	

Table 59 SMT Menus Overview (continued)

MENUS	SUB MENUS	
24 System Maintenance	24.1 System Status	
	24.2 System Information and Console Port Speed	24.2.1 System Information
		24.2.2 Console Port Speed
	24.3 Log and Trace	24.3.2 Syslog Logging
		24.3.4 Call-Triggering Packet
	24.4 Diagnostic	
	24.5 Backup Configuration	
	24.6 Restore Configuration	
	24.7 Upload Firmware	24.7.1 Upload System Firmware
		24.7.2 Upload System Configuration File
	24.8 Command Interpreter Mode	
24.10 Time and Date Setting		
24.11 Remote Management Setup		

15.4 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyAIR.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 60 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of No . Press [SPACE BAR] once to change No to Yes , then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].

Table 60 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Required fields	<?> or ChangeMe	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with ChangeMe must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

Figure 106 G-3000H SMT Main Menu

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.	
ZyAIR G-3000H Main Menu	
Getting Started	Advanced Management
1. General Setup	22. SNMP Configuration
3. LAN Setup	23. System Security
	24. System Maintenance
Advanced Applications	
14. Dial-in User Setup	
16. VLAN Setup	
	99. Exit
Enter Menu Selection Number:	

15.4.1 System Management Terminal Interface Summary

Table 61 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
14	Dial-in User Setup	Use this menu to set up local user profiles on the ZyAIR.
16	VLAN Setup	Use this menu to set up your VLAN.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password and enable network user authentication.

Table 61 Main Menu Summary

#	MENU TITLE	DESCRIPTION
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
99	Exit	Use this to exit from SMT and return to a blank screen.

CHAPTER 16

General Setup

The chapter shows you the information on general setup.

16.1 General Setup

Menu 1 – General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. It is recommended you type your computer's "Computer name".

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyAIR via DHCP.

16.1.1 Procedure To Configure Menu 1

Enter 1 in the Main Menu to open **Menu 1 – General Setup** as shown next.

Figure 107 Menu 1 General Setup

```

Menu 1 - General Setup

System Name= G-3000H
Domain Name=
First System DNS Server= From DHCP
  IP Address= N/A
Second System DNS Server= None
  IP Address= N/A
Third System DNS Server= None
  IP Address= N/A

```

Fill in the required fields. Refer to the following table for more information about these fields.

Table 62 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.

Table 62 Menu 1 General Setup

FIELD	DESCRIPTION
First/Second/Third System DNS Server	Press [SPACE BAR] to select From DHCP , User Defined or None and press [ENTER]. These fields are not available on all models.
IP Address	Enter the IP addresses of the DNS servers. This field is available when you select User-Defined in the field above.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 17

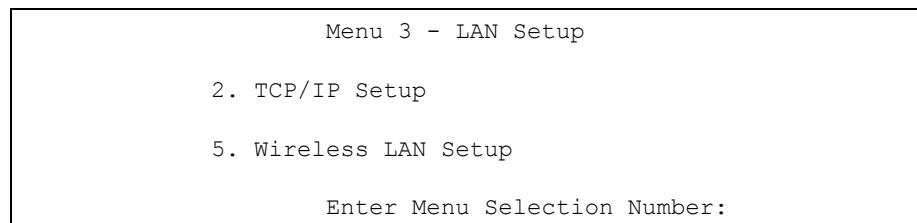
LAN Setup

This chapter shows you how to configure the LAN on your ZyAIR.

17.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 – LAN Setup**. From the main menu, enter 3 to display menu 3.

Figure 108 Menu 3 LAN Setup



Detailed explanation about the LAN Setup menu is given in the next chapter.

17.2 TCP/IP Ethernet Setup

Use menu 3.2 to configure your ZyAIR for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3-LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2-TCP/IP Setup**, as shown next:

Figure 109 Menu 3.2 TCP/IP Setup

<pre> Menu 3.2 - TCP/IP Setup IP Address Assignment= Static IP Address= 192.168.1.2 IP Subnet Mask= 255.255.255.0 Gateway IP Address= 0.0.0.0 </pre>
--

Follow the instructions in the following table on how to configure the fields in this menu.

Table 63 Menu 3.2 TCP/IP Setup

FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic to have the ZyAIR obtain an IP address from a DHCP server. You must know the IP address assigned to the ZyAIR (by the DHCP server) to access the ZyAIR again. Select Static to give the ZyAIR a fixed, unique IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable.
IP Address	Enter the (LAN) IP address of your ZyAIR in dotted decimal notation
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same network segment as your ZyAIR.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

17.3 Wireless LAN Setup

Use menu 3.5 to set up your ZyAIR as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

Figure 110 Menu 3.5 Wireless LAN Setup

Menu 3.5 - Wireless LAN Setup	
Operating Mode= Bridge / Repeater	Edit MAC Address Filter= N/A
Hide Name (SSID)= N/A	Edit Roaming Configuration= N/A
Channel ID= CH06 2437MHz	Edit SSID Profile= N/A
RTS Threshold= 2432	Select SSID Profile= N/A
Frag. Threshold= 2432	Edit Bridge Link Configuration= No
	Preamble= Long
	802.11 Mode= Mixed
	Max. Frame Burst= 650
	Breathing LED= Yes
	Block Intra-BSS Traffic= No
	Output Power= <11b>17dBm/<11g>13dBm
	Edit Layer-2 Isolation= N/A
Press ENTER to Confirm or ESC to Cancel:	
Press Space Bar to Toggle.	

The following table describes the fields in this menu.

Table 64 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
Operating Mode	Press [SPACE BAR] and select Access Point, Bridge / Repeater, AP + Bridge or MESSID . This field is not available on all models.
Name (SSID)	The SSID (Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the AP must have the same SSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters. This field is only available when you select Access Point or AP + Bridge in the Operating Mode field.
Hide Name (SSID)	Press [SPACE BAR] and select Yes to hide the SSID in the outgoing data frame so an intruder cannot obtain the SSID through scanning.
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 800 and 2432.
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Edit MAC Address Filter	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 3.5.1 - WLAN MAC Address Filter .
Edit Bridge Link Configuration	Use [SPACE BAR] to choose Yes and press [ENTER] to go to Menu 3.5.4 - Bridge Link Configuration .
Edit Roaming Configuration	Use [SPACE BAR] to choose Yes and press [ENTER] to go to Menu 3.5.2 - Roaming Configuration . This field is not available when you select Bridge / Repeater in the Operating Mode field.

Table 64 Menu 3.5 Wireless LAN Setup

FIELD	DESCRIPTION
Edit SSID Profile	Use [SPACE BAR] to choose Yes and press [ENTER] to go to Menu 3.5.6 - SSID Profile Edit . This field is only available when you select MESSID in the Operating Mode field.
Select SSID Profile	Use [SPACE BAR] to choose an SSID profile. This field is only available when you select Access Point in the Operating Mode field.
Preamble	Use [SPACE BAR] to choose a preamble type. Choices are Long , Short and Dynamic . The default setting is Long . See the section on preamble for more information.
802.11 Mode	Select B Only to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyAIR. Select G Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyAIR. Select Mixed to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyAIR. The transmission rate of your ZyAIR might be reduced.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets its maximum time, in microseconds, that the ZyAIR transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.
Breathing LED	Select Yes to enable the Breathing LED, also known as the ZyAIR LED. The blue ZyAIR LED is on when the ZyAIR is on and blinks (or breaths) when data is being transmitted to/from its wireless stations. Clear the check box to turn this LED off even when the ZyAIR is on and data is being transmitted/received.
Block Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Select No to allow Intra-BSS traffic, select Yes to block all Intra-BSS traffic.
Output Power	Set the output power of the ZyAIR in this field. If there is a high density of APs within an area, decrease the output power of the ZyAIR to reduce interference with other APs. The options are 17dBm (50mW), 15dBm (32mW), 13dBm (20mW), 11dBm (12.6mW) or 7dBm (5mW) for IEEE802.11b mode and 13dBm (20mW), 11dBm (12.6mW), 9dBm (7.9mW), 7dBm (5mW) or 3dBm (2mW) for IEEE802.11g mode.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.3.1 Configuring MAC Address Filter

Your ZyAIR checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyAIR.

- 1** From the main menu, enter 3 to open **Menu 3 – LAN Setup**.
- 2** Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 111 Menu 3.5 Wireless LAN Setup

```

Menu 3.5 - Wireless LAN Setup

Operating Mode= Access Point
Hide Name (SSID)= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432

Edit MAC Address Filter= Yes
Edit Roaming Configuration= No
Edit SSID Profile= N/A
Select SSID Profile= SSID01
Edit Bridge Link Configuration= N/A
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

Breathing LED= Yes
Block Intra-BSS Traffic= No
Output Power= <11b>17dBm/<11g>13dBm
Edit Layer-2 Isolation= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

3 Press [SPACE BAR] to select **Access Point** or **AP + Bridge** in the **Operating Mode** field and press [ENTER].

4 In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.

Figure 112 Menu 3.5.1 WLAN MAC Address Filter

```

Menu 3.5.1 - WLAN MAC Address Filter

Active= No
Filter Action= Allowed Association
-----
1= 00:00:00:00:00:00 13= 00:00:00:00:00:00 25= 00:00:00:00:00:00
2= 00:00:00:00:00:00 14= 00:00:00:00:00:00 26= 00:00:00:00:00:00
3= 00:00:00:00:00:00 15= 00:00:00:00:00:00 27= 00:00:00:00:00:00
4= 00:00:00:00:00:00 16= 00:00:00:00:00:00 28= 00:00:00:00:00:00
5= 00:00:00:00:00:00 17= 00:00:00:00:00:00 29= 00:00:00:00:00:00
6= 00:00:00:00:00:00 18= 00:00:00:00:00:00 30= 00:00:00:00:00:00
7= 00:00:00:00:00:00 19= 00:00:00:00:00:00 31= 00:00:00:00:00:00
8= 00:00:00:00:00:00 20= 00:00:00:00:00:00 32= 00:00:00:00:00:00
9= 00:00:00:00:00:00 21= 00:00:00:00:00:00
10= 00:00:00:00:00:00 22= 00:00:00:00:00:00
11= 00:00:00:00:00:00 23= 00:00:00:00:00:00
12= 00:00:00:00:00:00 24= 00:00:00:00:00:00
-----
Enter here to CONFIRM or ESC to CANCEL:

```

The following table describes the fields in this menu.

Table 65 Menu 3.5.1 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select Yes and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyAIR, press [SPACE BAR] to select Deny Association and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, Allowed Association , permits association with the ZyAIR. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
1..32	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyAIR in these address fields.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.3.2 Configuring Roaming

Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

- 1 From the main menu, enter 3 to display **Menu 3 – LAN Setup**.
- 2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 113 Menu 3.5 Wireless LAN Setup

```

Menu 3.5 - Wireless LAN Setup

Operating Mode= MESSID
Hide Name (SSID)= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432

Edit MAC Address Filter= No
Edit Roaming Configuration= Yes
Edit SSID Profile= No
Select SSID Profile= N/A
Edit Bridge Link Configuration= No
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

Breathing LED= Yes
Block Intra-BSS Traffic= No
Output Power= <11b>15dBm/<11g>11dBm
Edit Layer-2 Isolation= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

- 3** Move the cursor to the **Edit Roaming Configuration** field. Press [SPACE BAR] to select **Yes** and then press [ENTER]. **Menu 3.5.2 – Roaming Configuration** displays as shown next.

Figure 114 Menu 3.5.2 Roaming Configuration

```

Menu 3.5.2 - Roaming Configuration

Active= Yes
Port #= 3517

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

The following table describes the fields in this menu.

Table 66 Menu 3.5.2 Roaming Configuration

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select Yes to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet.
Port #	Type the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 3517. Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.3.3 Configuring SSID Profiles

Follow the steps below to configure SSID profiles on your ZyAIR.

1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 115 Menu 3.5 Wireless LAN Setup

```
Menu 3.5 - Wireless LAN Setup

Operating Mode= MESSID
Hide Name (SSID)= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432

Edit MAC Address Filter= No
Edit Roaming Configuration= No
Edit SSID Profile= Yes
Select SSID Profile= N/A
Edit Bridge Link Configuration= No
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

Breathing LED= Yes
Block Intra-BSS Traffic= No
Output Power= <11b>15dBm/<11g>11dBm
Edit Layer-2 Isolation= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

3 In the **Operating Mode** field, press [SPACE BAR] to select **MESSID** and press [ENTER].

4 Move the cursor to the **Edit SSID Profile** field. Press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.6 - SSID Profile Edit** displays as shown next.

Figure 116 Menu 3.5.6 - SSID Profile Edit

Menu 3.5.6 - SSID Profile Edit	
1 SSID03 Active= Yes	5 SSID01 Active= No
2 SSID01 Active= No	6 SSID01 Active= No
3 SSID01 Active= No	7 SSID01 Active= No
4 SSID01 Active= No	8 SSID01 Active= No
Press ENTER to Confirm or ESC to Cancel:	
Press Space Bar to Toggle.	

The following table describes the fields in this menu.

Table 67 Menu 3.5.6 - SSID Profile Edit

FIELD	DESCRIPTION
SSID 1~8	Press [SPACE BAR] to select an SSID from 1 to 16. The SSID (Service Set IDentity) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.
Active	Press [SPACE BAR] to select Yes or No and press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.3.4 Configuring Bridge Link

Follow the steps below to configure bridge link on your ZyAIR.

- 1** From the main menu, enter 3 to open **Menu 3 – LAN Setup**.
- 2** Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 117 Menu 3.5 Wireless LAN Setup

```
Menu 3.5 - Wireless LAN Setup

Operating Mode= Bridge / Repeater
Hide Name (SSID)= N/A
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432

Edit MAC Address Filter= N/A
Edit Roaming Configuration= N/A
Edit SSID Profile= N/A
Select SSID Profile= N/A
Edit Bridge Link Configuration= Yes
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

Breathing LED= Yes
Block Intra-BSS Traffic= No
Output Power= <11b>15dBm/<11g>11dBm
Edit Layer-2 Isolation= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

- 3** In the **Operating Mode** field, press [SPACE BAR] to select **Bridge / Repeater** or **AP + Bridge** and press [ENTER].
- 4** Move the cursor to the **Edit Bridge Link Configuration** field. Press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.4 – Bridge Link Configuration** displays as shown next.

Figure 118 Menu 3.5.4 Bridge Link Configuration

```

Menu 3.5.4 - Bridge Link Configuration

Enable Link 1= Yes           Peer MAC Address= 0b:16:21:2c:37:45
PSK= *****
Enable Link 2= No           Peer MAC Address= 00:0b:16:2c:37:3d
PSK= *****
Enable Link 3= Yes         Peer MAC Address= 0b:16:21:2c:37:3e
PSK= *****
Enable Link 4= No         Peer MAC Address= 0b:16:21:2c:37:3f
PSK= *****
Enable Link 5= Yes         Peer MAC Address= 0b:16:21:2c:37:40
PSK= *****

Enable WDS Security= Yes

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

The following table describes the fields in this menu.

Table 68 Menu 3.5.4 Bridge Link Configuration

FIELD	DESCRIPTION
Enable Link 1 ~ 5	Press [SPACE BAR] to select Yes or No and press [ENTER].
Peer MAC Address	Type the MAC address of peer device in valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols)
Enable WDS Security	Select Yes to enable WDS on your ZyAIR. A Wireless Distribution System (WDS) is a wireless connection between two or more APs. When you select Yes , you are prompted to type a Pre-Shared Key (PSK) in the PSK fields of each bridge link you want to configure. The ZyAIR uses TKIP to encrypt traffic on the WDS between AP's. Note: Other AP's must use the same encryption method to enable WDS.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.3.5 Configuring Layer-2 Isolation

Follow the steps below to configure layer-2 isolation on your ZyAIR.

- 1 From the main menu, enter 3 to open **Menu 3 – LAN Setup**.
- 2 Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

Figure 119 Menu 3.5 Wireless LAN Setup

```

Menu 3.5 - Wireless LAN Setup

Operating Mode= MESSID
Hide Name (SSID)= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432

Edit MAC Address Filter= No
Edit Roaming Configuration= No
Edit SSID Profile= No
Select SSID Profile= N/A
Edit Bridge Link Configuration= No
Preamble= Long
802.11 Mode= Mixed
Max. Frame Burst= 650

Breathing LED= Yes
Block Intra-BSS Traffic= No
Output Power= <11b>17dBm/<11g>13dBm
Edit Layer-2 Isolation= Yes

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

- 3** Move the cursor to the **Edit Layer-2 Isolation** field. Press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.5 – Layer 2 Isolation** displays as shown next.

Figure 120 Menu 3.5.5 Layer-2 Isolation

```

Menu 3.5.5 - Layer-2 Isolation

Allow devices with these MAC addresses
-----
1= 00:00:00:00:00:00 13= 00:00:00:00:00:00 25= 00:00:00:00:00:00
2= 00:00:00:00:00:00 14= 00:00:00:00:00:00 26= 00:00:00:00:00:00
3= 00:00:00:00:00:00 15= 00:00:00:00:00:00 27= 00:00:00:00:00:00
4= 00:00:00:00:00:00 16= 00:00:00:00:00:00 28= 00:00:00:00:00:00
5= 00:00:00:00:00:00 17= 00:00:00:00:00:00 29= 00:00:00:00:00:00
6= 00:00:00:00:00:00 18= 00:00:00:00:00:00 30= 00:00:00:00:00:00
7= 00:00:00:00:00:00 19= 00:00:00:00:00:00 31= 00:00:00:00:00:00
8= 00:00:00:00:00:00 20= 00:00:00:00:00:00 32= 00:00:00:00:00:00
9= 00:00:00:00:00:00 21= 00:00:00:00:00:00
10= 00:00:00:00:00:00 22= 00:00:00:00:00:00
11= 00:00:00:00:00:00 23= 00:00:00:00:00:00
12= 00:00:00:00:00:00 24= 00:00:00:00:00:00
-----

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

Table 69 Menu 3.5.5 Layer-2 Isolation

FIELD	DESCRIPTION
Allow devices with these MAC addresses	<p>These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the ZyAIR can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table. Type the MAC addresses of the wireless client, AP, computer or router that you want to allow the ZyAIR associated wireless clients to have access to in these address fields. Type the MAC address in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.F</p> <p>Note: The Block Intra-BSS Traffic changes from No to Yes when you enable layer-2 isolation.</p>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.</p>	

CHAPTER 18

Dial-in User Setup

This chapter shows you how to create user accounts on the ZyAIR.

18.1 Dial-in User Setup

By storing user profiles locally, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your ZyAIR.

From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

Figure 121 Menu 14- Dial-in User Setup

Menu 14 - Dial-in User Setup			
1. _____	9. _____	17. _____	25. _____
2. _____	10. _____	18. _____	26. _____
3. _____	11. _____	19. _____	27. _____
4. _____	12. _____	20. _____	28. _____
5. _____	13. _____	21. _____	29. _____
6. _____	14. _____	22. _____	30. _____
7. _____	15. _____	23. _____	31. _____
8. _____	16. _____	24. _____	32. _____
Enter Menu Selection Number:			

Type a number and press [ENTER] to edit the user profile.

Figure 122 Menu 14.1- Edit Dial-in User

```
Menu 14.1 - Edit Dial-in User
User Name= test
Active= Yes
Password= *****
Press ENTER to Confirm or ESC to Cancel:
Leave name field blank to delete profile
```

The following table describes the fields in this screen.

Table 70 Menu 14.1- Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select Yes and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 19

VLAN Setup

This chapter explains VLAN Setup menu 16. Refer to the Multiple-ESS and VLAN chapter for background information on VLAN.

19.1 VLAN Setup

To setup VLAN, select option 16 from the main menu to open **Menu 16 – VLAN Setup** as shown next.

Figure 123 Menu 16 VLAN Setup

Menu 16 - VLAN Setup		
VLAN Tagging=	Yes	Native VLAN ID= 1
1.Active=	Yes	ID= 1 Name= zyxel
2.Active=	No	ID= N/A Name= N/A
3.Active=	No	ID= N/A Name= N/A
4.Active=	No	ID= N/A Name= N/A
5.Active=	No	ID= N/A Name= N/A
6.Active=	No	ID= N/A Name= N/A
7.Active=	No	ID= N/A Name= N/A
8.Active=	No	ID= N/A Name= N/A
9.Active=	No	ID= N/A Name= N/A
10.Active=	No	ID= N/A Name= N/A
11.Active=	No	ID= N/A Name= N/A
12.Active=	No	ID= N/A Name= N/A
13.Active=	No	ID= N/A Name= N/A
14.Active=	No	ID= N/A Name= N/A
15.Active=	No	ID= N/A Name= N/A
16.Active=	No	ID= N/A Name= N/A

Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this menu.

Table 71 Menu 16 VLAN Setup

FIELD	DESCRIPTION
VLAN Tagging	To enable VLAN tagging, press [SPACE BAR] to select Yes and press [ENTER].
Native VLAN ID	Enter a number from 1 to 4094. This field is activated only when you select Yes in the VLAN Tagging field.
Index	This displays the number of a VLAN mapping profile.

Table 71 Menu 16 VLAN Setup

FIELD	DESCRIPTION
Active	To enable a VLAN mapping profile, press [SPACE BAR] to select Yes and press [ENTER].
ID	Press [SPACE BAR] to select a VLAN ID or enter one from 1 to 4094. Incoming traffic from the WLAN is authorized and assigned a VLAN ID by the RADIUS server before it is sent to the LAN interface of the wireless client. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Name	Press [SPACE BAR] to select a name or type a name to have the ZyAIR check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured Name field is checked against these attributes. If the configured Name field matches these attributes, the corresponding VLAN ID entry is used to access the specific VLAN group. If the configured Name field does not match the VLAN related attributes sent from the RADIUS server, a wireless station is assigned the associated SSID VLAN ID. See VLAN ID in the SSID screen.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 20

SNMP Configuration

This chapter explains SNMP Configuration menu 22. See the web configurator chapter on SNMP for background information.

20.1 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 – SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

Figure 124 Menu 22 SNMP Configuration

```

Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the SNMP configuration parameters.

Table 72 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set Community , which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.

Table 72 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

CHAPTER 21

System Security

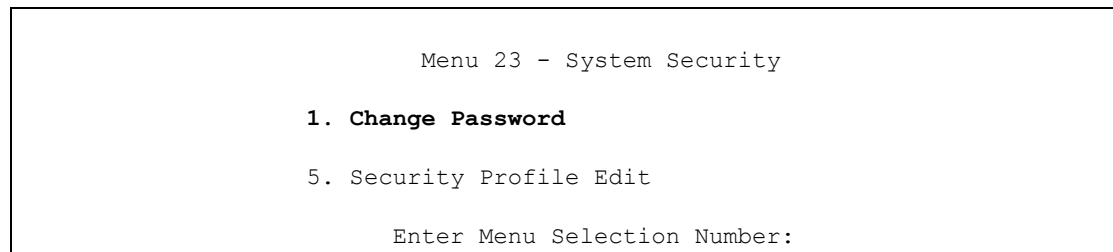
This chapter describes how to configure the system security on the ZyAIR.

21.1 System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

21.1.1 System Password

Figure 125 Menu 23 System Security



You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the ZyAIR in the *Introducing the Web Configurator* chapter.

21.1.2 Configuring Security Profiles

Enter 23 in the main menu to display **Menu 23 – System Security**.

Figure 126 Menu 23 - System Security

```
Menu 23 - System Security

1. Change Password

5. Security Profile Edit

Enter Menu Selection Number:
```

From **Menu 23 - System Security**, enter 5 to display **Menu 23.5 – Security Profile Edit** as shown next.

Figure 127 Menu 23.5 Security Profile Edit

```
Menu 23.5 - Security Profile Edit

Index= 1
Profile Name= security01
Mode= WEP
Authentication Databases= N/A
ReAuthentication Timer (in second)= N/A
Idle Timeout (in second)= N/A
Group Key Update Timer(in second)= N/A
PSK = N/A
WEP Encryption= 64bit
WEP code= ASCII
Default Key= 1
Key1= *****
Key2= *****
Key3= *****
Key4= *****
Authen. Method= Auto

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The fields in this screen vary according to the security **Mode** you select. See [Wireless Security Configuration, on page 73](#) for a description of the fields displayed in this screen.

CHAPTER 22

System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu and press [ENTER] to open **Menu 24 – System Maintenance**, as shown in the following figure.

Figure 128 Menu 24 System Maintenance

```

Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode

10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:

```

22.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your ZyAIR. Specifically, it gives you information on your Ethernet and Wireless LAN status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 – System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Entering 9 resets the counters; pressing [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are read-only and meant for diagnostic purposes.

Figure 129 Menu 24.1 System Maintenance: Status

```

Menu 24.1 - System Maintenance - Status                                01:55:5
                                                                    Sat. Jan. 01, 200

Port  Status      TxPkts    RxPkts    Cols    Tx B/s    Rx B/s    Up Tim
Ethernet 100M/Full  5802      2001      0        303       128       1:54:
Wireless  54M           3811      74        0         64        0         1:55:

Port  Ethernet Address      IP Address      IP Mask      DHCP
Ethernet 00:13:49:2A:2A:F5    192.168.1.2    255.255.255.0  None
Wireless 00:13:49:2A:2A:F5

System up Time:      1:55:57
ZyNOS F/W Version:  V3.50(AAC.1)b2 | 08/11/2005
Name: G-3000H

Press Command:

COMMANDS: 9-Reset Counters  ESC-Exit

```

The following table describes the fields present in this menu.

Table 73 Menu 24.1 System Maintenance: Status

FIELD	DESCRIPTION
Port	This is the port type. Port types are: Ethernet, WLAN1 and WLAN 2.
Status	This shows the status of the remote node.
TxPkts	This is the number of transmitted packets to this remote node.
RxPkts	This is the number of received packets from this remote node.
Cols	This is the number of collisions on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
Ethernet Address	This shows the MAC address of the port.
IP Address	This shows the IP address of the network device connected to the port.
IP Mask	This shows the subnet mask of the network device connected to the port.
DHCP	This shows the DHCP setting (None or Client) for the port.
System Up Time	This is the time the ZyAIR is up and running from the last reboot.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Name	This displays the device name.

22.2 System Information

To get to the System Information:

- 1 Enter 24 to display **Menu 24 – System Maintenance**.
- 2 Enter 2 to display **Menu 24.2 – System Information and Console Port Speed**.
- 3 From this menu you have two choices as shown in the next figure:

Figure 130 Menu 24.2 System Information and Console Port Speed

```

Menu 24.2 - System Information and Console Port Speed
  1. System Information
  2. Console Port Speed

Please enter selection:

```

Note: The ZyAIR also has an internal console port for support personnel only. Do not open the ZyAIR as it will void your warranty.

22.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

Figure 131 Menu 24.2.1 System Information: Information

```

Menu 24.2.1 - System Maintenance - Information

Name: G-3000H
Routing: BRIDGE
ZyNOS F/W Version: V3.50(AAC.0)b1 | 05/25/2005
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:F5:02:02
IP Address: 192.168.1.2
IP Mask: 255.255.255.0
DHCP: None

Press ESC or RETURN to Exit:

```

The following table describes the fields in this menu.

Table 74 Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
Name	Displays the system name of your ZyAIR. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.

Table 74 Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your ZyAIR.
IP Address	This is the IP address of the ZyAIR in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyAIR.
DHCP	This field shows the DHCP setting of the ZyAIR.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

22.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your ZyAIR supports 9600 (default), 19200, 38400, 57600 and 115200 bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 132 Menu 24.2.2 System Maintenance: Change Console Port Speed

```

Menu 24.2.2 - System Maintenance - Change Console Port Speed

      Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:

```

After you changed the console port speed on your ZyAIR, you must also make the same change to the console port speed parameter of your communication software.

22.3 Log and Trace

Your ZyAIR provides the error logs and trace records that are stored locally.

22.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- 1 Type 24 in the main menu to display **Menu 24 – System Maintenance**.
- 2 From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

Figure 133 Menu 24.3 System Maintenance: Log and Trace

```

Menu 24.3 - System Maintenance - Log and Trace
1. View Error Log
Please enter selection:

```

- 3** Enter 1 from **Menu 24.3 – System Maintenance – Log and Trace** and press [ENTER] twice to display the error log in the system.

After the ZyAIR finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

Figure 134 Sample Error and Information Messages

```

55 Sat Jan 1 00:00:00 2000 PP05 ERROR Wireless LAN init fail, code=-1
56 Sat Jan 1 00:00:01 2000 PP07 INFO LAN promiscuous mode <1>
57 Sat Jan 1 00:00:01 2000 PINI INFO Last errorlog repeat 1 Times
58 Sat Jan 1 00:00:01 2000 PINI INFO main: init completed
59 Sat Jan 1 00:00:02 2000 PP05 -WARN SNMP TRAP 3: link up
60 Sat Jan 1 00:00:30 2000 PSSV -WARN SNMP TRAP 0: cold start
61 Sat Jan 1 00:01:38 2000 PINI INFO SMT Session Begin
62 Sat Jan 1 00:06:44 2000 PINI INFO SMT Session End
63 Sat Jan 1 00:11:13 2000 PINI INFO SMT Session Begin
Clear Error Log (y/n):

```

22.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyAIR to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Figure 135 Menu 24.4 System Maintenance: Diagnostic

```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
1. Ping Host
2. DHCP Release
3. DHCP Renewal

System
11. Reboot System

Enter Menu Selection Number:
Host IP Address= N/A

```

Follow the procedure next to get to display this menu:

- 1** From the main menu, type 24 to open **Menu 24 – System Maintenance**.
- 2** From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for your ZyAIR and the connections.

Table 75 Menu 24.4 System Maintenance Menu: Diagnostic

FIELD	DESCRIPTION
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
DHCP Release	Release the IP address assigned by the DHCP server.
DHCP Renewal	Get a new IP address from the DHCP server.
Reboot System	Reboot the ZyAIR.
Host IP Address	If you typed 1 to Ping Host, now type the address of the computer you want to ping.

CHAPTER 23

Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files using the SMT screens.

23.1 Filename Conventions

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

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyAIR.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file config.cfg.

If your [T]FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyAIR only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyAIR and the external filename refers to the filename not on the ZyAIR, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

Table 76 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the ZyAIR. Uploading the rom-0 file replaces the entire ROM file system, including your ZyAIR configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyAIR.

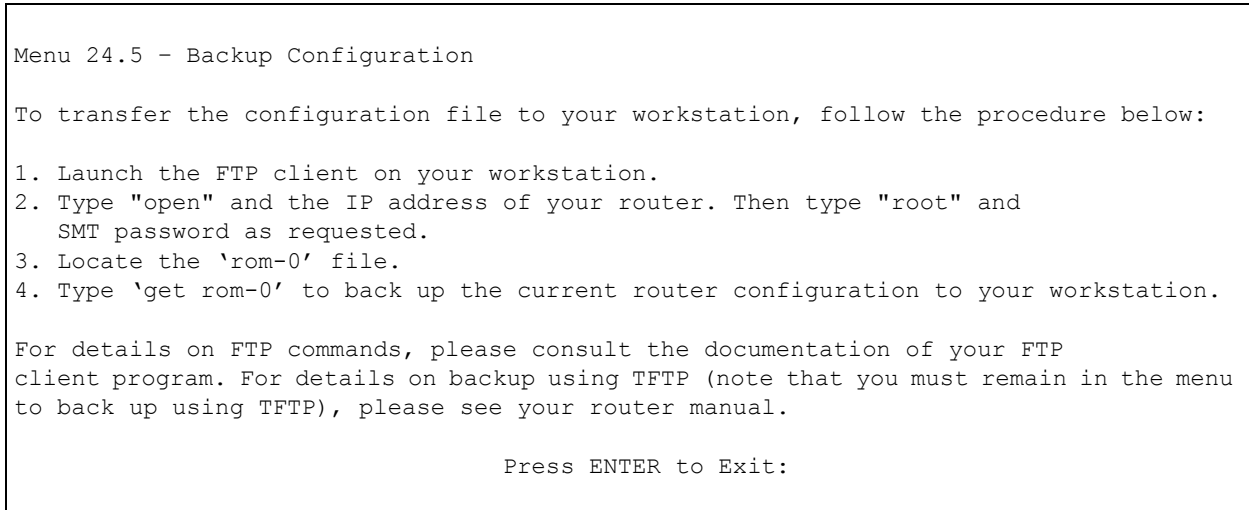
23.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyAIR configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyAIR to the computer, while upload means from your computer to the ZyAIR.

23.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 – System Maintenance** to get the following screen.

Figure 136 Menu 24.5 Backup Configuration

23.2.2 Using the FTP command from the DOS Prompt

- 1** Launch the FTP client on your computer.
- 2** Enter “open” and the IP address of your ZyAIR.
- 3** Press [ENTER] when prompted for a username.
- 4** Enter “root” and your SMT password as requested. The default is 1234.
- 5** Enter “bin” to set transfer mode to binary.
- 6** Use “get” to transfer files from the ZyAIR to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyAIR to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- 7** Enter “quit” to exit the FTP prompt.

Figure 137 FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit

```

The following table describes some of the commands that you may see in third party FTP clients.

Table 77 General Commands for Third Party FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

23.2.3 Backup Configuration Using TFTP

The ZyAIR supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next:

- 1** Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

- 3 Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the configuration file is rom-0 (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyAIR to the computer and “binary” to set binary transfer mode.

23.2.4 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyAIR IP address, “get” transfers the file source on the ZyAIR (rom-0 name of the configuration file on the ZyAIR) to the file destination on the computer and renames it config.rom.

The following table describes some of the fields that you may see in third party TFTP clients.

Table 78 General Commands for Third Party TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyAIR. 192.168.1.2 is the ZyAIR's default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyAIR and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyAIR. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

23.2.5 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- 1 Display menu 24.5 and enter “y” at the following screen.

Figure 138 System Maintenance: Backup Configuration

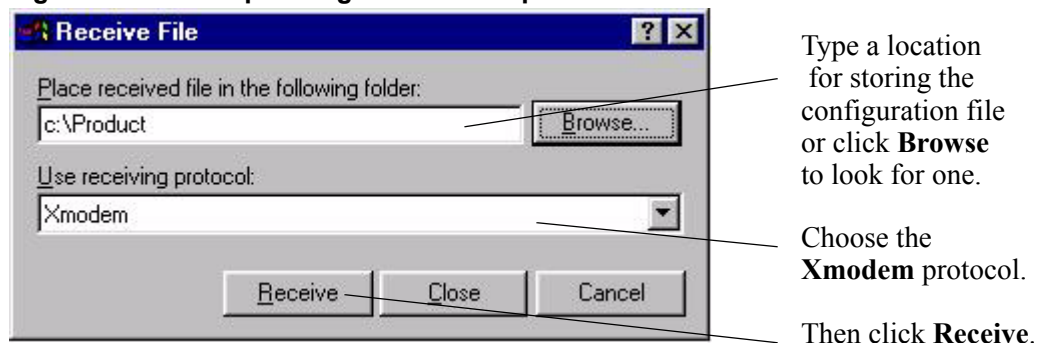
```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

- 2 The following screen indicates that the Xmodem download has started.

Figure 139 System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

- 3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 140 Backup Configuration Example

- 4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 141 Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

23.3 Restore Configuration

Menu 24.6 — System Maintenance – Restore Configuration allows you to restore the configuration via FTP or TFTP to your ZyAIR. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The ZyAIR restarts automatically after the file transfer is complete.

23.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 142 Menu 24.6 Restore Configuration

```

Menu 24.6 - Restore Configuration
To transfer the firmware and the configuration file, follow the procedure
below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-spt is the
   Remote file name on the router. This restores the configuration to your
   router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:

```

23.4 Uploading Firmware and Configuration Files

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file.

Note: WARNING! PLEASE WAIT A FEW MINUTES FOR THE ZYAIR TO RESTART AFTER FIRMWARE OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS MAY PERMANENTLY DAMAGE YOUR ZYAIR.

Figure 143 Menu 24.7 System Maintenance: Upload Firmware

```

Menu 24.7 - System Maintenance - Upload Firmware

1. Upload System Firmware
2. Upload System Configuration File

Enter Menu Selection Number:

```

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

23.4.1 Firmware Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyAIR, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 144 Menu 24.7.1 System Maintenance: Upload System Firmware

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name of your
   firmware upgrade file on your workstation and "ras" is the remote file name on the
   system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP), please see
your manual.

Press ENTER to Exit:
```

23.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 145 Menu 24.7.2 System Maintenance: Upload System Configuration File

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT
   password as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of
   your system configuration file on your workstation, which will be transferred to the
   "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration file process
   is complete.

For details on FTP commands, please consult the documentation of your FTP client
program. For details on uploading system firmware using TFTP (note that you must
remain on this menu to upload system firmware using TFTP), please see your manual.

Press ENTER to Exit:
```

To transfer the firmware and the configuration file, follow these examples:

23.4.3 Using the FTP command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter “open” and the IP address of your ZyAIR.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter “root” and your SMT password as requested. The default is 1234.
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the ZyAIR, e.g., put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the ZyAIR and renames it “ras”. Similarly “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyAIR and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyAIR to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the FTP prompt.

Figure 146 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands that you may find in third party FTP clients are listed earlier in this chapter.

23.4.4 TFTP File Upload

The ZyAIR also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

- 1 Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.

- 2** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3** Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4** Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.
- 5** Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyAIR to the computer, “put” the other way around, and “binary” to set binary transfer mode.

23.4.5 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyAIR’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyAIR).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

23.4.6 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyAIR. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyAIR via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

23.4.7 Uploading Firmware File Via Console Port

Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

Figure 147 Menu 24.7.1 as seen using the Console Port

```

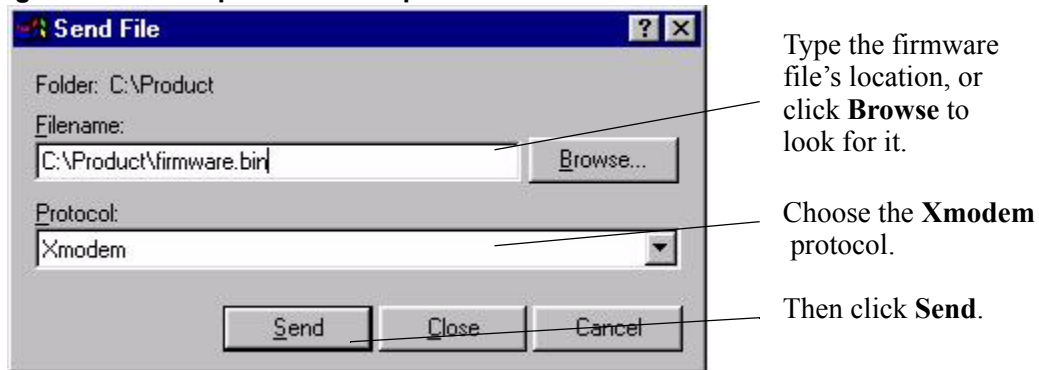
Menu 24.7.1 - System Maintenance - Upload System Firmware
To upload system firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.
Warning: Proceeding with the upload will erase the current system
firmware.
Do You Wish To Proceed: (Y/N)

```

After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

23.4.8 Example Xmodem Firmware Upload Using HyperTerminal

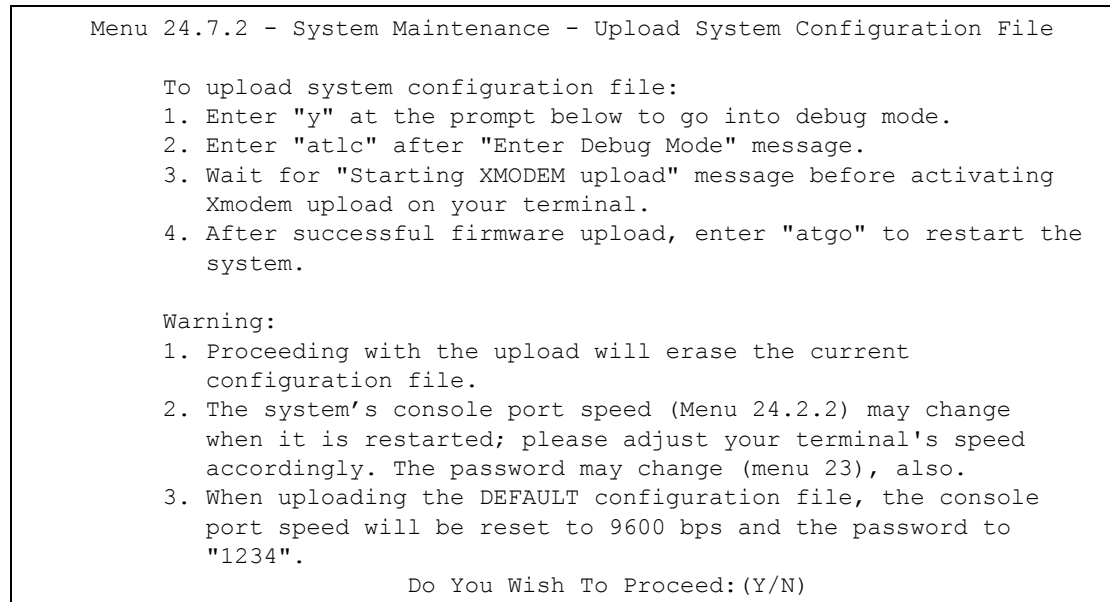
Click **Transfer**, then **Send File** to display the following screen.

Figure 148 Example Xmodem Upload

After the firmware upload process has completed, the ZyAIR will automatically restart.

23.4.9 Uploading Configuration File Via Console Port

- 1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

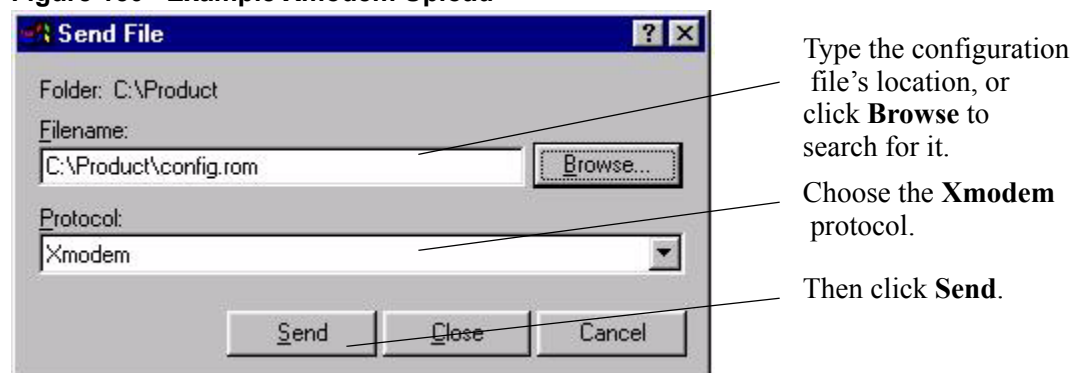
Figure 149 Menu 24.7.2 as seen using the Console Port

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter "atgo" to restart the ZyAIR.

23.4.10 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 150 Example Xmodem Upload

After the configuration upload process has completed, restart the ZyAIR by entering "atgo"

CHAPTER 24

System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

24.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

Figure 151 Menu 24 System Maintenance

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode

10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

Figure 152 Valid CI Commands

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
G-3000H> ?
Valid commands are:
sys          exit          ether          wlan
ip           bridge         certificates   8021x
wcfg
G-3000H>
```

24.1.1 CNM

Vantage CNM (Centralized Network Management) is a browser-based, global management solution that allows an administrator to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyXEL device to be managed by Vantage CNM, then you should not configure it without notifying the Vantage CNM administrator.

24.1.2 Configuring Vantage CNM

Vantage CNM is disabled on the device by default. You can configure Vantage CNM on your ZyXEL device by using the following commands.

Figure 153 CNM CL

```

G-3000H>cnm
active          sgid          managerIp      debug
reset          simulate      encrykey       encrymode
G-3000H>

```

The following table describes the commands in this screen. All commands begin with “cnm” so for example, type “cnm active 1” to enable Vantage CNM on your device.

Table 79 CNM Commands

COMMAND	SUB COMMAND	DESCRIPTION
active	<0:Disable 1:Enable CNM via WAN 2:Enable CNM via WAN or LAN>	This displays the ZyXEL device connection status with Vantage CNM and displays the last date and time that the ZyXEL device registered with the Vantage CNM server. If Vantage CNM is disabled on the ZyXEL device, active 0 is displayed. If Vantage CNM is enabled on the ZyXEL device using a WAN connection, active 1 is displayed. If Vantage CNM is enabled on the ZyXEL device using a WAN or LAN connection, active 2 is displayed.
	0	Use this command to disable Vantage CNM on your ZyXEL device.
	1	Use this command to enable Vantage CNM on your ZyXEL device using a WAN connection.
	2	Use this command to enable Vantage CNM on your ZyXEL device using a WAN or LAN connection.
	Last Register Time: 0-0-0 0:0:0	For example if Last Register Time 2004-11-20 10:34:23 is displayed then the last date the device registered with Vantage CNM was the 20th November 2003 at 10:34 PM. The last register time displays the last date (year-month-date) and time (hours : minutes : seconds) that the ZyXEL device registered with Vantage CNM. It displays all zeroes if it has not yet registered with the Vantage CNM server.
sgid		This command displays your ZyXEL device's unique ID in Vantage CNM.

Table 79 CNM Commands

COMMAND	SUB COMMAND	DESCRIPTION
managerIp	[addr]	<p>This command displays the public IP address of the Vantage CNM server.</p> <p>If the Vantage server is on the same subnet as the ZyXEL device, enter the private or public IP address of the Vantage CNM server.</p> <p>If the Vantage CNM server is on a different subnet to the ZyXEL device, enter the public IP address of the Vantage CNM server.</p> <p>If the Vantage CNM server is behind a NAT router, enter the WAN Public IP address of the NAT router here and configure the NAT router to forward UDP port 1864 traffic to the Vantage CNM server.</p> <p>If the Vantage CNM server is behind a firewall, you may have to create a rule on the firewall to allow UDP port 1864 traffic through to the Vantage CNM server (most (new) ZyXEL firewalls automatically allow this).</p> <p>Use this command to set the IP address of the Vantage CNM server.</p>
debug	<pre><0:Disable 1:Vantage 2:Agent tester 3:Server></pre> <p>0</p> <p>1</p> <p>2</p> <p>3</p>	<p>This command displays the output of Vantage CNM debug messages.</p> <p>Type this command to not display Vantage CNM debug messages.</p> <p>Type this command to display Vantage CNM debug messages on the console after the ZyXEL device registers with the Vantage CNM server.</p> <p>Type this command to display Vantage CNM debug messages on the console after the ZyXEL device registers with the Vantage CNM server.</p> <p>Type this command to display Vantage CNM debug messages on the console after the ZyXEL device registers with the Vantage CNM server.</p>
reset		Have the ZyXEL device send register request messages to the Vantage CNM server.
encrykey	[string]	<p>This displays the encryption key, which is used to encrypt and decrypt messages between Vantage CNM and the device.</p> <p>Use this command to specify the encryption key.</p> <p>Type eight alphanumeric characters when you choose DES encryption algorithm.</p> <p>Type 24 alphanumeric characters when you choose 3DES encryption algorithm.</p> <p>The ZyXEL device must have the same encryption key as the Vantage CNM server.</p>

Table 79 CNM Commands

COMMAND	SUB COMMAND	DESCRIPTION
encrymode	<0:NONE 1:DES 2:3DES>	This command is used to encrypt communications between the ZyXEL device and the Vantage CNM server. Use this command to set the encryption mode. Type 0 to have no encryption, type 1 to have the ZyXEL device use DES encryption or type 2 to have the ZyXEL device use 3DES encryption. The ZyXEL device must use the same encryption mode as the Vantage CNM server.
keepalive	0 [seconds]	Keepalive messages are sent to the Vantage CNM server by the ZyXEL device. They show the connection status between the ZyXEL device and the Vantage CNM server. This command displays the time interval in seconds between the keepalive messages that the ZyXEL device sends to the Vantage CNM server. Use this command to disable keepalive message sending. To set a time interval type the cnm keepalive command followed by a number from 10 to 655.
version		This displays the Vantage CNM version.

24.1.3 Configuration Example

This is an example allowing Vantage CNM server (on the same subnet as your ZyXEL device) with an IP address of 10.1.1.1, to manage your device. The device and Vantage CNM communicate using DES encryption and a password of “12345678”.

Figure 154 CNM Configuration Example

```
G-3000H> cnm
active          sgid          managerIp      debug
reset          encrykey       encrymode      keepalive
version
G-3000H>

G-3000H> cnm active
cnm active 0 <0:Disable 1:Enable CNM via WAN 2:Enable CNM via
WAN or LAN>
Last Register Time: 0-0-0 0:0:0
G-3000H> cnm active 1
cnm active 1
G-3000H>

G-3000H> cnm managerIp
managerIp 0.0.0.0
G-3000H> cnm managerIp 10.1.1.1
managerIp 10.1.1.1
G-3000H>

G-3000H> cnm debug
cnm debug 0 <0:Disable 1:Vantage 2:Agent tester 3:Server>
G-3000H>

G-3000H> cnm sgid
sgId 0X0000000000000000
G-3000H> cnm sgid 0a1b2c3d4e5f6a
sgId 0X000a1b2c3d4e5f6a
G-3000H>

G-3000H> cnm encrymode
cnm encrymode 0 <0:NONE 1:DES 2:3DES>
G-3000H> cnm encrymode 1
cnm encrymode 1
G-3000H>

G-3000H> cnm encrykey 12345678
encrykey 12345678
G-3000H>

cnm keepalive 20
Send SGMP keepalive timer change event
G-3000H>
sgmpd: Change keepalive timer to 20 seconds
G-3000H>

G-3000H> cnm version
cnm version: 2.0.2-b4
G-3000H>
```

24.2 Time and Date Setting

The ZyAIR keeps track of the time and date. There is also a software mechanism to set the

time manually or get the current time and date from an external server when you turn on your ZyAIR. Menu 24.10 allows you to update the time and date settings of your ZyAIR. The real time is then displayed in the ZyAIR error logs.

- 1 Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.
- 2 Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyAIR as shown in the following screen.

Figure 155 Menu 24.10 System Maintenance: Time and Date Setting

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= NTP (RFC-1305)
Time Server Address= 128.105.39.21

Current Time:                05 : 47 : 19
New Time (hh:mm:ss):        05 : 47 : 17
Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01
Time Zone= GMT
Daylight Saving= No
Start Date (mm-dd):          01 - 01
End Date (mm-dd):            01 - 01

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

Table 80 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC-1305) is similar to Time (RFC-868) . None. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose Yes .
Start Date	If using daylight savings time, enter the month and day that it starts on.

Table 80 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

24.2.1 Resetting the Time

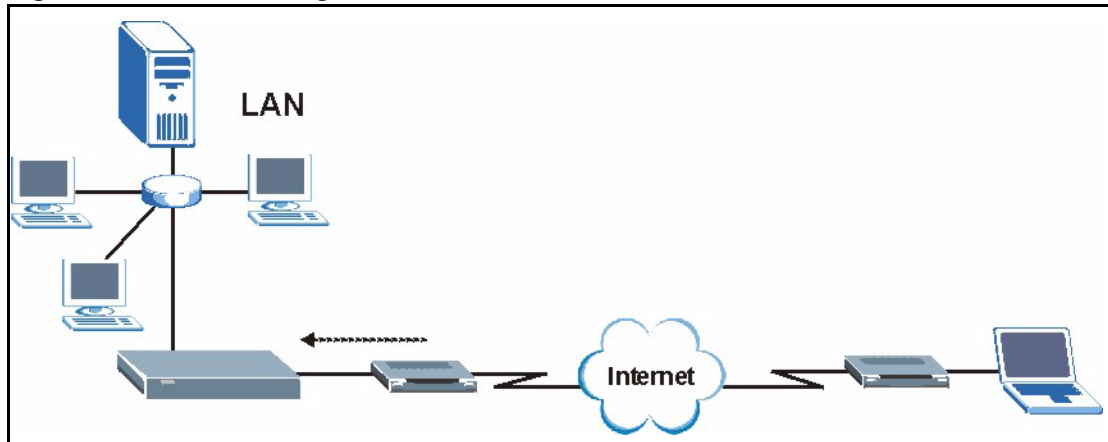
The ZyAIR resets the time in three instances:

- 1 On leaving menu 24.10 after making changes.
- 2 When the ZyAIR starts up, if there is a timeserver configured in menu 24.10.
- 3 24-hour intervals after starting.

24.3 Remote Management Setup

24.3.1 Telnet

You can configure your ZyAIR for remote Telnet access as shown next.

Figure 156 Telnet Configuration on a TCP/IP Network

24.3.2 FTP

You can upload and download ZyAIR firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

24.3.3 Web

You can use the ZyAIR's embedded web configurator for configuration and file management. See the *online help* for details.

24.3.4 Remote Management Setup

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your ZyAIR from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

Table 81 Remote Management Port Control

WAN only (Internet)	ALL (LAN and WAN)
LAN only	Disable (Neither)

Note: If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter 11, from menu 24, to display **Menu 24.11 - Remote Management Control** (shown next)

Figure 157 Menu 24.11 Remote Management Control

Menu 24.11 - Remote Management Control	
TELNET Server:	Port = 23 Access = ALL Secure Client IP = 0.0.0.0
FTP Server:	Port = 21 Access = ALL Secure Client IP = 0.0.0.0
HTTPS Server:	Certificate = auto_generated_self_signed_cert Authenticate Client Certificates = No Port = 443 Access = ALL Secure Client IP = 0.0.0.0
HTTP Server:	Port = 80 Access = ALL Secure Client IP = 0.0.0.0
SNMP Service:	Port = 161 Access = ALL Secure Client IP = 0.0.0.0
Press ENTER to Confirm or ESC to Cancel:	

The following table describes the fields in this menu.

Table 82 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
TELNET Server: FTP Server: HTTPS Server: HTTP Server: SNMP Service:	Each of these read-only labels denotes a server or service that you may use to remotely manage the ZyAIR. See "SSL Passthrough" for information on HTTPS.
Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: LAN only , WAN only , All or Disable . The default is LAN only .
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyAIR. Enter an IP address to restrict access to a client with a matching IP address.
Certificate	This field displays the name used to identify this certificate. The ZyAIR has an auto_generated_self_signed_cert by factory default. The factory default certificate is common to all ZyAIR's that use certificates. You can replace the certificate when you log into the ZyAIR, see the section Introducing the Web Configurator or you can go to the Certificates configuration screen, see the Certificates chapter.
Authenticate Client Certificates	Select Yes by pressing the [SPACE BAR]. The internal RADIUS server uses one of the certificates listed in the My Certificates screen to authenticate each wireless client. The exact certificate used, depends on the certificate information configured on the wireless client.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

24.3.5 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in menu 24.11.
- 3 The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
- 4 There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
- 5 There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

24.4 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

24.5 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyAIR will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Appendix A

Troubleshooting

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

Problems Starting Up the ZyAIR

Table 83 Troubleshooting the Start-Up of Your ZyAIR

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adaptor.	Make sure you are using the supplied power adaptor 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 ZyAIR reboots automatically sometimes.	The supplied power to the ZyAIR is too low. Check that the ZyAIR is receiving enough power. Make sure the power source is working properly.

Problems with the Ethernet Interface

Table 84 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the LAN.	If the ETHN LED on the front panel is off, check the Ethernet cable connection between your ZyAIR and the Ethernet device connected to the ETHERNET 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 ZyAIR, the Ethernet device and your computer are on the same subnet.
I cannot ping any computer on the LAN.	If the ETHN LED on the front panel is off, check the Ethernet cable connections between your ZyAIR 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 ZyAIR, the Ethernet device and the LAN computers are on the same subnet.

Problems with the Password

Table 85 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR.	The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the RESET button on the top panel of the ZyAIR to restore the factory default configuration file (hold this button in for about 10 seconds or until the link LED turns red). This will restore all of the factory defaults including the password.

Problems with Telnet

Table 86 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR through Telnet.	Refer to the Problems with the Ethernet Interface section for instructions on checking your Ethernet connection.

Problems with the WLAN Interface

Table 87 Troubleshooting the WLAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the WLAN.	Make sure the wireless card is properly inserted in the ZyAIR and the link LED is on. Make sure the wireless adapter on the wireless station is working properly. Check that both the ZyAIR and your wireless station are using the same ESSID, channel and WEP keys (if WEP encryption is activated).
I cannot ping any computer on the WLAN.	Make sure the wireless card is properly inserted in the ZyAIR and the link LED is on. Make sure the wireless adapter on the wireless station(s) is working properly. Check that both the ZyAIR and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Appendix B

Specifications

Hardware

Table 88 Hardware

Power Specification	DC 12V 1200mA
Operation Temperature	5° C ~ 50° C
Storage Temperature	-20° C ~ 55° C
Operation Humidity	10% to 90% (Non-condensing)
Storage Humidity	5% to 95% (Non-condensing)

Firmware

Table 89 Firmware

Standards	IEEE 802.3 and 802.3u 10Base-T and 100Base-TX. IEEE 802.11b specification compliance for wireless LAN. IEEE 802.11g specification compliance for wireless LAN. IEEE 802.1x security standard. IEEE 802.3af standard. Wi-Fi certificate.
Spanning Tree Protocol	IEEE 802.1d
DHCP Relay	Ability to act as a DHCP relay to pass the IP address from the DHCP server from either WAN port or NAT router.
Security	MAC address filtering through WLAN, supporting 32 accounts. IEEE 802.1x security; MD5, EAP-TLS, EAP-TTLS and PEAP included. 64/128 bits WEP. WPA support. Dynamic WEP key exchange. Mixed WEP & WPA mode supporting both 802.1x with Dynamic WEP and WPA clients. SSL passthrough. VPN passthrough.

Table 89 Firmware (continued)

Diagnostics Capabilities	The access point can perform self-diagnostic tests. These tests check the integrity of the following circuits: FLASH memory. DRAM. Wireless port. Syslog. Errorlog. Trace log. Packet Log.
Management	Embedded Web Configurator management. Command-line interface. Telnet support; Password-protected telnet access to internal configuration manager. FTP/TFTP/Web for firmware downloading, configuration backup and restoration. Telnet remote access support. Built-in Diagnostic Tool. SNMP Management. RADIUS client.

Appendix C

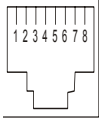
Power over Ethernet (PoE) Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7

Table 90 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 91 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

Appendix D

Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See [Appendix I](#) for information on the command structure.

Table 92 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Appendix E

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.

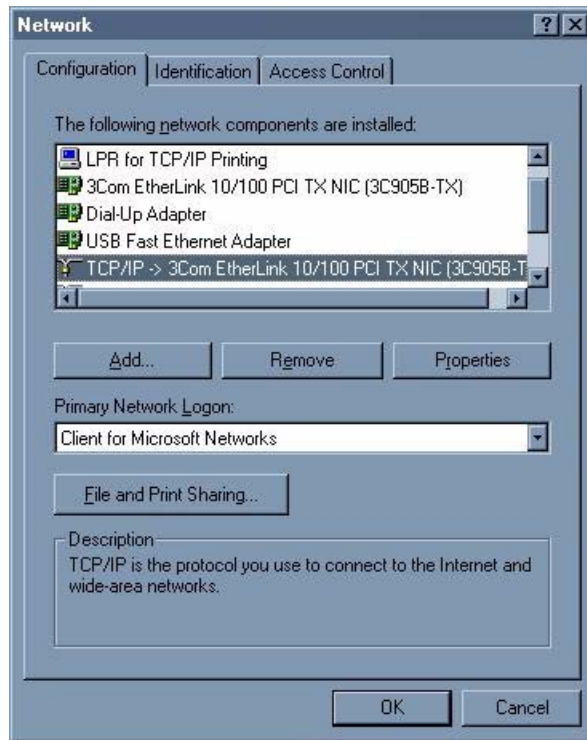
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 ZyAIR's LAN port.

Windows 95/98/Me

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

Figure 158 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:

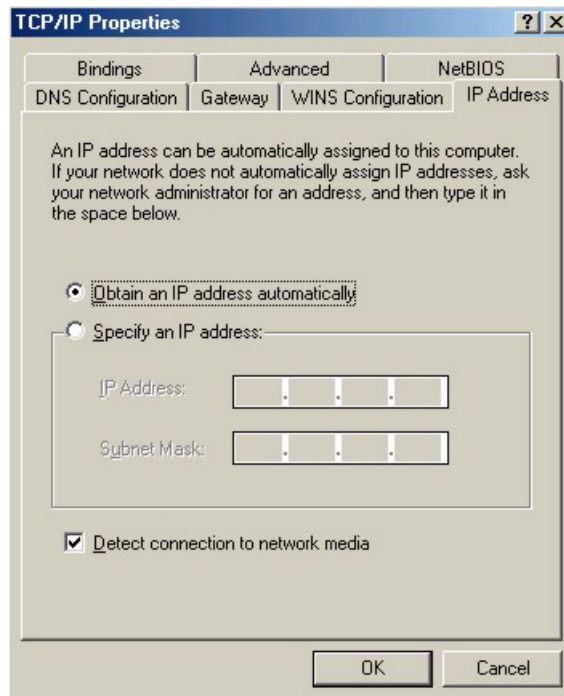
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

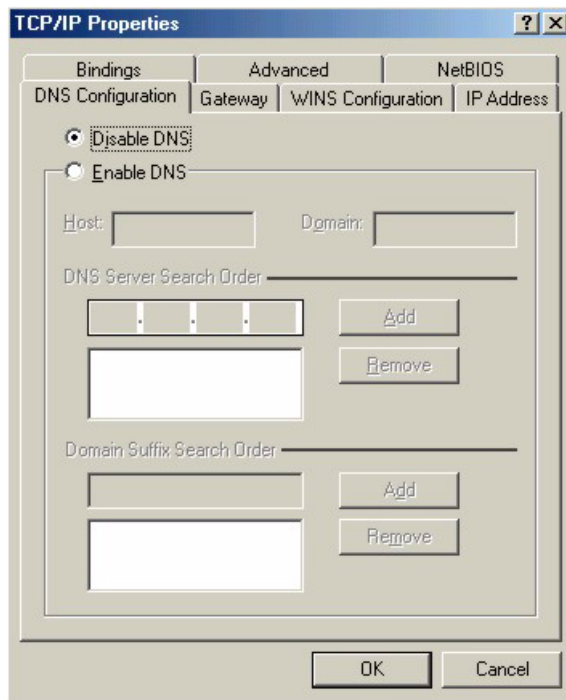
Configuring

- 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 159 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 160 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 ZyAIR 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

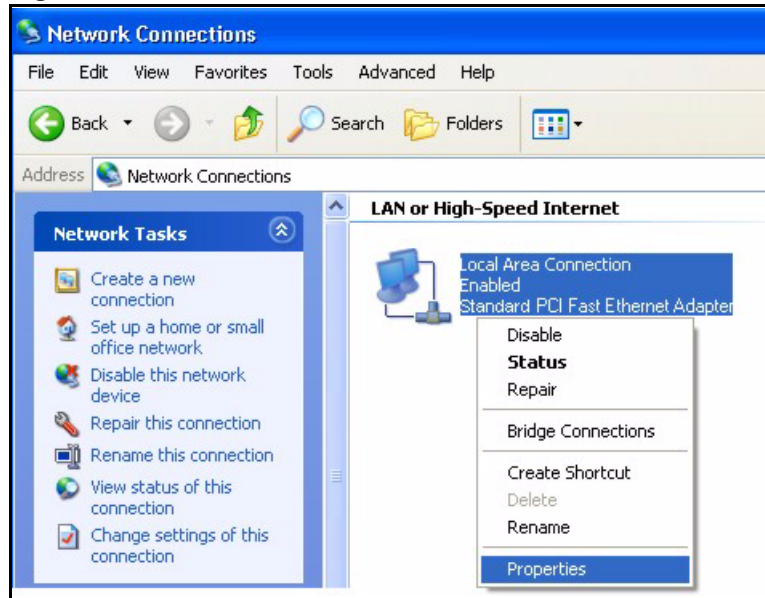
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 161 Windows XP: Start Menu

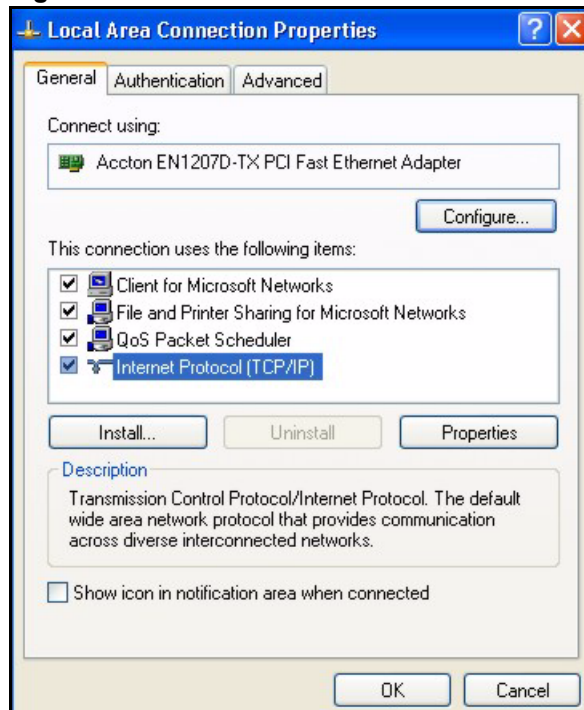
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 162 Windows XP: Control Panel

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

Figure 163 Windows XP: Control Panel: Network Connections: Properties

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

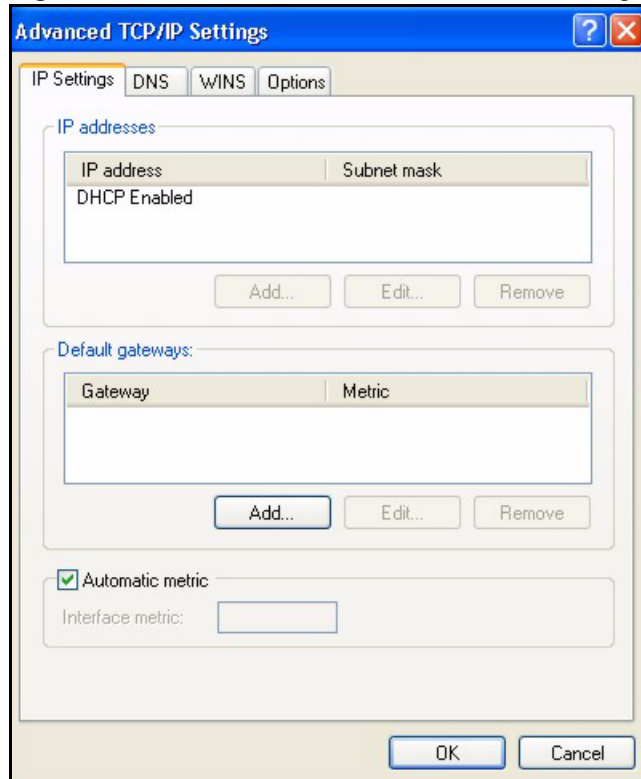
Figure 164 Windows XP: Local Area Connection Properties

- 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 165 Windows XP: Advanced TCP/IP Settings



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

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

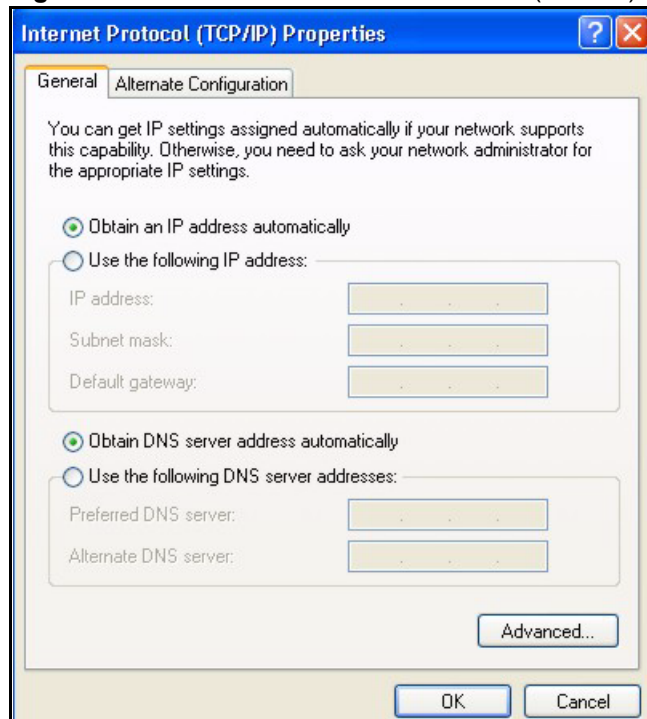
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

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

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

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

Figure 166 Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.
- 10 Turn on your ZyAIR and restart your computer (if prompted).

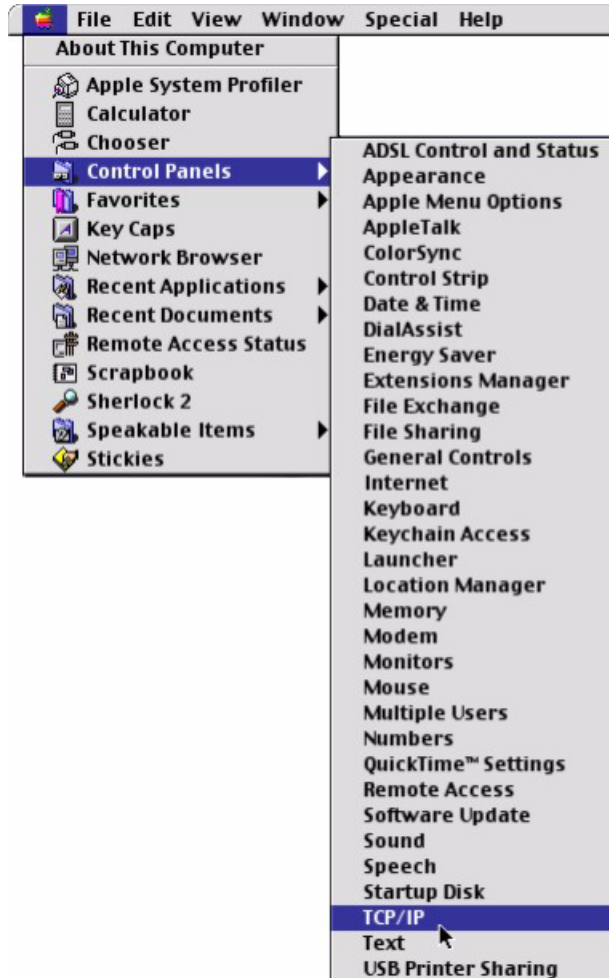
Verifying Settings

- 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

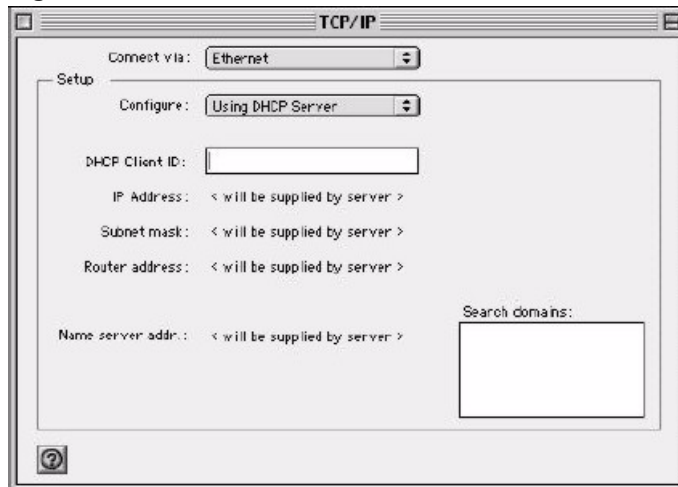
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 167 Macintosh OS 8/9: Apple Menu



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

Figure 168 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 ZyAIR 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 ZyAIR and restart your computer (if prompted).

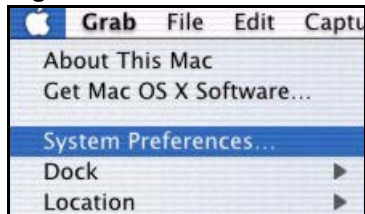
Verifying Settings

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

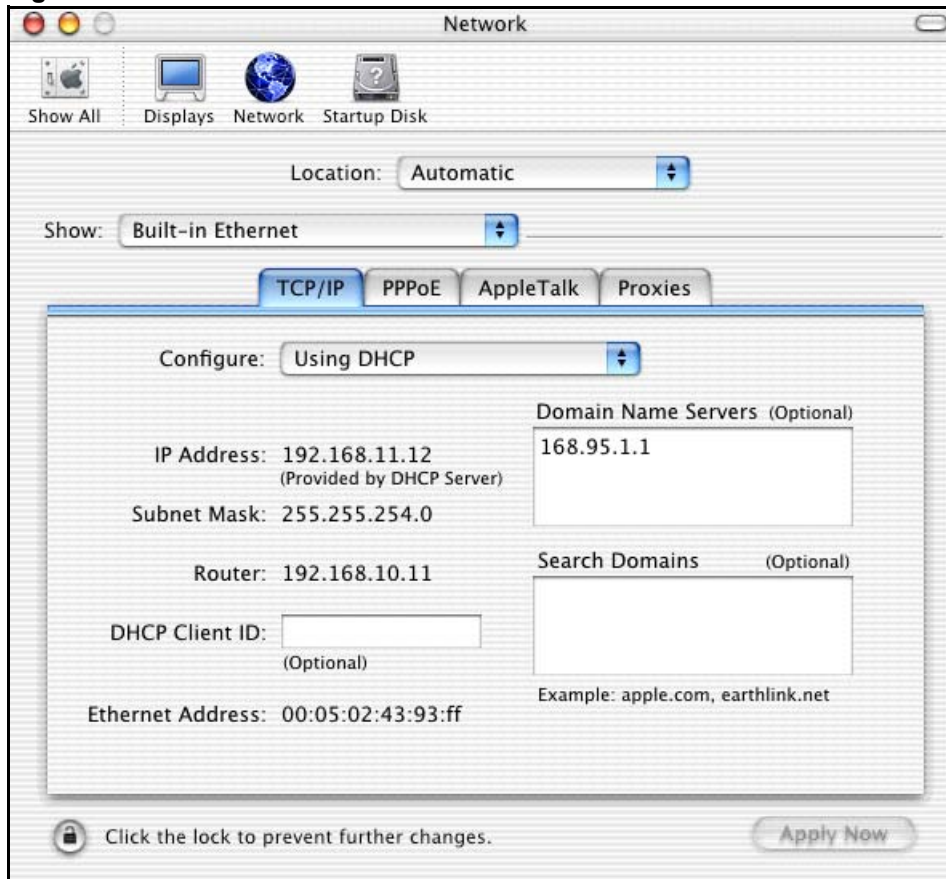
Macintosh OS X

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

Figure 169 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 170 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 ZyAIR in the **Router address** box.

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

6 Turn on your ZyAIR and restart your computer (if prompted).

Verifying Settings

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

Appendix F

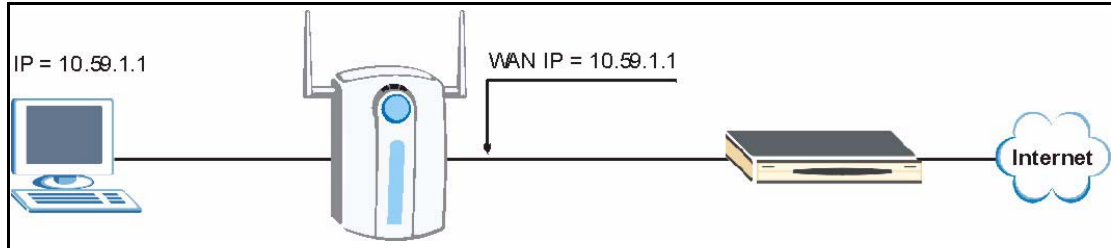
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The ZyAIR is using the same LAN and WAN IP addresses

The following figure shows an example where the ZyAIR is using a WAN IP address that is the same as the IP address of a computer on the LAN.

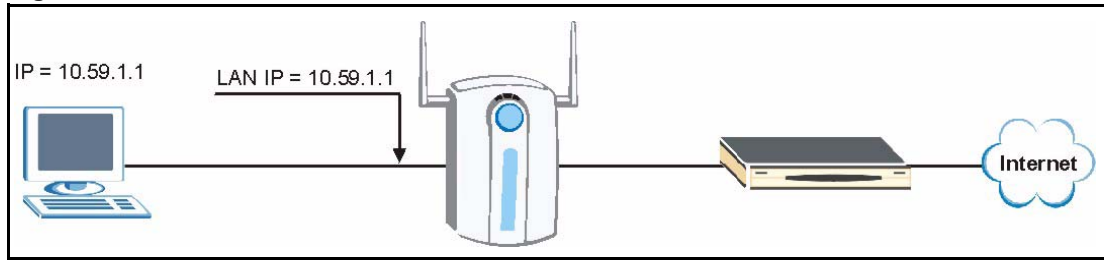
Figure 171 IP Address Conflicts: Case A



You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

Case B: The ZyAIR LAN IP address conflicts with the DHCP client IP address

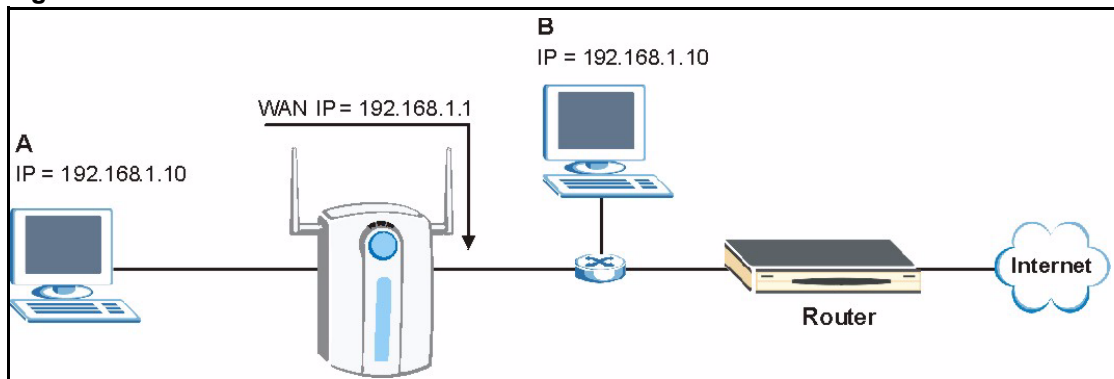
In the following figure, the ZyAIR is acting as a DHCP server. The ZyAIR assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

Figure 172 IP Address Conflicts: Case B

To solve this problem, make sure the ZyAIR LAN IP address is not in the DHCP IP address pool.

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the ZyAIR.

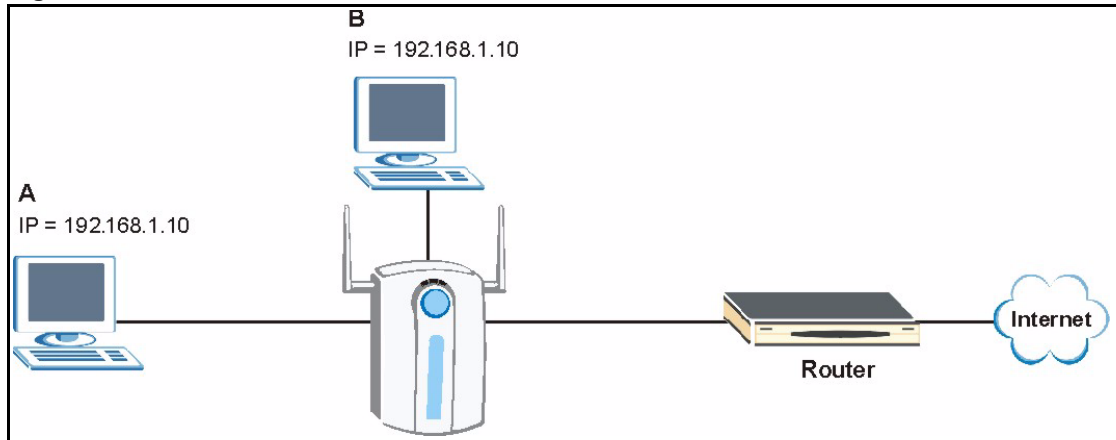
Figure 173 IP Address Conflicts: Case C

You must set the ZyAIR to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyAIR. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyAIR use a public WAN IP address.

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyAIR allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the ZyAIR DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

Figure 174 IP Address Conflicts: Case D

This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

Appendix G

Wireless LANs

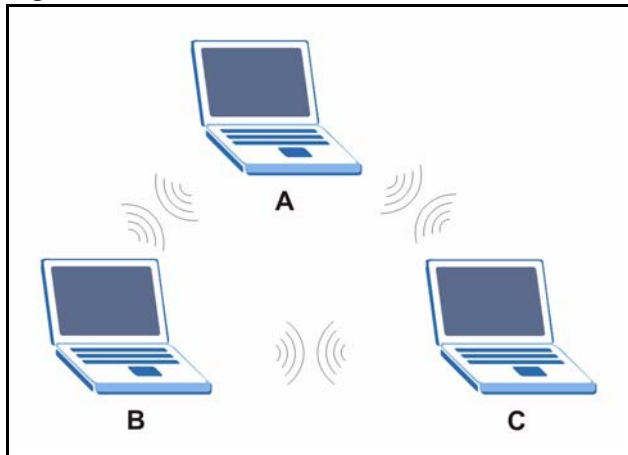
Wireless LAN Topologies

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.

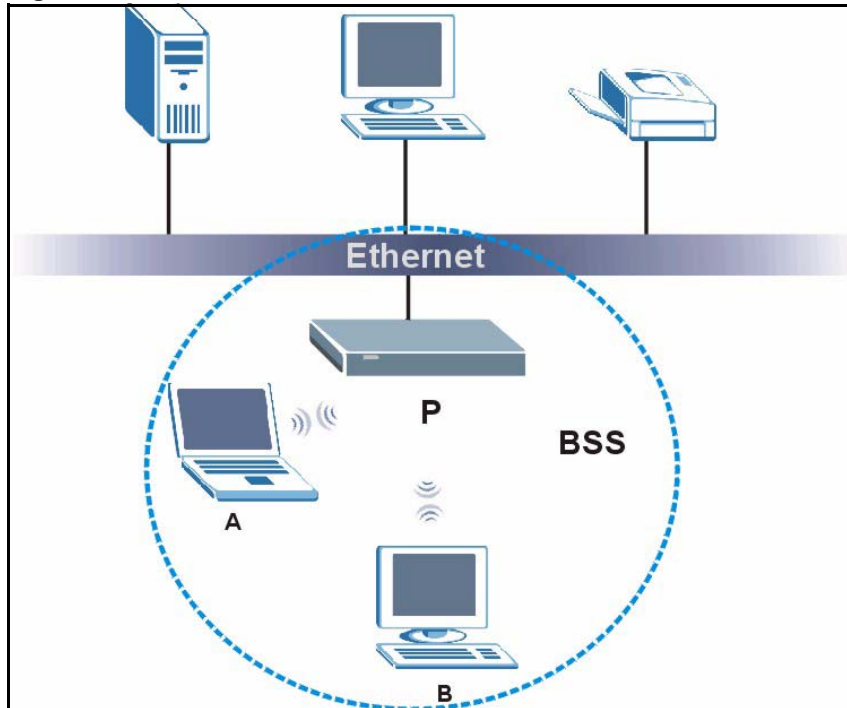
Figure 175 Peer-to-Peer Communication in an Ad-hoc Network



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.

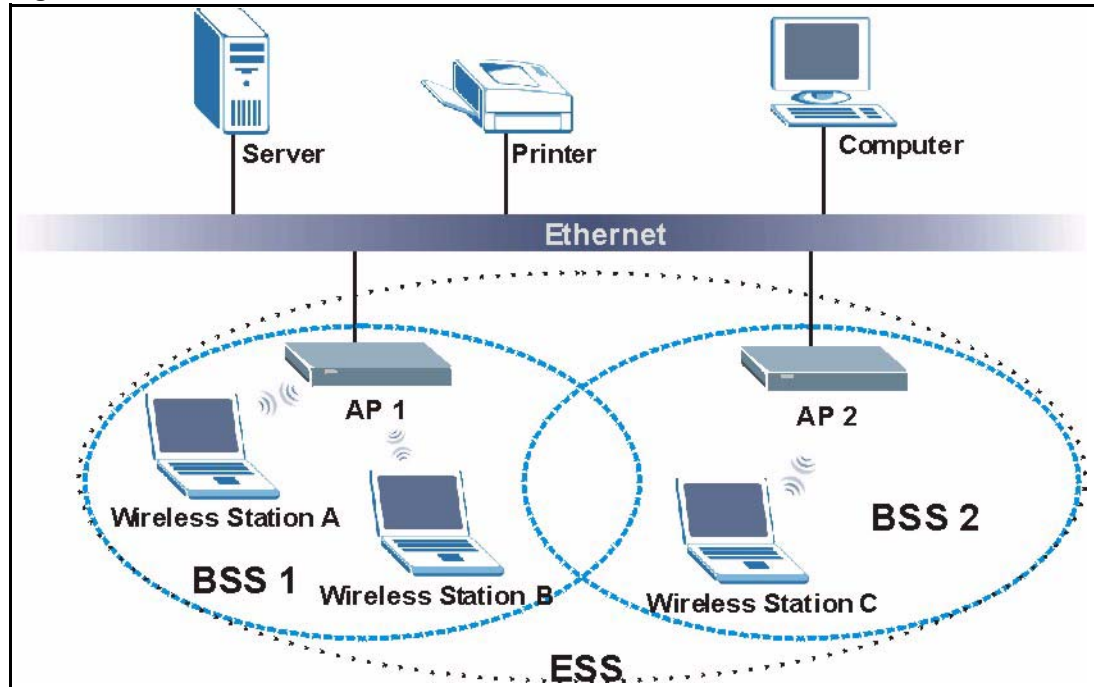
Figure 176 Basic Service Set

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 177 Infrastructure WLAN

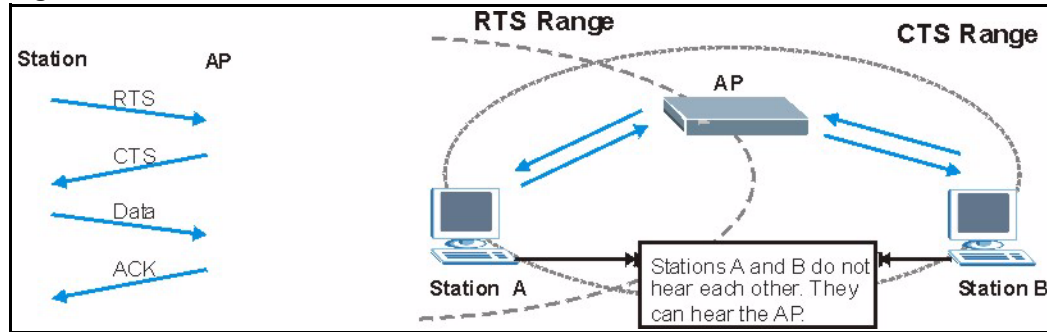
Channel

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 178 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.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations **MUST** use the same preamble mode in order to communicate.

IEEE 802.11b Wireless LAN

The 802.11b data rate and corresponding modulation techniques are shown in the table below. The modulation technique defines how bits are encoded onto radio waves.

Table 93 IEEE 802.11b

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shifted Keying)
2	DQPSK (Differential Quadrature Phase Shifted Keying)
5.5 / 11	CCK (Complementary Code Keying)

Note: The ZyAIR may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

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.

Types of Authentication

This appendix 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.

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 94 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)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA 2 (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.

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.

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

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

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 decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

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

User Authentication

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

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.

Security Parameters Summary

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

Table 95 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable

Table 95 Wireless Security Relational Matrix (continued)

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

Appendix H

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Table 96 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.

A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Table 97 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

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 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 as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Table 98 “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 left most 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 99 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

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 100 Two Subnets Example

	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”). You want to have two separate 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 form 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 101 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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 102 Subnet 2

	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	

The remaining 7 bits determine the number of hosts each subnet can have. 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 of 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 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 103 Subnet 1

	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
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 104 Subnet 2

	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 105 Subnet 3

	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 106 Subnet 4

	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 8 subnets (001, 010, 011, 100, 101, 110).

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

Table 107 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 108 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 96](#)) available for subnetting.

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

Table 109 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 I

Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix J

Log Descriptions

This appendix provides descriptions of example log messages.

Table 110 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
SMT Login Successfully	Someone has logged on to the router's SMT interface.
SMT Login Fail	Someone has failed to log on to the router's SMT interface.
WEB Login Successfully	Someone has logged on to the router's web configurator interface.
WEB Login Fail	Someone has failed to log on to the router's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via FTP.
FTP Login Fail	Someone has failed to log on to the router via FTP.

Table 111 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect

Table 111 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 112 Sys log

LOG MESSAGE	DESCRIPTION
<pre>Mon dd hr:mm:ss hostname src=<srcIP:srcPort> dst=<dstIP:dstPort> msg=<msg> note=<note></pre>	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

Log Commands

Go to the command interpreter interface (the [Command Interpreter appendix](#) explains how to access and use the commands).

Configuring What You Want the ZyAIR to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyAIR is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 113 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyAIR (you must do this in order to record logs).

Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyAIR's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyAIR log category.

Use the `sys logs clear` command to erase all of the ZyAIR's logs.

Log Command Example

This example shows how to set the ZyAIR to record the error logs and alerts and then view the results.

```

ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

#.      time                source                destination          notes      message
0 | 11/11/2002 15:10:12 | 172.22.3.80:137 | 172.22.255.255:137 | ACCESS   BLOCK

```


Appendix K

Indoor Installation Recommendations

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Appendix L

Power Adaptor Specifications

Table 114 North American Plug Standards

AC Power Adaptor Model	ADS6818-1812-W 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5A, 18W
Power Consumption	6 W Max
Safety Standards	UL, CUL (UL60950 Third Edition, CSA C22.2 No. 60950)

Table 115 European Plug Standards

AC Power Adaptor Model	ADS6818-1812-B 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS, CE (EN 60950)

Table 116 United Kingdom Plug Standards

AC Power Adaptor Model	ADS6818-1812-D 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS (BS EN 60950)

Table 117 Australia and New Zealand Plug Standards

AC Power Adaptor Model	ADS6818-1812-A 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	DOFT (AS/NZS 60950, AS/NZSB 3112:1-2)

Index

A

Address Assignment [48](#), [127](#)
Alternative Subnet Mask Notation [269](#)
Antenna
 Directional [282](#)
 Omni-directional [282](#)
Antenna gain [281](#)
AP (access point) [257](#)
Applications [36](#)
Authentication databases [85](#), [86](#)
Auto-crossover Ethernet/Fast Ethernet Interface [31](#)
Auto-negotiating Ethernet/Fast Ethernet Interface [31](#)
auto-negotiation [31](#)

B

Backup [168](#)
backup [208](#)
Basic Service Set [57](#)
Bridge Protocol Data Units (BPDUs) [63](#)
Bridge/Repeater [32](#)
Brute-Force Password Guessing Protection [35](#)
BSS [57](#), [255](#)

C

CA [262](#)
Certificate Authority [262](#)
Channel [45](#), [257](#)
 Interference [257](#)
Channel ID [181](#)
Class of Service [61](#)
Class of Service (CoS) [61](#)
CLI Command
 Configure tagged VLAN example [115](#)
Collision [202](#)
Command Interpreter [219](#)
Community [197](#)
Contact Information [6](#)
Contacting Customer Support [6](#)

CoS [61](#)
CPU Load [202](#)
CTS (Clear to Send) [258](#)
Customer Support [6](#)

D

Data encryption [45](#)
Default [170](#)
Denmark, Contact Information [6](#)
DHCP [204](#)
Diagnostic [205](#)
Diagnostic Tools [201](#)
Differentiated Services [61](#)
DiffServ [61](#)
DiffServ Code Point (DSCP) [61](#)
DiffServ Code Points [61](#)
DiffServ marking rule [61](#)
Distribution System [58](#)
DS Field [61](#)
DS field [61](#)
DSCPs [61](#)
Dynamic WEP Key Exchange [75](#), [262](#)

E

EAP [35](#), [73](#), [74](#)
EAP Authentication [261](#)
EAP-MD5 [261](#)
EAP-TLS [262](#)
EAP-TTLS [262](#)
Encryption [76](#), [263](#)
Error Log [204](#)
Error/Information Messages
 Sample [205](#)
ESS [58](#), [256](#)
ESS ID [45](#)
ESS IDentification [58](#)
Extended Service Set [58](#), [256](#)
Extended Service Set IDentification [65](#), [96](#), [187](#)

F

Filename Conventions [207](#)
Finland, Contact Information [6](#)
Firmware File
 Maintenance [166](#)
Fragment Threshold [181](#)
Fragmentation Threshold [258](#)
Fragmentation threshold [258](#)
France, Contact Information [6](#)
FTP [147](#), [151](#), [229](#)
 Restrictions [229](#)
FTP File Transfer [214](#)
FTP Restrictions [147](#)

G

General Setup [46](#), [51](#), [177](#)
General Specifications [235](#)
Germany, Contact Information [6](#)

H

Hidden Menus [173](#)
Hidden node [257](#)
Host [53](#)
Host IDs [267](#)
How STP Works [63](#)
HyperTerminal program [211](#)

I

IBSS [255](#)
IEEE 802.1x [35](#), [260](#)
In-band Management [115](#)
Independent Basic Service Set [165](#), [255](#)
Internet access [179](#)
Internet Security Gateway [31](#)
IP Address [48](#), [127](#), [128](#), [180](#), [204](#), [206](#)
IP Addressing [267](#)
IP Classes [267](#)
IPSec VPN Capability [34](#)

L

LAN [162](#)
LEAP [262](#)
Link type [202](#)
Log and Trace [205](#)
Log Descriptions [277](#)
Logs [157](#)

M

MAC address [108](#)
MAC Address Filter Action [109](#), [184](#)
MAC Address Filtering [182](#)
MAC Filter [108](#)
MAC filter [73](#)
MAC Filtering [35](#)
MAC service data unit [65](#), [69](#), [95](#)
Main Menu [174](#)
Management Information Base (MIB) [153](#)
Management VLAN [115](#)
Max Age [63](#)
Max. Frame Burst [66](#), [97](#)
MSDU [65](#), [69](#), [95](#)

N

Network Management [36](#)
North America Contact Information [6](#)
Norway, Contact Information [6](#)

O

Out-of-band Management [115](#)

P

Packets [202](#)
Password [52](#), [171](#), [197](#)
Path cost [62](#)
PEAP [262](#)
Per-Hop Behavior [61](#)

PHB (Per-Hop Behavior) [61](#)

Ping [206](#)

PoE [32](#), [235](#)

Power over Ethernet [32](#)

Power Specification [235](#)

Preamble Mode [259](#)

Priorities [60](#)

Private IP Address [48](#), [127](#)

Product Model [6](#)

Product Serial Number [6](#)

Q

Quick Start Guide [41](#)

R

RADIUS [35](#), [260](#)

 Shared Secret Key [261](#)

RADIUS Message Types [260](#)

RADIUS Messages [260](#)

Rapid STP [62](#)

RAS [204](#)

Rate

 Receiving [202](#)

 Transmission [202](#)

ReAuthentication Time [84](#), [86](#), [87](#), [88](#)

Regular Mail [6](#)

Related Documentation [27](#)

Remote Authentication Dial In User Service [35](#)

Remote Management and NAT [148](#)

Remote Management Limitations [147](#), [229](#)

Remote Management Setup [227](#)

Remote Node [202](#)

Required fields [174](#)

Reset Button [31](#)

Restore [169](#)

Restore Configuration [212](#)

Roaming [109](#)

 Requirements [111](#)

Root bridge [62](#)

RTS (Request To Send) [258](#)

RTS Threshold [181](#), [257](#), [258](#)

RTS/CTS handshake [65](#), [69](#), [95](#)

S

Security Parameters [264](#)

Serial Number [6](#)

Service Set [65](#), [96](#), [187](#)

SMT Menu Overview [172](#)

SNMP [35](#), [152](#)

 Community [197](#)

 Configuration [197](#)

 Manager [153](#)

 MIBs [154](#)

 Traps [155](#)

 Trusted Host [197](#)

Spain, Contact Information [7](#)

Spanning Tree Protocol [62](#)

SSL Passthrough [35](#)

STP [62](#)

STP (Spanning Tree Protocol) [34](#)

STP Path Costs [62](#)

STP Port States [63](#)

STP Terminology [62](#)

Subnet Mask [48](#), [127](#), [180](#), [204](#)

Subnet Masks [268](#)

Subnetting [268](#)

Support E-mail [6](#)

Sweden, Contact Information [7](#)

Syntax Conventions [28](#)

System

 Console Port Speed [204](#)

 Diagnostic [205](#)

 Log and Trace [204](#)

 System Information [203](#)

 System Status [201](#)

 Time and Date [224](#)

System Information [203](#)

System Information & Diagnosis [201](#)

System Maintenance [201](#), [203](#), [208](#), [210](#), [212](#), [213](#), [216](#),
[217](#), [219](#), [225](#)

System Name [51](#)

System Timeout [148](#), [229](#)

T

TCP/IP [206](#), [226](#)

Telephone [6](#)

Telnet [150](#), [226](#)

Telnet Configuration [226](#)

Telnet Under NAT [226](#)

TFTP

 Restrictions [229](#)

TFTP File Transfer [215](#)
TFTP Restrictions [147](#)
Time and Date Setting [225](#)
Time Setting [53](#)
Time Zone [226](#)
ToS [60](#)
Trace Records [204](#)
Troubleshooting
 Accessing ZyAIR [232](#)
 Ethernet Port [231](#)
 Start-Up [231](#)
Type Of Service [60](#)

U

Upload Firmware [213](#)
Use Authentication [264](#)
User Authentication [76](#)
User Profiles [193](#)

V

Valid CI Commands [220](#)
Virtual Local Area Network [113](#)
VLAN [33](#), [113](#)

W

Warranty Information [6](#)
WDS [33](#), [67](#)
Web [148](#)
Web Configurator [41](#), [43](#)
Web Site [6](#)
WEP [45](#)
WEP Encryption [35](#), [83](#)
WEP encryption [74](#)
Wi-Fi Multimedia QoS [60](#)
Wi-Fi Protected Access [32](#)
Wireless Client WPA Supplicants [79](#)
Wireless Distribution System [33](#)
Wireless LAN [180](#)
Wireless LAN Setup [180](#)
Wireless LAN Topologies [255](#)
Wireless security [73](#)
Wizard Setup [45](#), [46](#), [48](#)

WLAN
 Interference [257](#)
 Security parameters [264](#)
Worldwide Contact Information [6](#)
WPA [32](#), [75](#)
WPA with RADIUS Application [77](#)
WPA, WPA2 [263](#)

Z

ZyAIR LED [32](#)
ZyNOS [208](#)
ZyNOS F/W Version [208](#)